The Black Notebook

Anyone's Guide To Phreaking And Shit
compiled by The Messiah
About This Project

Boxes:

Other Info:

If you get caught doing something you shouldn't with one of these boxes, you're on you're own. I assume **no** responsibility for your actions, nor would I want to.

tm@sinnerz.com
http://www.sinnerz.com
IRC- TM or TMessiah on UNDERNET

Big hello to everyone out there...

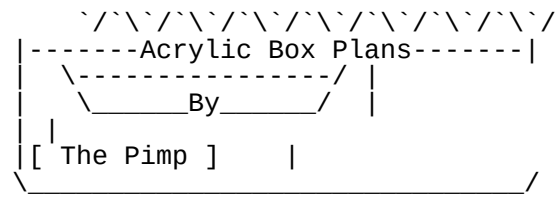
I've always wanted to make a big file full of phreaking info. You know, a nice, searchable index of all the boxes around and all the other stuff. So here it is, biatch...

I've tried to keep the files in their original condition, but some of them are all fucked up and stuff.

Some of these files are bound to be obsolete, incorrect, or simply fucked up, so I assume no responsibility for their accuracy, your actions, or my actions, for that matter.

The name comes from a friend of mine, who had this huge black notebook with all sorts of phreaking info in it. I thought that was a pretty nifty idea, so I thought I would make this digital one.

Any comments from me will look like this:
//This is a comment!



Call:
/\/\aharaja's Hi-Times

10 Meg BBS C/F 600+ G-Files
(xxx) - x x x - x x x x
A High Mtn. Hackers
Presentation

Ok the purpose of this box is to get Three-Way-Calling, Call Waiting, programmable Call Forwarding, and an easier way of extended Bud Boxing ALLfor FREE.

Materials:

1) Wire stripers
2) Couple Feet Wire
3) AT&T/BELL Can
4) Hex Wrench

Idea: Ok the idea of this box is to get all of the above features by stealing them from the fortunate ones on your block.

Procedure:

Step 1) Find AT&T/BELL Can that is being used to service you surrounding
area.

Step 2) Open can with Hex wrench.

Step 3) Find your line and another persons line who has 3-way, Call (waiting/forwarding), if the # of all the lines are not listed in the box you will have to use your local ANI to find them.

Step 4) Once you have found the lines then wire the (Black & Yellow) wires on the victims line to the (Black & Yellow) wires on you line (Be sure your phone at home uses all 4 wire as some of the cheap phones don't).

Step 5) Then disconnect the victims (Black & Yellow) Wires, resulting the the loss of these features to their line (you mat want to leave these wires connected, this may or may not cause problems I haven't tried it that may yet).

Well That Sums It Up!

Procedure for easier extended Bud Box.

If if for some reason your line is disconnected, or you just want to use hook someone's line to your line for fearless phreaking follow the procedure below.

Ok Go to the local can and find a line that is used by weekend visitors or a summer/winter home, and hook their (Red & Green) Wires to your (Red & Green) Wires, and your off into the fearless world of phreaking (i recommend you phreak from these line, so that the owners don't get uptight and look into the matter), unless of course you are doing it for revenge!

Some Suggestions:

Take a Bud box Along to do a ANI just to make sure you have the right line, also in some cases you will have to switch between the (Red/Green) (Black/Yellow) or any other combination if your area has changed the standard format which id very unlikely.

Have Fun

And Call /\/\aharaja's Hi-Times
10 Meg BBS C/F Line
600+ G-files

And I'm not responsible for your actions.
If you have any questions just call me at the BBS above.

Acrylic Box: Written & Created
By
[The Pimp]

```
 /-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/
  /-/   Building The Aqua Box   /-/
  /-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/
```

Every true phreaker lives in fear of the dreaded F.B.I. 'Lock in Trace.' For a long time, it was impossible to escape from the lock in trace. This box does offer an escape route with simple directions to it.This box is quite a simple concept, and almost any phreaker with basic electronics knowledge can construct and use it.

```
  /-/-/-/-/-/-/-/-/-/-/-/-/-/
  /-/    The Lock/-/
  /-/    in Trace/-/
  /-/-/-/-/-/-/-/-/-/-/-/-/-/
```

A lock in trace is a device used by the F.B.I. to lock into the phone users location so that he can not hang up while a trace is in progress. For those of you who are not familiar with the concept of 'locking in', then here's a brief description.

The F.B.I. can tap into a conversation, sort of like a three-way call connection. Then, when they get there, they can plug electricity into the phone line. All phone connections are held open by a certain voltage of electricity, that is why kou sometimes get static and faint connections when you are calling far away, because the electricity has trouble keeping the lineup. What the lock in trace does is cut into the line and generate that same voltage straight into the lines. That way, when you try and hang up, voltage is retained. Your phone will ring just like someone was calling you even after you hang up. (If you have call waiting, you should understand better about that, for call waiting intercepts the electricity and makes a tone that means someone is going through your line. Then, it is a matter of which voltage is higher. When you push down the receiver, then it see-saws the electricity to the other side. When you have a person on each line it is impossible to hang up unless one or both of them will hang up. If you try to hang up, voltage is retained, and your phone will ring. That should give you an understanding of how calling works, also. When electricity passes through a certain point on your phone, the electricity causes a bell to ring or on some newer phones an electronic ring to sound.)

