Introduction To TPH #1

This phile was written for beginning as well as those uninformed "advanced" phreaks who need something as a reference when reading or writing philes concerning phreaking or fone phraud. Of course, you could be a beginning phreak and use this phile to B.S. your way into a big group by acting like you know a lot, or something, but that is up to you. Anyway, I compiled this listing phrom various sources, the majority is listed as references at the end of this phile.

This phile's only goal is to educate and inform. Any illegal or fraudulent activity is neither encouraged nor supported by the author of this phile, not by the majority of the >TRUE< phreaking community. The author assumes NO responsibility for the actions of the reader.

Also, I know that some of the stuff covered in this release of TPH will be old and outdated; however, I will try to clean that up by the next release of TPH, and will notify you, the reader, of the changes due to these revisions.

The Phreak's Vitals:

True Definition Of The Phreaker

"Many people think of phone phreaks as slime, out to rip off Bell for all she is worth. Nothing could be further from the truth! Granted, there are some who get their kicks by making free calls; however, they are not true phone phreaks. Real phone phreaks are 'telecommunications hobbyists' who experiment, play with, and learn from the phone system. Occasionally, this experimenting and a need to communicate with other phreaks, without going broke, leads to free calls. The free calls are but a small subset of a >TRUE< phone phreak's activities."

- Wise Words Of The Magician

The Phone Phreak's Ten Commandments

I. Box thou not over thine home telephone wires, for those who doest will surely bring the wrath of the Chief Special Agent down upon thy head.
II. Speakest thou not of important matters over thine home telephone wires, for to do so is to risk thine right of freedom.
III. Use not thine own name when speaking to other phreaks, for that every third phreak is an FBI agent is well known.
IV. Let not overly many people know that thy be a phreak, as to do so is to use thine own self as a sacrificial lamb.
V. If thou be in school, strive to get thine self good grades, for the

authorities well know that scholars never break the law.

VI. If thou workest, try to be an employee and impressest thine boss with thine enthusiasm, for important employees are often saved by their own bosses.

VII. Storest thou not thine stolen goodes in thine own home, for those who do are surely non-believers in the Bell System Security Forces, and are not long for this world.

VIII. Attractest thou not the attention of the authorities, as the less noticeable thou art, the better.

IX. Makest sure thine friends are instant amnesiacs and willst not remember thou hast called illegally, for their cooperation with the authorities willst surely lessen thine time for freedom on this earth.

X. Supportest thou TAP, as it is thine newsletter, and without it, thy work would be far more limited.

The Phreaker's Glossary

1XB - No.1 Crossbar system. See XBAR for more information.

2600 - A hack/phreak oriented newsletter that periodically was released and still is being released. See Phile 1.6 for more information on the magazine and ordering.

4XB - No.4 Crossbar system. See XBAR for more information.

5XB - No.5 Crossbar system. The primary end office switch of Bell since the 60's and still in wide use. See XBAR for more detail.

700 Services - These services are reserved as an advanced forwarding system, where the forwarding is advanced to a user-programed location which could be changed by the user.

800 Exceptional Calling Report - System set up by ESS that will log any caller that excessively dials 800 numbers or directory assistance. See ESS for more information.

800 Services - Also known as WATS. These services often contain WATS extenders which, when used with a code, may be used to call LD. Many LD companies use these services because they are toll-free to customers. Most 800 extenders are considered dangerous because most have the ability to trace.

900 Services - Numbers in the 900 SAC usually are used as special services, such as TV polls and such. These usually are $.50 for the first minute and $.35 for each additional minute. Dial (900)555-1212 to find out what the 900 services currently have to offer.

950 - A nationwide access exchange in most areas. Many LD companies have extenders located somewhere on this exchange; however, all services on this exchange are considered dangerous due to the fact that they ALL have the ability to trace. Most 950 services have

crystal clear connections.

ACCS - Automated Calling Card Service. The typical 0+NPA+Nxx+xxxx method of inputting calling cards and then you input the calling card via touch tones. This would not be possible without ACTS.

ACD - Automatic Call Distributor.

ACD Testing Mode - Automatic Call Distributor Test Mode. This level of phreaking can be obtained by pressing the "D" key down after calling DA. This can only be done in areas that have the ACD. The ACD Testing Mode is characterized by a pulsing dial tone. From here, you can get one side of a loop by dialing 6, the other side is 7. You may also be able to REMOB a line. All possibilities of the ACD Test have not been experimented with. See silver box for more details.

ACTS - Automated Coin Toll Service. This is a computer system that automates phortress fone service by listening for red box tones and takes appropriate action. It is this service that is commonly heard saying, "Two dollars please. Please deposit two dollars for the next three minutes." Also, if you talk for more than three minutes and then hang up, ACTS will call back and demand your money. ACTS is also responsible for ACCS.

Alliance - A teleconferencing system that is apart from AT&T which allows the general public to access and use its conferencing equipment. The equipment allows group conversations with members participating from throughout the United States. The fone number to Alliance generally follows the format of 0-700-456-x00x depending on the location the call originates from and is not accessible direct by all cities/states.

AMA - Automated Message Accounting. Similar to the CAMA system; see CAMA for more info.

analog - As used for a word or data transmission, a continuously varying electrical signal in the shape of a wave.

ANI - Automatic Number Identification - This is the system you can call, usually a three digit number or one in the 99xx's of your exchange, and have the originating number you are calling from read to you by a computer. This is useful if you don't know the number you are calling from, for finding diverters, and when you are playing around with other fone equipment like cans or beige boxes. The ANI system is often incorporated into other fone companies such as Sprint and MCI in order to trace those big bad phreaks that abuze codez.

ANIF - Automatic Number Identification Failure. When the ANI system of a particular office fails.