So, in order to eliminate the trace, you somehow must lower the voltage level on your phone line. You should know that every time someone else picks up the phone line, then the voltage does decrease a little. In the first steps of planning this out, Xerox suggested getting about a hundred phones all hooked into the same line that could all be taken off the hook at the same time.That would greatly decrease the voltage level. That is also why most three-way connections that are using the bell service three

way calling (which is only $3 a month) become quite faint after a while.

By now, you should understand the basic idea. You have to drain all of the power out of the line so the voltage can not be kept up. A rather sudden draining of power could quickly short out the F.B.I. voltage machine, because it was only built to sustain the exact voltage necessary to keep the voltage out.

For now, image this. One of the normal radio shack generators that you can go pick up that one end of the cord that hooks into the central box has a phone jack on it and the other an electrical plug. This way, you can "flash" voltage THROUGH the line, but cannot drain it. So, some modifications have to be done.

/-/-/-/-/-/-/-/-/-/-/-/
/-/ The Aqua Box /-/
/-/-/-/-/-/-/-/-/-/-/-/

Materials needed-

- A BEOC (Basic Electrical Output Socket), like a small lamp type connection, where you just have a simple plug and wire that would plug into a light bulb.
- One of cords mentioned above, if you can't find one then construct your own... same voltage connection, but the restrain or must be the central box)
- TWO phone jacks (one for the modem, one for if you are being traced to plug the aqua box into)
- Some cdeativity and easy work.

NOTICE: No phones have to be destroyed/modified to make this box, so don't go out and buy a new phone for it!

All right, this is a very simple procedure. If you have the BEOC, it could drain into anything, a radio, or whatever. The purpose of having that is you are going to suck the voltage out from the phone line into the electrical appliance so there would be no voltage left to lock you in with.

1) Take the connection cord. Examine the plug at the end. It should have only two prongs, if it has three, still, do not fear. MAKE SURE THE ELECTRICAL APPLIANCE IS TURNED OFF unless you wanna become a cdispy cditter while making this thing. Most plugs will have a hard plastic design on the top of them to prevent you from getting in at the electrical wires inside. Well, get a knife and remove it. If you want to keep the plug (I don't see why...) then just cut the top off.

When you look inside, lo and behold, you will see that at the base of the prongs there are a few wires connecting in. Those wires conduct the power into the appliance. So, you carefully unwrap those from the sides and pull them out until they are about an inch ahead of the prongs. If you don't wanna keep the jack, then just rip the prongs out. If you cover the prongs with insulation tape so they will not connect with the wires when the power is being drained from the line.

2) Do the same thing with the prongs on the other plug, so you have the wires evenly connected. Now, wrap the end of the wires around each other.
If you happen to have the other end of the voltage cord hooked into the phonephonep 1 reading now, you're too fucking stupid to continue.

After you've wrapped the wires around each other, then cover the whole thing with the plugs with insulating tape. Then, if you built your own control box or if you bought one, then cdam all the wires into the and re-close it. That box is your ticket out of this.

3) Re-check everything to make sure it's all in place. This is a pretty flimsy connection, but on later models when you get more experienced at it then you can solder away at it and form the whole device into one big box, with some kind of cheap mattel hand-held game inside to be the power connector.

In order to use itl ofuld pkeep this box handy. Plug it into the jack if you want, but it will slightly lower the voltage so it isn't connected. When you plug it in, if you see sparks, un-plug it and restart the WHOLE thing. But if it just seems fine then leave it.

/-/-/-/-/-/-/-/-/-/
/-/ Using it !! /-/
/-/-/-/-/-/-/-/-/-/

Now, so you have the whole thing plugged in and all... DO NOT USE
THIS UNLESS THE SITUATION IS DESPERATE! When the trace has gone on, don't
panic, un plug your phone, and turn on the appliance that it was hooked
to. It will need energy to turn itself on, and here's a great source..
.
the voltage to keep a phone line open is pretty small and a simple light
bulb should drain it all in and probably short the F.B.I. computer at the
same time.

Happy boxing and stay free!
r

```
 /-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/
  /-/  /-/
  /-/ THE AQUA BOX    /-/
  /-/  /-/
  /-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/
  /-/  /-/
  /-/ CONCEPT BY: CAPTAIN XEROX /-/
  /-/  /-/
  /-/ PLANS BY: THE TRAVELER    /-/
  /-/  /-/
  /-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/
```

EVERY TRUE PHREAKER LIVES IN FEAR OF THE DREDDED F.B.I. 'LOCK IN TRACE.' FOR A LONG TIME, IT WAS IMPOSSIBLE TO ESCAPE FROM THE LOCK IN TRACE. THIS BOX DOES OFFER AND 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 BREIF 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. I 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, IMAGE THIS. ONE OF THE NORMAL RADIO SHACK GENERATORS THAT YOU CAN GO
PICK UP THAT ONE END OF THE CORD THAT HOOKS INTO THE CENTRAL BOX HAS A PHONE
JACK ON IT AND THE OTHER HAS AN ELECTRICAL PLUG. THIS WAY, YOU CAN "FLASH"
VOLTAGE THROUGH THE LINE, BUT CANNOT DRAIN IT. SO, SOME MODIFICATIONS HAVE
TO BE DONE.

```
/-/-/-/-/-/-/-/-/-/-/-/-/
/-/   THE AQUA BOX  /-/
/-/-/-/-/-/-/-/-/-/-/-/-/
```

MATERIALS NEEDED- A BEOC (BASIC ELECTRICAL OUTPUT SOCKET), LIKE A SMALL LAMP
TYPE CONNECTION, WHERE YOU JUST HAVE A SIMPLE PLUG AND WIRE
THAT WOULD PLUG INTO A LIGHT BULB.
- ONE OF CORDS MENTIONED ABOVE, IF YOU CAN'T FIND ONE THEN
CONSTRUCT YOUR OWN... SAME VOLTAGE CONNECTION, BUT THE
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!

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
APPLICENCE 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 APPLIENCE IS TURNED OFF UNLESS YOU WANNA BECOME A CRISPY CRITTER WHILE MAKING THIS THING. MOST PLUG WILL HAVE A HARD PLASTIC DESIGN ON THE TOP OF THEM TO PREVENT YOU FROM GETTING IN AT THE ELECTRICAL WIRES INSIDE. WELL, GET A NICE AND REMOVE IT. IF YOU WANT TO KEEP THE PLUG (I DON'T SEE WHY...) THEN JUST CUT THE TOP OFF.

WHEN YOU LOOK INSIDE, LOW 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 AND INCH AHEAD OF THE PRONGS. IF YOU WDON'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, YOUR TOO FUCKING STUPID TO CONTINUE.

AFTER YOU'VE WRAPPED THE WIRES AROUND EAHC 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 THE 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 SAUDER AWAY AT IT AND FORM THE WHOLE DEVICE INTO ONE BIG BOX, WITH SOME KIND OF CHEAP MATTEL HAND-HELD GAME INSUkjsoida.

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.

/-/-/-/-/-/-/-/-/-/
/-/ USING IT !! /-/
/-/-/-/-/-/-/-/-/-/

NOW, SO YOU HAVE THE WHOLE THING PLUGGED IN AND ALL... DO NOT USE THIS UNLESS THE SITUATION IS DESPERATE! WHEN THE TRACE HAS GONE ON, DON'T PANIC, UNPLUG YOUR PHONE, AND TURN ON THE APPLIANCE THAT IT WAS HOOKED TO. IT WILL NEED

ENERGY TO TURN ITSELF ON, AND HERE'S A GREAT SOURCE... THE VOLTAGE TO KEEP
A PHONE LINE OPEN IS PRETTY SMALL AND A SIMPLE LIGHT BULB SHOULD DRAIN IT ALL
IN AND PROBABLY SHORT THE F.B.I. COMPUTER AT THE SAME TIME.

HAPPY BOXING AND STAY FREE!

LATER,
KOPY KAT

CALL THESE BBS:

```
 /------------------------------\
 |LITTLE AMERICA   (xxx)xxx-xxxx|
 |BRAINSTORM  (xxx)xxx-xxxx|
 |ROGUES GALLERY   (xxx)xxx-xxxx|
 |APPLE ENTERTAIN  (xxx)xxx-xxxx|
 |CITY OF ATLANTIS (xxx)xxx-xxxx|
 |KING'S LAIR (xxx)xxx-xxxx|
 \------------------------------/
```

/\/\/\\/\/\/\/\uploaded by Dos Ranger/\/\/\/\/\/\/\//\/\

```
 /-/-/-/-/-/-\-\-\-\-\-\
 <:-\-Biege Box Plans-/-:>
  \-\-\-\-\-\-/-/-/-/-/-/
```

(>Introduction

Have you ever wanted a lineman's handset? Surely every phreak has at least once considered the phun that he could have with one. After searching unlocked phone company trucks for one for months, we had an idea. We could build one. We did, and named it the "Beige Box, " simply because that is the color of ours. In the following file we will give complete instructions for the construction and use of a Beige Box.

(>Construction

The construction is very simple. First, you must understand the concept of the device. In a modular jack, there are four wires. These are red, green, yellow, and black. For a single line telephone, however, only two matter: the red (ring) and green (tip). The yellow and black are not necessary for this project. A lineman's handset only has two clips on it: the ring and the tip.