APF - All PINs Fail. This is a security measure which is designed to frustrate attempts at discovering valid PINs by a hacking method.

aqua box - A box designed to drain the voltage of the FBI lock-in-

trace/trap-trace so you can hang up your fone in an emergency and phrustrate the Pheds some more. The apparatus is simple, just connect the two middle wires of a phone wire and plug, which would be the red and green wires if in the jack, to the cord of some electrical appliance; ie, light bulb or radio. KEEP THE APPLIANCE OFF. Then, get one of those line splitters that will let you hook two phone plugs into one jack. Plug the end of the modified cord into one jack and your fone into the other. THE APPLIANCE MUST BE OFF! Then, when the Pheds turn their lame tracer on and you find that you can't hang up, remove your fone from the jack and turn the appliance ON and keep it ON until you feel safe; it may be awhile. Then turn it off, plug your fone back in, and start phreaking again.
Invented by: Captain Xerox and The Traveler.

BAUDOT - 45.5 baud. Also known as the Apple Cat Can.

BEF - Band Elimination Filter. A muting system that will mute the 2600 Hz tone which signals hang-up when you hang up.

beige box - An apparatus that is a home-made lineman's handset. It is a regular fone that has clips where the red and green wires normally connect to in a fone jack. These clips will attach to the rings and tips found in many of MA's output devices. These are highly portable and VERY useful when messing around with cans and other output devices the fone company has around.
Invented by: The Exterminator and The Terminal Man.

BITNET - Nationwide system for colleges and schools which accesses a large base of education-oriented information. Access ports are always via mainframe.

bit stream - Refers to a continuous series of bits, binary digits, being transmitted on a transmission line.

black box - The infamous box that allows the calling party to not be billed for the call placed. We won't go in depth right now, most plans can be found on many phreak oriented BBS's. The telco can detect black boxes if they suspect one on the line. Also, these will not work under ESS.

bleeper boxes - The United Kingdom's own version of the blue box, modified to work with the UK's fone system. Based on the same principles. However, they use two sets of frequencies, foreword and backwards.

Blotto box - This box supposedly shorts every fone out in the immediate area, and I don't doubt it. It should kill every fone in the immediate area, until the voltage reaches the fone company, and the fone company filters it. I won't cover this one in this issue, cuz it is dangerous, and phreaks shouldn't destroy MA's equipment, just phuck it up. Look for this on your phavorite BBS or ask your phavorite phreak for info if you really are serious about seriously phucking some fones in some area.

blue box - An old piece of equipment that emulated a true operator placing calls, and operators get calls for free. The blue box seizes an open trunk by blasting a 2600 Hz tone through the line after dialing a party that is local or in the 800 NPA so calls will be local or free for the blue boxer. Then, when the blue boxer has seized a trunk, the boxer may then, within the next 10-15 seconds, dial another fone number via MF tones. These MF tones must be preceded by a KP tone and followed with a ST tone. All of these tones are standardized by Bell. The tones as well as the inter-digit intervals are around 75ms. It may vary with the equipment used since ESS can handle higher speeds and doesn't need inter-digit intervals. There are many uses to a blue box, and we will not cover any more here. See your local phreak or phreak oriented BBS for in depth info concerning blue boxes and blue boxing. Incidentally, blue boxes are not considered safe anymore because ESS detects "foreign" tones, such as the 2600 Hz tone, but this detection may be delayed by mixing pink noise of above 3000 Hz with the 2600 Hz tone. To hang up, the 2600 Hz tone is played again. Also, all blue boxes are green boxes because MF "2" corresponds to the Coin Collect tone on the green box, and the "KP" tone corresponds to the Coin Return tone on the green box. See green box for more information. Blue boxing is IMPOSSIBLE under the new CCIS system slowly being integrated into the Bell system.

blue box tones - The MF tones generated by the blue box in order to place calls, emulating a true operator. These dual tones must be entered during the 10-15 second period after you have seized a trunk with the 2600 Hz tone.

```
                    700:  1 :  2 :  4 :  7 : 11 :    KP= Key Pulse
 Parallel Frequencies   900: ** :  3 :  5 :  8 : 12 :    ST= STop
  2= Coin Collect     1100: ** : ** :  6 :  9 : KP :   KP2= Key Pulse 2
 KP= Coin Return       1300: ** : ** : ** : 10 :KP2 :    **= None
 (green box tones)    1500: ** : ** : ** : ** : ST :
                     : 900:1100:1300:1500:1700:   75ms pulse/pause
```

BLV - Busy Line Verification. Allows a TSPS operator to process a customer's request for a confirmation of a repeatedly busy line. This service is used in conjunction with emergency break-ins.

BNS - Billed Number Screening.

break period - Time when the circuit during pulse dialing is left open. In the US, this period is 40ms; foreign nations may use 33ms break periods.

break ratio - The interval pulse dialing breaks and makes the loop when dialing. The US standard is 10 pulses per second. When the circuit is opened, it is called the break interval. When the circuit is closed, it is called the make interval. In the US, there is a 60ms make period and a 40ms break period. This is often referred to as a 60% make interval. Many foreign nations have a 67% make interval.

bridge - I don't really understand this one, but these are important phreak toys. I'll cover them more in the next issue of TPH.

British Post Office - The United Kingdom's equivalent to Ma Bell.

busy box - Box that will cause the fone to be busy, without taking it OFF-HOOK. Just get a piece of fone wire with a plug on the end, cut it off so there is a plug and about two inches of fone line. Then, strip the wire so the two middle wires, the tip and the ring, are exposed. Then, wrap the ring and the tip together, tape with electrical tape, and plug into the fone jack. The fone will be busy until the box is removed.

cans - Cans are those big silver boxes on top of or around the telephone poles. When opened, the lines can be manipulated with a beige box or whatever phun you have in mind.

calling card - Another form of the LD service used by many major LD companies that composes of the customers fone number and a PIN number. The most important thing to know when questioned about calling cards are the area code and the city where the calling card customer originated from.