You will need a phone (we reccommend a touch-tone) with a modular plug, a modular jack, and two large alligator clips (preferably red and green, respectively). Take the modular jack and look at the bottom of its casing. There should be a grey jack with four wires (red, green, yellow, and black) leading out of it. To the end of the red wire attach a red alligator clip. To the end of the green wire attach a green alligator clip. The yellow and black wires can be removed, although I would only set them aside so that you can use the modular jack in future projects. Now insert your telephone's modular plug into the modular jack. That's it.

This particular model is nice because it can be easily made, is inexpensive, uses common parts that are readily available, is small, is lightweight, and does not require the destruction of a phone.

(>Uses

There are many uses for the Beige Box. However, before you can use it, you must know how to attach it to its output device. This device can be any of several Bell switching apparatus that include terminal sets (i.e., remote switching centers, bridging heads, cans, etc.). To open most Bell Telephone switching apparatus, you must have a 7/16 inch hex driver. This piece of equipment can be picked up at your local hardware store. With your 7/16 hex driver, turn the security bolt(s) approximately 1/8 of an inch counter-clockwise and open. If your output device is locked, then you must have some knowledge of destroying and/or picking locks. However, we have never encountered a locked output device. Once you have opened your output device, you should see a mass of wires connected to terminals. On most of your output devices, the terminals should be labeled "T" (Tip -- if not labeled, it is usually on the left) and "R" (Ring -- if not labeled, it is usually on the right). Remember: Ring - red - right. The "Three R's" -- a simple way to remember which is which.

Now you must attach the red alligator clip (ring) to the "R" (ring) terminal. Attach the green alliagtor clip (tip) to the "T" (tip) terminal. NOTE: If instead of a dial tone you hear nothing, re-adjust the alligator clips so that they are not touching each other

or other terminals. Also make sure that they are firmly attached. By this time you should hear a dial tone. Dial ANI and find out the number that you are using (you wouldn't want to use your own).

Here are some practical applications:

- Eavesdropping
- Long distance, static-free phone calls to phriends
- Dialing direct to Alliance Conferencing (also static-free)
- Phucking people over
- Bothering the operator at little risk to yourself
- Blue Boxing with a greatly reduced chance of getting caught
- Anything at all that you want, since you are an extension on that line

<>Eavesdropping:

To be most effective, first attach the Beige Box and then your phone. This eliminates static caused by connecting the box, therefore reducing the potential suspicion of your victim. When eavesdropping, it is always best to be neither seen nor heard. If you hear someone dialing out, do not panic; but rather hang up, wait, and pick up the receiver again. The person will either have hung up or tried to complete their call again. If the latter is true, then listen in, and perhaps you will find information worthy of blackmail! If you would like to know who you are listening to, after dialing ANI, pull a CN/A on the number.

<>Dialing Long Distance:

This section is self-explanatory, but don't forget to dial a "1" before the NPA.

<>Dialing Direct to Alliance Conferencing:

Simply dial 0-700-456-1000 and you will get instructions from there. I prefer this method over PBXs, since PBXs often have poor reception and are more difficult to come by.

<>Phucking People Over:

This is a very large topic for discussion. Just by using the other functions described, you can create a large phone bill for the person (they will not have to pay it, but it is a hassle for them). In addition, since you are an extension of the person's line, leave your phone off hook, and they will not be able to make or recieve calls. This can be extremely nasty because no one would suspect the cause of the problem.

<>Bothering the Operator:

This is also self-explanatory and can provide hours of entertainment. Simply ask or say things to her that are offensive and you would not like traced to your line. This also corresponds with the previous described section, Phucking People Over. After all, guess who's line it gets traced to? He he he...

<>Blue Boxing:

See a file on Blue Boxing for more details. This is an especially nice feature if you live in an ESS-equipped prefix, since the calls are, once again, not traced to your line.

(>Potential Risks

Overuse of the Beige Box may cause suspicions within the Gestapo, and result in legal problems. Therefore, I would recommend that you:

- Use more than one output device
- Choose a secluded spot to do your Beige Boxing
- Keep a low profile (i.e., do not post under your real name on a public BBS concerning your accomplishments)
- In order to make sure that the enemy has not been inside your ouput device, I reccomend that you place a piece of transparent tape over the opening of your output device. Therefore, if it is opened in your absence, the tape will be displaced and you will be aware of the fact that someone has been intruding upon your territory.

THE BEIGE BOX

A beige box is an easy way of tapping into phone lines. It is basically an adaptor for connecting a normal phone with a BT plug onto a pair of phone wires.

You will need: one cheap phone, two crocodile clips, some wire and a telephone socket and wallbox. If you use a master (primary) socket your phone will be able to ring; if you just use a secondary (slave) socket, it will never ring. {but see below.}

HOW TO MAKE IT

Solder the crocodile clips onto each end of half a metre of wire. Cut the wire and pass it through a convenient knockout in the socket wallbox, so that the clips are on the outside. Connect one wire to pin 2 of the phone socket, and one to pin 5 of the phone socket. {it is easier if your socket has screw terminals rather than IDC terminals, especially if your wire is stranded.} Screw the socket onto the wallbox and plug in the phone. That's it.

HOW TO USE IT

Clip the clips onto the two wires of a phone line, and dial away. That's all you have to do.

IDEAS FOR IMPROVEMENTS

1. If you used a secondary socket but later decide you would rather have a primary socket, simply add a 1.8uF 100V capacitor in the position marked C1 on the PCB inside the socket. {1.5uF or 2.2uF will do the job, if you can't get 1.8uF, but it must NOT be an electrolytic capacitor, and it MUST be rated 100V or over.} If you are using a slimline socket without a PCB, the capacitor should be wired between pins 2 and 3.

2. If you want a line status indicator: get a two-colour LED {the type with two leads, that glows red when the current is in one direction and green in the other} and a 6.8k resistor. Wire these, in series, across the position marked SP1 on the PCB. {don't connect the middle of the series pair to anywhere.} For PCB-less sockets, this is the equivalent of pins 2 and 5, ie the pair connected to the clips. It will indicate the line polarity {red or green} which is not particularly important, and the line status {dim = in use, bright = clear} which is.

Brought to you by ....
: :..: :.. :.' .:.....:.
: : : :... : `. `... .:...

Original idea by Jolly Roger, modified by THE KEZ for the UK.

disclaimer: this is for informational purposes only. no responsibility
is accepted for any consequences of use or misuse of any information
contained herein. any material whose source i have not acknowledged is
believed to be my own - if it sounds like something you invented, just
remember great minds think alike.
K

```
   Introducing the:    !
B B B B BBEEEEEEEEEE   IIIIIIIIIIII    GGGGGGGGG  EEEEEEEEE  !
B    B    E   I    G E !
BB   E   I    G E !
B B B B B B    EEEEEEEEEI    G EEEEEEEEE  !
BB   E   I    G   GGGGG   E !
B B  E   I    G   G  E !
BBBBBBBBBBB   EEEEEEEEE   IIIIIIIIIIII    GGGGGGGGG  EEEEEEEEE  !
   !
 B !
  O    - Construction and Use -  !
   X    Invented and Written by: !
The Exterminator and The Terminal Man !
_____________________________________________________________________!
```

Introduction

Have you ever wanted a lineman's handset? Surely every phreak has at least once considered the phun that he could have with one. After searching unlocked phone company trucks for months, we had an idea. We could build one. We did, and named it the "Beige Box" simply because that is the color of ours. In the following file we will give the construction and use of a Beige Box.

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 attar plug into the modular jack. That's it. This particular model is nice because it is can be easily made, is inexpensive, usues 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)

aproximately 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
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:

- o Eavesdropping
- o Long distance, static free free fone calls to phriends
- o Dialing direct to Alliance Telec Code scan: to 999999

BLACK BOX PLANS

HERE IS HOW YOU CONSTRUCT A BLACK BOX.

WHEN YOUR PHONE IS JUST SITTING THERE DOING NOTHING THE VOLTAGE THROUGH THE PHONE LINE IS ZERO. THEN IF SOMEONE CALLS YOU (FOR SOME STRANGE REASON) AND THE PHONE IS RINGING. THE VOLTAGE JUMPS TO 48 VOLTS WHICH TELLS MA BELL TO STAND BY IF YOU SHOULD PICK UP SO SHE CAN BILL YOU. WHEN YOU EVENTUALLY PICK UP THE PHONE, THE VOLTAGE DROPS TO 10 VOLTS AND THE BILLING STARTS. WHAT A BLACK BOX DOES IS KEEPS THE THE VOLTAGE AS 36 VOLTS, THEREFORE THE INCOMING CALLER NEVER GETS BILLED (INGEINIOUS)

THE ORIGINAL BLACK BOX WAS CREATED BY AN EX-BELL EMPLOYEE WHO WENT BY THE NAME "CAPTAIN CRUNCH". HE GOT HIS NAME FROM THOSE LITTLE WHISLES YOU GOT IN BOXES OF CAPTAIN CRUNCH BECAUSE THEY EMITED A TONE THAT WAS EQUAL TO A COIN.CAPTAIN CRUNCH JUST ANNOUNCED HIS RETIREMENT FROM PHREAKING WHEN HE WAS RELEASED FROM A CALIFORNIA JAIL. HE WAS CAUGHT WITH A BLUE BOX.

CONSTRUCTION OF A
BLACK BOX

1] A 36 VOLT ZENER DIODE.
2] A CERAMIC OR MYLAR CAPACITOR OF 0.1 MICROFARAD.
3] A ELECTROLYTIC CAPACITOR OF 1.0 MICROFARAD.