CAMA - Centralized Automatic Message Accounting. System that records the numbers called by fones and other LD systems. The recording can be used as evidence in court.

CC - Calling Card.

CC - Credit Card.

CCIS - Common Channel Inter-office Signaling. New method being incorporated under Bell that will send all the signaling information over separate data lines. Blue boxing is IMPOSSIBLE under this system.

CCITT - The initials of the name in French of the International Telegraph and Telephone Consultative Committee. At CCITT representatives of telecommunications authorities, operators of public networks and other interested bodies meet to agree on standards needed for international intermarrying of telecommunications services.

CCS - Calling Card Service.

CCSS - Common Channel Signalling System. A system whereby all signalling for a number of voice paths are carried over one common channel, instead of within each individual channel.

CDA - Coin Detection and Announcement.

CF - Coin First. A type of fortress fone that wants your money before you receive a dial tone.

Channel - A means of one-way transmission or a UCA path for electrical transmission between two or more points without common carrier, provided terminal equipment. Also called a circuit, line, link, path, or facility.

cheese box - Another type of box which, when coupled with call forwarding

services, will allow one to place free fone calls. The safety of this box is unknown. See references for information concerning text philes on this box.

clear box - Piece of equipment that compromises of a telephone pickup coil and a small amp. This works on the principal that all receivers are also weak transmitters. So, you amplify your signal on PP fortress fones and spare yourself some change.

CN/A - Customer Name And Address. Systems where authorized Bell employees can find out the name and address of any customer in the Bell System. All fone numbers are listed on file, including unlisted numbers. Some CN/A services ask for ID#'s when you make a request. To use, call the CN/A office during normal business hours, and say that you are so and so from a certain business or office, related to customers or something like that, and you need the customer's name and address at (NPA)Nxx-xxxx. That should work. The operators to these services usually know more than DA operators do and are also susceptible to "social engineering." It is possible to bullshit a CN/A operator for the NON PUB DA number and policy changes in the CN/A system.

CO Code - Central Office code which is also the Nxx code. See Nxx for more details. Sometimes known as the local end office.

conference calls - To have multiple lines inter-connected in order to have many people talking in the same conversation on the fone at once. See Alliance and switch crashing for more information.

credit operator - Same as TSPS operator. The operator you get when you dial "0" on your fone and phortress fones. See TSPS for more information.

CSDC - Circuit Switched Digital Capability. Another USDN service that has no ISDN counterpart.

DA - Directory Assistance. See directory assistance.

DAO - Directory Assistance Operator. See directory assistance.

data communications - In telefone company terminology, data communications refers to an end-to-end transmission of any kind of information other than sound, including voice, or video. Data sources may be either digital or analog.

data rate - The rate at which a channel carries data, measured in bits per second, bit/s, also known as "data signalling rate."

data signalling rate - Same as "data rate." See data rate.

DCO-CS - Digital Central Office-Carrier Switch.

DDD - Direct Distance Dialed.

Dial-It Services - See 900 Services.

digital - A method to represent information to be discrete or individually distinct signals, such as bits, as opposed to a continuously variable analog signal.

digital transmission - A mode of transmission in which all information to be transmitted is first converted to digital form and then transmitted as a serial stream of pulses. Any signal, voice, data, television, can be converted to digital form.

Dimension 2000 - Another LD service located at (800)848-9000.

directory assistance - Operator that you get when you call 411 or NPA-555-1212. This call will cost $.50 per call. These won't know where you are calling from, unless you annoy them, and do not have access to unlisted numbers. There are also directory assistance operators for the deaf that transfer BAUDOT. You can call these and have interesting conversations. The fone number is 800-855-1155, are free, and use standard Telex abbreviations such as GA for Go Ahead. These are nicer than normal operators, and are often subject to "social engineering" skills (bullshitting). Other operators also have access to their own directory assistance at KP+NPA+131+ST.

diverter - This is a nice phreak tool. What a diverter is is a type of call forwarding system done externally, apart from the fone company, which is a piece of hardware that will foreword the call to somewhere else. These can be found on many 24 hour plumbers, doctors, etc. When you call, you will often hear a click and then ringing, or a ring, then a click, then another ring, the second ring often sounds different from the first. Then, the other side picks the fone up and you ask about their company or something stupid, but DO NOT ANNOY them. Then eventually, let them hang up, DO NOT HANG UP YOURSELF. Wait for the dial tone, then dial ANI. If the number ANI reads is different from the one you are calling from, then you have a diverter. Call anywhere you want, for all calls will be billed to the diverter. Also, if someone uses a tracer on you, then they trace the diverter and you are safe. Diverters can, however, hang up on you after a period of time; some companies make diverters that can be set to clear the line after a set period of time, or click every once in a while, which is super annoying, but it will still work. Diverters are usually safer than LD extenders, but there are no guarantees. Diverters can also be accessed via phortress fones. Dial the credit operator and ask for the AT&T CREDIT OPERATOR. They will put on some lame recording that is pretty long. Don't say anything and the recording will hang up. LET IT HANG UP, DO NOT HANG UP. Then the line will clear and you will get a dial tone. Place any call you want with the following format: 9+1+NPA+Nxx+xxxx, or for local calls, just 9+Nxx+xxxx. I'd advise that you call ANI first as a local call to make sure you have a diverter.

DLS - Dial Line Service.

DNR - Also known as pen register. See pen register.

DOV - Data-Over-Voice.

DSI - Data Subscriber Interface. Unit in the LADT system that will concentrate data from 123 subscribers to a 56k or a 9.6k bit-per-second trunk to a packet network.

DT - Dial tone.

DTF - Dial Tone First. This is a type of fortress fone that gives you a dial tone first.

DTI - Digital Trunk Interface.

DTMF - Dual-Tone-Multi-Frequency, the generic term for the touch tone. These include 0,1,2,3,4,5,6,7,8,9 as well as A,B,C,D. See silver box for more details.

DVM - Data Voice Multiplexor. A system that squeezes more out of a transmission medium and allows a customer to transmit voice and data simultaneously to more than one receiver over the existing telefone line.

emergency break-in - Name given to the art of "breaking" into a busy number which will usually result in becoming a third party in the call taking place.

end office - Any class 5 switching office in North America.

end-to-end signalling - A mode of network operation in which the originating central office, or station, retains control and signals directly to each successive central office, or PBX, as trunks are added to the connection.

ESS - Electronic Switching System. "The phreak's nightmare come true." With ESS, EVERY SINGLE digit you dial is recorded, even mistakes. The system records who you call, when you call, how long you talked, and, in some cases, what you talked about. ESS is programed to make a list of people who make excessive 800 calls or directory assistance. This is called the "800 Exceptional Calling Report." ESS can be programed to print out logs of who called certain numbers, such as a bookie, a known communist, a BBS, etc. ESS is a series of programs working together; these programs can be very easily changed to do whatever the fone company wants ESS to do. With ESS, tracing is done in MILLISECONDS and will pick up any "foreign" tones on the line, such as 2600 Hz. Bell predicts the whole country will be on ESS by 1990! You can identify an ESS office by the functions, such as dialing 911 for help, fortress fones with DT first, special services such as call forwarding, speed dialing, call waiting, etc., and ANI on LD calls. Also, black boxes and Infinity transmitters will NOT work under ESS.

extender - A fone line that serves as a middleman for a fone call, such as the 800 or 950 extenders. These systems usually require a multi-digit code and have some sort of ANI to trace suspicious calls with.

facsimile - A system for the transmission of images. The image is scanned

at the transmitter, reconstructed at the receiving station, and duplicated on some form of paper. Also known as a FAX.

FAX - See facsimile for details.

FiRM - A large cracking group who is slowly taking the place of PTL and the endangered cracking groups at the time of this writing.

fortress phone - Today's modern, armor plated, pay fone. These may be the older, 3 coin/coin first fones or the newer, 1 coin/DT first fones. There are also others, see CF, DTF, and PP. Most phortresses can be found in the 9xxx or 98xx series of your local Nxx.

gateway city - See ISC.

Gestapo - The telefone company's security force. These nasties are the ones that stake out misused phortresses as well as go after those bad phreaks that might be phucking with the fone system.

green base - A type of output device used by the fone company. Usually light green in color and stick up a few feet from the ground. See output device for more information.

green box - Equipment that will emulate the Coin Collect, Coin Return, and Ringback tones. This means that if you call someone with a fortress fone and they have a green box, by activating it, your money will be returned. The tones are, in hertz, Coin Collect=700+1100, Coin Return=1100+1700, and Ringback=700+1700. However, before these tones are sent, the MF detectors at the CO must be alerted, this can be done by sending a 900+1500 Hz or single 2600 Hz wink of 90ms followed by a 60ms gap, and then the appropriate signal for at least 900ms.

gold box - This box will trace calls, tell if the call is being traced, and can change a trace.

grey box - Also known as a silver box. See silver box.

group chief - The name of the highest ranking official in any fone office. Ask to speak to these if an operator is giving you trouble.

high-speed data - A rate of data transfer ranging upward from 10,000 bits per second.

H/M - Hotel/Motel.

ICH - International Call Handling. Used for overseas calls.

ICVT - InComing Verification Trunk.

IDA - Integrated Digital Access. The United Kingdom's equivalent of ISDN.

IDDD - International Direct Distance Dialing - The ability to place international calls direct without processing through a station.

Usually, one would have to place the call through a 011, station, or a 01, operator assisted, type of setup.

IDN - Integrated Digital Networks. Networks which provide digital access and transmission, in both circuit switched and packet modes.

in-band - The method of sending signaling information along with the conversion using tones to represent digits.

INS - Information Network System. Japan's equivalent of ISDN.

Intercept - The intercept operator is the one you get connected to when there are not enough recordings available to tell you that the number has been disconnected or changed. These usually ask what number you are calling and are the lowest form of the operator.

intermediate point - Any class 4X switching office in North America. Also known as an RSU.

international dialing - In order to call across country borders, one must use the format PREFIX + COUNTRY CODE + NATION #. The prefix in North America is usually 011 for station-to-station calls or 01 for operator-assisted calls. If you have IDDD, you don't need to place this prefix in.

INTT - Incoming No Test Trunks.

INWARD - An operator that assists your local TSPS '0' operator in connecting calls. These won't question you as long as the call is within their service area. The operator can ONLY be reached by other operators or a blue box. The blue box number is KP+NPA+121+ST for the INWARD operator that will help you connect to any calls in that area ONLY.

INWATS - Inward Wide Area Telecommunications Service. These are the 800 numbers we are all familiar with. These are set up in bands; 6 total. Band 6 is the largest, and you can call band 6 INWATS from anywhere in the US except the state where the call is terminated. This is also why some companies have a separate 800 number for their state. Band 5 includes the 48 contiguous states. All the way down to band 1, which only includes the states contiguous to that one. Understand? That means more people can reach a band 6 INWATS as compared to the people that can access a band 1 INWATS.

IOCC - International Overseas Completion Centre. A system which must be dialed in order to re-route fone calls to countries inaccessible via dialing direct. To route a call via IOCC with a blue box, pad the country code to the RIGHT with zeroes until it is 3 digits. Then KP+160 is dialed, plus the padded country code, plus ST.

IPM - Interruptions Per Minute. The number of times a certain tone sounds during a minute.

ISC - Inter-Nation Switching Centers. Most outgoing calls from a certain numbering system will be routed through these "gateway cities" in

order to reach a foreign country.