YOU CAN GET THESE AT YOUR LOCAL RADIO SHACK DEALER.

FIRST YOU HAVE TO OPEN UP YOUR PHONE.YOU SHOULD NOTICE THREE WIRES COMING IN FROM THE BACK OF THE PHONE, A GREEN, RED, AND YELLOW. MOST OF THE TIME THEY CAN DIFFER.DON'T WORRY ABOUT THE YELLOW WIRE, WE WILL NOT BE USING THIS.YOU WILL NEED TO FIND THE MOST POSITIVE OF THE REMAINING TWO WIRES.(ALMOST ALWAYS THE GREEN WIRE). NOW CONNECT THE BANDED END OF THE ZENER DIODE TO THE MORE POSITIVE OF THESE TWO WIRES. "IN SERIES". YOU HAVE JUST COMPLETED THE FIRST STEP. FOR THE SECOND STEP YOU NEED A CERAMIC OR MYLAR CAPACITOR OF 0.1 MICROFARAD. YOU CONNECT THIS "IN PARRALLEL" ACROSS THE DIODE. THIS IS NEEDED TO ALLOW THE DIODE TO PASS VOICE SIGNALS. NOW FOR THE FINAL STEP TAKE YOUR ELECTROLYTIC CAPACITOR OF UP TO ONE MICROFARAD WITH ITS '+' END CONNECTED TO THE BANDED END OF THE DIODE AND THE OTHER END SHOULD BE CONNECTED TO THE ANODE END OF THE DIODE. MA BELL IS NOT TOTALLY OBLIVIOUS TO THIS.IF THE PHONE RINGS FOR ABOUT A HALF-HOUR THEY WILL THINK SOMETHING IS WRONG AND BILL YOU ANYWAY. WHEN USING A BLACK BOX,YOUR PHONE WILL CONTINUE RING EVEN THOUGH YOU PICKED IT UP. YOU HAVE TO MAKE A SWITCH TO CONNECT ONE OF THE RINGER WIRES.THAT WILL SHUT IT OFF. THAT'S IT! HAVE PHUN!!!!!!!!!!!!!!!!
<><><><><><><><><><><><><><><><><><><><><><><><><><<><>

p

FROM: THE PIRATE CLUB/1200

EDITED BY: CRACKER JACK

```
************************************
*  *
* HOW TO BUILD A BLACK BOX  *
*  *
************************************
```

TO ALL WHO DARE --

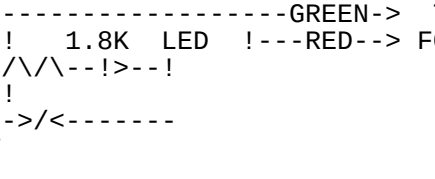
WHAT IS A BLACK BOX? A BLACK BOX IS A DEVICE THAT IS HOOKED UP TO YOUR FONE THAT FIXES YOUR FONE SO THAT WHEN YOU GET A CALL, THE CALLER DOESN'T GET CHARGED FOR THE CALL. THIS IS GOOD FOR CALLS UP TO 1/2 HOUR, AFTER 1/2 HOUR THE FONE CO. GETS SUSPICIOUS, AND THEN YOU CAN GUESS WHAT HAPPENS.

THE WAY IT WORKS:

WHAT THIS LITTLE BEAUTY DOES IS KEEP THE LINE VOLTAGE FROM DROPPING TO 10V WHEN YOU ANSWER YOUR FONE. THE LINE IS INSTED KEPT AT 36V AND IT WILL MAKE THE FONE THINK THAT IT IS STILL RINGING WHILE YOUR TALKING. THE REASON FOR THE 1/2 HOUR TIME LIMIT IS THAT THE FONE CO. THINKS THAT SOMETHING IS WRONG AFTER 1/2 AN HOUR OF RINGING.

ALL PARTS ARE AVAILABLE RADIO SHACK. USING THE LEAST POSSIBLE PARTS AND ARANGEMENT, THE COST IS $0.98 !!!! AND THAT IS PARTS FOR TWO OF THEM! TALK ABOUT A DEAL! IF YOU WANT TO SPLURGE THEN YOU CAN GET A SMALL PC BOARD, AND A SWITCH. THERE ARE TWO SCHEMATICS FOR THIS BOX, ONE IS FOR MOST NORMAL FONES. THE SECOND ONE IS FOR FONES THAT DON'T WORK WITH THE FIRST. IT WAS MADE FOR USE WITH A BELL TRIMLINE TOUCH TONE FONE.

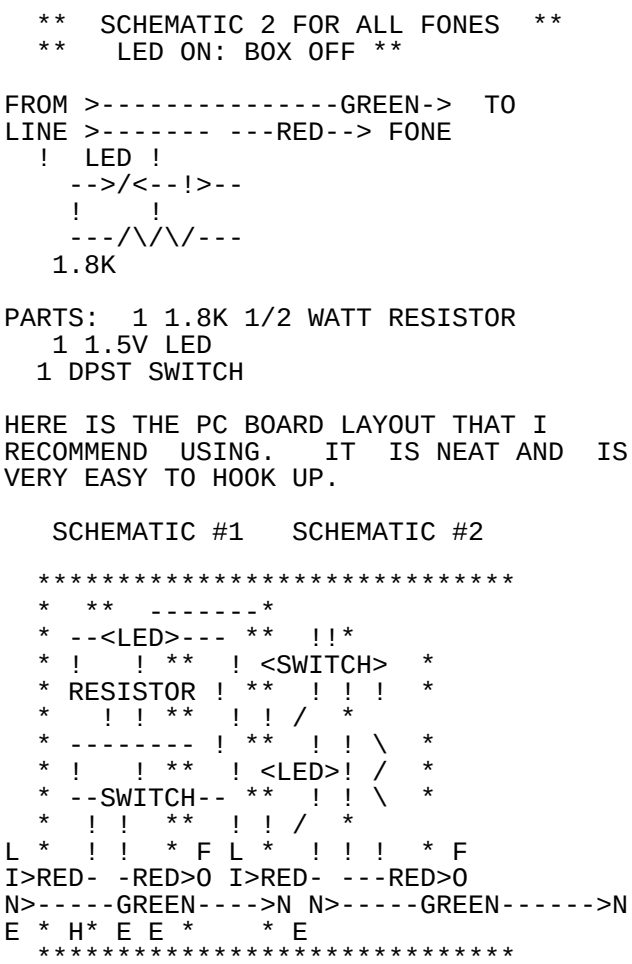
```
  **  SCHEMATIC 1 FOR MOST FONES  **
  **    LED ON: BOX ON  **
```



PARTS: 1 1.8K 1/2 WATT RESISTOR
1 1.5V LED
1 SPST SWITCH

YOU MAY JUST HAVE TWO WIRES WHICH YOU

CONNECT TOGETHER FOR THE SWITCH.



PARTS: 1 1.8K 1/2 WATT RESISTOR
1 1.5V LED
1 DPST SWITCH

HERE IS THE PC BOARD LAYOUT THAT I RECOMMEND USING. IT IS NEAT AND IS VERY EASY TO HOOK UP.

SCHEMATIC #1 SCHEMATIC #2

ONCE YOU HAVE HOOKED UP ALL THE PARTS, YOU MUST FIGURE OUT WHAT SET OF WIRES GO TO THE LINE AND WHICH GO TO THE FONE. THIS IS BECAUSE OF THE FACT THAT LED'S MUST BE PUT IN, IN A CERTAIN DIRECTION. DEPENDING ON WHICH WAY YOU PUT THE LED IS WHAT CONTROLS WHAT WIRES ARE FOR THE LINE & FONE.

HOW TO FIND OUT:

HOOK UP THE BOX IN ONE DIRECTION USING ONE SET OF WIRES FOR LINE AND THE OTHER FOR FONE.

NOTE FOR MODEL I SWITCH SHOULD BE OFF.
NOTE FOR MODEL][SWITCH SHOULD BE SET TO SIDE CONNECTING THE LED.

ONCE YOU HAVE HOOKED IT UP, THEN PICK UP THE FONE AND SEE IF THE LED IS ON. IF IT IS, THE LED WILL BE LIT. IF

IS DOESN'T LIGHT THEN SWITCH THE WIRES AND TRY AGAIN. ONCE YOU KNOW WHICH ARE WHICH THEN LABEL THEM. *NOTE* - IF NEITHER DIRECTIONS WORKED THEN YOUR SWITCH WAS IN THE WRONG POSITION. NOW LABLE THE SWITCH IN ITS CURRENT POSITION AS BOX ON.

HOW TO USE IT:

THE PURPOSE OF THIS BOX IS NOT TO POEPLE WHO CALL YOU SO IT WOULD MAKE SENCE THAT IT CAN ONLY BE USED TO RECEIVE! CALLS. WHEN THE BOX IS *ON* THEN YOU MAY ONLY RECIEVE CALLS. YOUR FONE WILL RING LIKE NORMAL AND THE LED ON THE BOX WILL FLASH. IF YOU ANSWER THE FONE NOW, THEN THE LED WILL LIGHT AND THE CALLER WILL NOT BE CHARGE D.
HANG UP THE FONE AFTER YOU ARE DONE TALKING LIKE NORMAL. YOU WILL NOT BE ABLE TO GET A DIAL-TONE OR CALL WHEN THE BOX IS ON, SO TURN THE BOX *OFF* FOR NORMAL CALLS. I DON'T RECOMMEND THAT YOU LEAVE IT ON ALL THE TIME, AS YOU DON'T WANT IT TO ANSWER WHEN MA BELL CALLS!

```
 /-/-/-/-/-/-\-\-\-\-\-\
 <:-\-Black Box Plans-/-:>
  \-\-\-\-\-\-/-/-/-/-/-/
```

(>Introduction<)

What is a BLACK BOX? A BLACK BOX is a device that is hooked up to your phone that fixes your phone so that when you get a call, the caller doesn't get charged for the call. This is good for calls up to 1/2 hour, after 1/2 hour the Gestapo (the you can guess what happens.