ISDN - Integrated Services Digital Network. ISDN is a planned hierarchy of digital switching and transmission systems. Synchronized so that all digital elements speak the same "language" at the same speed, the ISDN would provide voice, data, and video in a unified manner.

ITT - This is another large LD service. The extenders owned by this company are usually considered dangerous. The format is ACC-ESS#, (NPA)Nxx-xxxx,1234567.

KP - Key Pulse. Tone that must be generated before inputting a fone number using a blue box. This tone is, in hertz, 1100+1700.

KP2 - Key Pulse 2. Tone that is used by the CCITT SYSTEM 5 for special international calling. This tone is, in hertz, 1300+1700.

LADT - Local Area Data Transport. LADT is a method by which customers will send and receive digital data over existing customer loop wiring. Dial-Up LADT will let customers use their lines for occasional data services; direct access LADT will transmit simultaneous voice and data traffic on the same line.

LAN - Local Area Network.

LAPB - Link Access Protocol Balanced.

LD - Long Distance

Leave Word And Call Back - Another new type of operator.

local loop - When a loop is connected between you and your CO. This occurs when you pick the fone up or have a fone OFF-HOOK.

loop - A pair or group of fone lines. When people call these lines, they can talk to each other. Loops consist of two or more numbers, they usually are grouped close together somewhere in the Nxx-99xx portions of your exchange. The lower number in a loop is the tone side of the loop, or the singing switch. The higher number is always silent. The tone disappears on the lower # when someone dials the other side of the loop. If you are the higher #, you will have to listen to the clicks to see if someone dialed into the loop. There also are such things as Non-Supervised loops, where the call is toll-free to the caller. Most loops will be muted or have annoying clicks at connection, but otherwise, you might find these useful goodies scanning the 99xx's in your exchange. Some loops allow multi-user capability; thus, many people can talk to each other at the same time, a conference of sorts. Since loops are genuine test functions for the telco during the day, most phreaks scan and use them at night.

MA - Ma Bell, the Bell Telesys Company. Telco, etc. See Ma Bell for more information.

Ma Bell - The telephone company. The Bell Telesys Phone Company. The company you phreak and hack with. The company that doesn't like you too much. The company you often phuck with, and sometimes phuck up. The company that can phuck u up if u aren't careful.

make period - The time when, during pulse dialing, the circuit is closed. In the US, this period is 60ms; however, foreign nations may use a 67ms make period. Make periods are also referred to in percentages, so a 60ms make period would be 60%, a 67ms as 67%.

marine verify - Another type of operator.

MCI - Yet another LD service that owns many dial-ups in most areas. However, the codes from various areas may not be interchangeable. Not much is known about MCI; however, MCI probably has some sophisticated anti-phreak equipment. The format is ACC-ESS#,12345, (NPA)Nxx-xxxx.

MCI Execunet - The calling card equivalent of the regular MCI LD service, but the codes are longer and interchangeable. For the local access port near you, call (800)555-1212. The format for the port will be ACC-ESS#,1234567,(NPA)Nxx-xxxx.

Metrofone - Owned by Western Union. A very popular system among fone phreaks. Call Metrofone's operator and ask for the local access number at (800)325-1403. The format is ACC-ESS#,CODE,(NPA)Nxx-xxxx. Metrofone is alleged to place trap codes on phreak BBS's.

MF - Multi-Frequency. These are the operator and blue box tones. An MF tone consists of two tones from a set of six master tones which are combined to produce 12 separate tones. These are NOT the same as touch tones. See blue box tones for frequencies.

mobile - A type of operator.

NAP/PA - North American Pirate/Phreak Association. A large group of bbs boards which include a lot of pirates/phreakers. I'm not quite sure where the group will go from here.

NON PUB DA - A reverse type of CN/A bureau. You tell the service the name and the locality, they will supply the fone number. However, they will ask for your name, supervisor's name, etc. Use your social engineering skills here (aka, bullshitting skills). You also can get detailed billing information from these bureaus.

NPA - Numbering Plan Area. The area code of a certain city/state. For example, on the number (111)222-3333, the NPA would be 111. Area codes never cross state boundaries sans the 800, 700, 900, and special exchanges.

Nxx - The exchange or prefix of the area to be dialed. For example of the number (111)222-3333, the Nxx would be 222.

OGVT - OutGoing Verification Trunk.

OFF-HOOK - To be on-line, to have the switchhook down. To have a closed connection. At this point, you also have a local loop.

ON-HOOK - To be off-line, to have the switchhook up. To have an open connection.

ONI - Operator Number Identification. Identifies calling numbers when an office is not equipped with CAMA, the calling number is not automatically recorded by CAMA, or has equipment failures, such as ANIF.

OPCR - Operator Actions Program. Standard TBOC or equivalent "0" operator.

OPEN - Northern Telecom's Open Protocol Enhanced Networks World Program.

OSI - Open System Interconnection. Form of telecommunication architechture which will probobly fail to SNA.

OST - Originating Station Treatment.

OTC - Operating Telefone Company.

out-of-band - Type of signaling which sends all of the signaling and supervisory informations, such as ON and OFF HOOK, over separate data links.

output device - Any type of interface such as cans, terminal sets, remote switching centers, bridging heads, etc., where the fone lines of the immediate area are relayed to before going to the fone company. These often are those cases painted light green and stand up from the ground. Most of these can be opened with a 7/16 hex driver, turning the security bolt(s)1/8 of an inch counter-clockwise, and opening. Terminals on the inside might be labeled "T" for tip and "R" for ring. Otherwise, the ring side is usually on the right and the tip side is on the left.

OUTWATS - Outward Wide Area Telecommunications Service. These are WATS that are used to make outgoing calls ONLY.

Paper Clip Method - This method of phreaking was illustrated in the movie War Games. What a phortress fone does to make sure money is in a fone is send an electrical pulse to notify the fone that a coin has been deposited, for the first coin only. However, by simply grounding the positive end of the microphone, enough current and voltage is deferred to the ground to simulate the first quarter in the coin box. An easy way to accomplish this is to connect the center of the mouthpiece to the coin box, touch tone pad, or anything that looks like metal with a piece of wire. A most convenient piece of wire is a bend out of a paper clip. Then you can send red box tones through the line and get free fone calls! Also, telco modified fones may require you to push the clip harder against the mouthpiece, or connect the mouthpiece to the earpiece. If pressing harder against the mouthpiece becomes a problem, pins may be an easier solution.

PBX - Private Branch eXchange. A private switchboard used by some big

companies that allow access to the OUTWATS line by dialing a 8 or a 9 after inputting a code.

PCM - Pulse Code-Modulated trunks.

PC Pursuit - A computer oriented LD system, comparable to Telenet, which offers low access rates to 2400 baud users. Hacking on this system is virtually impossible due to the new password format.

pen register - A device that the fone company puts on your line if they suspect you are fraudulently using your fone. This will record EVERY SINGLE digit/rotary pulse you enter into the fone as well as other pertinent information, which may include a bit of tapping. Also known as DNR.

Phortune 500 - An elite group of users currently paving the way for better quality in their trade.

PHRACK - Another phreak/hack oriented newsletter. See reference section, phile 1.6 for more information.

PHUN - Phreakers and Hackers Underground Network. They also release a newsletter that is up to #4 at the time of this writing. See phile 1.6 for more information on finding this phile.

PIN - Personal Identification Number - The last four digits on a calling card that adds to the security of calling cards.

plant tests - test numbers which include ANI, ringback, touch tone tests, and other tests the telco uses.

Post Office Engineers - The United Kingdom's fone workers.

PP - Dial Post-Pay Service. On phortress fones, you are prompted to pay for the call after the called party answers. You can use a clear box to get around this.

PPS - Pulses Per Second.

printmeter - The United Kingdom's equivalent of a pen register. See pen register for more info.

PTE - Packet Transport Equipment.

PTL - One of the bigger cracking groups of all time. However, the group has been dying off and only has a few nodes as of this writing.

PTS - Position and Trunk Scanner.

PTT - Postal Telephone Telegraph.

pulse - See rotary phones.

purple box - This one would be nice. Free calls to anywhere via blue boxing, become an operator via blue box, conference calling,

disconnect fone line(s), tap fones, detect traces, intercept directory assistance calls. Has all red box tones. This one may not be available under ESS.

rainbow box - An ultimate box. You can become an operator. You get free calls, blue box. You can set up conference calls. You can forcefully disconnect lines. You can tap lines. You can detect traces, change traces, and trace as well. All incoming calls are free. You can intercept directory assistance. You have a generator for all MF tones. You can mute and redial. You have all the red-box tones. This is an awesome box. However, it does not exist under ESS.

RAO - Revenue Accounting Office. The three digit code that sometimes replaces the NPA of some calling cards.

RBOC - Regional Bell Operating Company.

red box - Equipment that will emulate the red box tone generated for coin recognition in all phortress fones.

red box tones - Tones that tell the phortress fone how much money was inserted in the fone to make the required call. In one slot fones, these are beeps in pulses; the pulse is a 2200+1700 Hz tone. For quarters, 5 beep tones at 12-17 PPS, for dimes it is 2 beep tones at 5-8.5 PPS, and a nickel causes 1 beep tone at 5-8.5 PPS. For three slot fones, the tones are different. Instead of beeps, they are straight dual tones. For a nickel, it is one bell at 1050-1100 Hz, two bells for a dime, and one gong at 800 Hz for a quarter. When using red box tones, you must insert at least one nickel before playing the tones, cuz a ground test takes place to make sure some money has been inserted. The ground test may be fooled by the Paper Clip Method. Also, it has been known that TSPS can detect certain red box tones, and will record all data on AMA or CAMA of fraudulent activity.

regional center - Any class 1 switching office in North America.

REMOB - Method of tapping into lines by entering a code and the 7 digit number you want to monitor, from ACD Test Mode. A possibility of this may be mass conferencing.

ring - The red wire found in fone jacks and most fone equipment. The ring also is less positive than the tip. When looking at a fone plug on the end of typical 4 wire fone line from the top, let's say the top is the side with the hook, the ring will be the middle-right wire. Remember, the ring is red, and to the right. The three "R's" revived!

ring-around-the-rosy - 9 connections in tandem which would cause an endless loop connection and has never occurred in fone history.

ringback - A testing number that the fone company uses to have your fone ring back after you hang up. You usually input the three digit ringback number and then the last four digits to the fone number you are calling from.

ring trip - The CO process involved with stopping the AC ringing signal when a fone goes OFF-HOOK.

rotary phone - The dial or pulse phone that works by hooking and un-hooking the fone rapidly in secession that is directly related to the number you dialed. These will not work if another phone with the same number is off-hook at the time of dialing.

Rout & Rate - Yet another type of operator; assists your TSPS operator with rates and routings. This once can be reached at KP+800+141+1212+ST.

RPE - Remote Peripheral Equipment.

RQS - The Rate Quote System. This is the TSPS operator's rate/quote system. This is a method your '0' operator gets info without dialing the rate and route operator. The number is KP+009+ST.

RSU - Remote Switching Unit. The class 4X office that can have an unattended exchange attached to it.

RTA - Remote Trunk Arrangement.

SAC - Special Area Code. Separate listing of area codes, usually for special services such as TWX's, WATS, or DIAL-IT services.

SCC - Specialized Common Carriers. Common Nxx numbers that are specialized for a certain purpose. An example is the 950 exchange.

sectional center - Any class 2 switching office in North America.

service monitoring - This is the technical name of phone tapping.

SF - Supervision Control Frequency. The 2600 Hz tone which seizes any open trunk, which can be blue boxed off of.

short-haul - Also known as a local call.

signalling - The process by which a caller or equipment on the transmitting end of a line in: forms a particular party or equipment at the receiving end that a message is to be communicated. Signalling is also the supervisory information which lets the caller know the called know the called party is ready to talk, the line is busy, or the called party has hung up.

silver box - Equipment that will allow you to emulate the DTMF tones A,B,C,D. The MF tones are, in hertz, A=697+1633, B=770+1633, C=852+1633, D=941+1633. These allow special functions from regular fones, such as ACD Testing Mode.

Skyline - Service owned by IBM, Comsat, and AEtna. It has a local access number in the 950 exchange. The fone number is 950-1088. The code is either a 6 or 8 digit number. This company is alleged to be VERY dangerous.

SNA - System Network Architechture, by IBM. A possible future standard of architechture only competed by OSI.

SOST - Special Operator Service Treatment. These include calls which must be transferred to a SOST switchboard before they can be processed; services such as conferences, appointments, mobile, etc.

SPC - Stored Program Control. Form of switching the US has heavily invested in.

Sprint - One of the first LD services, also known as SPC. Sprint owns many extender services and is not considered safe. It is common knowledge that Sprint has declared war on fone phreakers.

SSAS - Station Signaling and Announcement System. System on most fortress fones that will prompt caller for money after the number, usually LD numbers, has been dialed, or the balance due before the call will be allowed to connect.

stacking tandems - The art of busying out all trunks between two points. This one is very amusing.

STart - Pulse that is transmitted after the KP+NPA+Nxx+xxxx through operator or blue boxed calls. This pulse is, in hertz, 1500+1700.

station # - The last four digits in any seven digit fone number.

STD - Subscriber Trunk Dialing. Mechanism in the United Kingdom which takes a call from the local lines and legimately elevates it to a trunk or international level.

step crashing - Method of using a rotary fone to break into a busy line. Example, you use a rotary fone to dial Nxx-xxx8 and you get a busy signal. Hang up and dial Nxx-xxx7 and in between the last pulse of your rotary dial and before the fone would begin to ring, you can flash your switchhook extremely fast. If you do it right, you will hear an enormous "CLICK" and all of a sudden, you will cut into your party's conversation.

STPS - Signal Transfer PointS. Associated with various switching machines and the new CCIS system.

switchhook - The button on your fone that, when depressed, hangs the fone up. These can be used to emulate rotary dial fones if used correctly.

SxS - Step-By-Step. Also known as the Strowger Switch or the two-motion switch. This is the switching equipment Bell began using in 1918. However, because of its limitations, such as no direct use of DTMF and maintenance problems, the fone company has been upgrading since. You can identify SxS switching offices by lack of DTMF or pulsing digits after dialing DTMF, if you go near the CO it will sound like a typewriter testing factory, lack of speed calling, lack of special services like call forwarding and call waiting, and fortress fones

want your money first, before the dial tone.

TAP - The "official" phone phreak's newsletter. Previously YIPL.

T&C - Time and Charge.

tapping - To listen in to a phone call taking place. The fone company calls this "service monitoring."

TASI - Time Assignment Speech Interpolation. This is used on satellite trunks, and basically allows more than one person to use a trunk by putting them on while the other person isn't talking.

Telenet - A computer-oriented system of relay stations which relay computer calls to LD numbers. Telenet has a vast array of access ports accessible at certain baud rates.

Tel-Tec - Another LD company that usually give out a weak connection. The format is (800)323-3026,123456,(NPA)Nxx-xxxx.

Tel-Tex - A subsidiary of Tel-Tec, but is only used in Texas. The number is *800)432-2071 and the format is the same as above.

terminal - A point where information may enter or leave a communication network. Also, any device that is capable of sending and/or receiving data over a communication channel.

tip - The green wire found in fone jacks and most fone equipment. The tip is the more positive wire compared to the ring. When looking at a fone plug from the top,lets say the hook side is the top, the tip will be the middle wire on the left.

toll center - Any class 4 switching office located in North America.

toll point - Any class 4P switching office in North America.

Toll LIB - Reverse CN/A bureau. See NON PUB DA for more info.

touch tone phone - A phone that uses the DTMF system to place calls.

touch tone test - This is another test number the fone company uses. You dial the ringback number and have the fone ring back. Then, when you pick it up, you will hear a tone. Press your touch-tone digits 1-0. If they are correct, the fone will beep twice.

trace - Something you don't want any fone company to do to you. This is when the fone company you are phucking with flips a switch and they find the number you are calling from. Sometimes the fone company will use ANI or trap and trace methods to locate you. Then the local Gestapo home in and terminate the caller if discovered.

trap and trace - A method used by the FBI and some step offices that forces a voltage through the line and traces simultaneously, which mean that you can't hang up unless the Pheds do, and pray you aren't calling from your own house. Trap and trace is also

known as the lock-in-trace.

trap codes - Working codes owned by the LD company, not a customer, that, when used, will send a "trouble card" to Ma Bell, no matter what company the card is coming from, and ESS will immediately trace the call. Trap codes have been in use for some time now, and it is considered safer to self-hack codes opposed to leeching them off of BBS's, since some LD companies post these codes on phreak oriented BBS's.

Travelnet - Service owned by GM that uses WATS as well as local access numbers. Travelnet also accepts voice validation for its LD codes.

TSPS - Traffic Service Position System. Operator that usually is the one that obtains billing information for Calling Card or 3rd number calls, identifies called customer on person-to-person calls, obtains acceptance of charges on collect calls, or identifies calling numbers. These operators have an ANI board and are the most dangerous type of operator.

TWX - Telex II consisting of 5 teletypewriter area codes. These are owned by Western Union. These may be reached via another TWX machine running at 110 baud. You can send TWX messages via Easylink (800)325-4122.

USDN - United States Digital Network. The US's version of the ISDN network.

videotext - Generic term for a class of two-way, interactive data distribution systems with output typically handled as in teletext systems and input typically accepted through the telephone or public data network.

WATS - Wide Area Telecommunications Service. These can be IN or OUT, see the appropriate sections.

WATS Extender - These are the LD companies everyone hacks and phreaks off of in the 800 NPA. Remember, INWATS + OUTWATS = WATS Extender.

white box - This is a portable DTMF keypad.

XBAR - Crossbar. Crossbar is another type of switching equipment the fone company uses in some areas. There are three major types of Crossbar systems called No.1 Crossbar (1XB), No.4 Crossbar (4XB), and No.5 Crossbar (5XB). 5XB has been the primary end office switch of MA since the 60's and is still in wide use. There is also Crossbar Tandem (XBT) used for toll-switching.

XBT - Crossbar Tandem. Used for toll-switching. See XBAR.

YIPL - The classic "official" phreak's magazine. Now TAP.

==========

Voltages & Technical Stuff

When your telephone is ON-HOOK, there is 48 volts of DC across the tip and the ring. When the handset of a fone is lifted a few switches close which cause a loop to become connected between you and the fone company, or OFF-HOOK. This is also known as the local loop. Once this happens, the DC current is able to flow through your fone with less resistance. This causes a relay to energize which causes other CO equipment to realize that you want service. Eventually, you will end up with a dial tone. This also causes the 48 VDC to drop down to around 12 VDC. The resistance of the loop also drops below the 2500 ohm level; FCC licensed telephone equipment must have an OFF-HOOK impedance of 600 ohms.

When your fone rings, the telco sends 90 volts of pulsing AC down the line at around 15-60 Hz, usually 20 Hz. In most cases, this causes a metal armature to be attracted alternately between two electromagnets; thus, the armature often ends up striking two bells of some sort, the ring you often hear when non-electronic fones receive a call. Today, these mechanical ringers can be replaced with more modern electronic bells and other annoying signaling devices, which also explains why deaf people can have lights and other equipment attached to their fones instead of ringers.

When you dial on a fone, there are two common types of dialing, pulse and DTMF. If you are like me, you probably don't like either and thought about using MF or blue box tones. Dialing rotary breaks and makes connections in the fone loop, and the telco uses this to signal to their equipment that you are placing a call. Since it is one fone that is disconnecting and reconnecting the fone line, if someone else picks up another fone on the same extension, both cannot make pulse fone calls until one hangs up. DTMF, on the other hand, is a more modern piece of equipment and relies on tones generated by a keypad, which can be characterized by a 0,1,2,3,4,5,6,7,8,9/A,B,C,D keypad. Most fones don't have an A,B,C,D keypad, for these frequencies are used by the telco for test and other purposes.

Scanning Phun Fone Stuff

Scanning is the act of either randomly or sequentially dialing fone numbers in a certain exchange when you are looking for several different things. These things could be carriers, extenders, ANI, "bug tracers," loops, as well as many other interesting "goodies" the fone company uses for test purposes.

When scanning for carriers, your local BBS probably has some scanning programs, as these became popular after the movie WARGAMES, but what these do are to call every fone in an exchange, or a specified range of fone numbers in certain exchanges to look for possible carriers and other interesting computer equipment. So, if your computer finds a carrier, or what seems like a carrier, it will either print it out or

save it in some file for later reference. With these carriers one finds, one can either call them and find out what each is or, if one of them is interesting, one can hack or attempt to break into some interesting systems available, not to the general public, of course.

Scanning telephone "goodies" requires time and patience. These goodies usually cannot be traced by most unmodified modems, as the frequencies and voice transmissions cannot be differentiated from other disturbances, such as the annoying operator saying, "We're sorry... blah blah..". Anyway, to scan these, you usually get a regular carrier scanner and, with the modem speaker on, sit by your wonderful computer and listen in on the scanning for any interesting tones, voices, or silences, which could be telco fone phun numbers, for us of course! Then write these down, and spread them around, use, abuze, etc. if you dare. Anyway, most telefone goodies are located in the 99xx suffixes of any fone exchange. If you found everything you think in the exchanges you have scanned, try the 0xxx and 1xxx suffixes in that order. You might even find loops, ANI, and other phun things if you mess around enough.

References & Suggested Reading

The following is a list of references and suggested reading for the beginning, as well as advanced phreak. See you local fone phreak for these, or call your local phreak oriented BBS for information regarding these publications.

2600 Magazine

Aqua Box, The
By Captain Xerox & The Traveler

Basic Alliance Teleconferencing
By The Trooper

Bell Hell
By The Dutchman & The Neon Knights

Better Homes And Blue Boxing
By Mark Tabas

BIOC Agent 003's Course In Basic Telecommunications
By BIOC Agent 003

History Of British Phreaking, The
By Lex Luthor & The Legion Of Doom

Home Phone Tips
By 13th Floor Enterprises

How To Build A Blotto Box
By The Traveler

How To Build A Cheese Box

By Mother Phucker

Introducing The Beige Box - Construction & Use
By The Exterminator and The Terminal Man

Integrated Services Digital Network [ISDN]
By Zander Zan

LOD/H Technical Journal

Loops I've Known And Loved
By Phred Phreak

PHRACK Magazine
Edited By Taran King and Knight Lightning UMCVMB

Phreakers And Hackers Underground Network [PHUN]
Edited By Red Knight
The Toll Center Bulletin Board System (718)358-9209

TAP - The Official Phreak Newsletter
Room 603
147 West 42nd Street
New York, NY 10036