What this little beauty does is keep the line voltage from dropping to 10v when you answer your phone. The line is insted kept at 36v and it will make the phone think that it is still ringing while your talking. The reason for the 1/2 hour time limit is that the Gestapo thinks that something is wrong after 1/2 an hour of ringing. (I mean, come on)

(>Phone Modification Instructions<)

All parts are available Radio Shack. Using the least possible parts and arrangement, the cost is $0.98; and that is parts for two of them! Talk about a deal! If you want to splurge then you can get a board, and a switch. There are two s

** Schematic 1 for most fones **
**   LED ON: BOX ON **

```
FROM >--------------------GREEN->  TO
LINE >--!   1.8k  LED  !---RED--> FONE
   !--/\/\/\--!>--!
   !    !
   ------>/<-------
   SPST
```

Parts: 1 1.8k 1/2 watt resistor
1 1.5v LED
1 SPST switch

*You may just have two wires which you connect together for the switch.

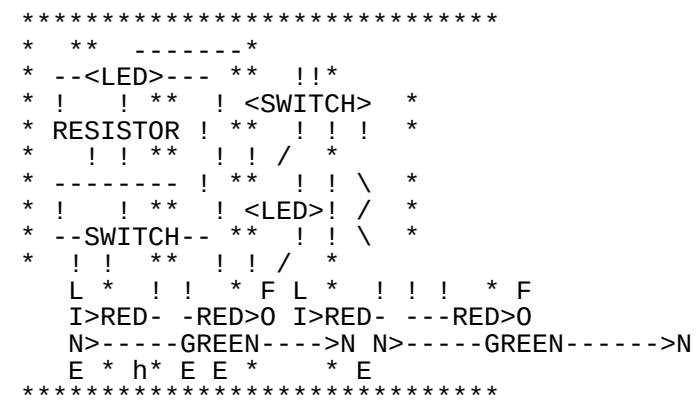
** Schematic 2 for all fones **
**   LED ON: BOX OFF **

```
 FROM >---------------GREEN->  TO
 LINE >------- ---RED--> FONE
   !  LED !
 ---->/<--!>--
 !    !
 ---/\/\/---
    1.8k
```

Parts: 1 1.8k 1/2 watt resistor
1 1.5v LED
1 DPST switch

Here is the PC board layout that I recommend using. It is neat and is very easy to hook up:

Schematic #1 Schematic #2



Once you have hooked up all the parts, you must figure out what set of wires go to the line and which go to the fone. This is because of the fact that LED's must be put in, in a certain direction. Depending on which way you put the LED is what controls what wires are for the line & fone.

In order to find out, hook up the box in one direction using one set of wires for line and the other for phone.

NOTE For Model I switch should be OFF.
NOTE For Model][switch should be set to side connecting the LED.

Once you have hooked it up, then pick up the fone and see if the LED is on. If it is, the LED will be lit. If is doesn't light then switch the wires and try again. Once you know which are which then label them. *NOTE* - If neither directions worked then your switch was in the wrong position. Now lable the switch in its current position as BOX ON.

(>Black Box Usage<)

The purpose of this box is not to people who call you so it would make sense that it can only be used to recieve calls. When the box is *ON* then you may only recieve calls. Your phone will ring like normal and the LED light on the box will flash. When you answer the fone the LED will light and the caller will not be charged. Hang up the fone after you are done like normal. You will not be ab

//TM sez: this one is incomplete. Sorry, gang.

```
************************************
*  *
* How to build a BLACK BOX  *
*  *
************************************
```

To all who dare --

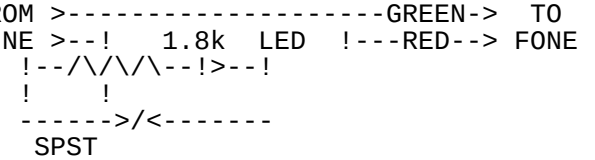
What is a BLACK BOX? A BLACK BOX is a device that is hooked up to your fone that fixes your fone so that when you get a call, the caller doesn't get charged for the call. This is good for calls up to 1/2 hour, after 1/2 hour the Fone Co. gets suspicious, and then you can guess what happens.

The way it works:

What this little beauty does is keep the line voltage from dropping to 10v when you answer your fone. The line is insted kept at 36v and it will make the fone think that it is still ringing while your talking. The reason for the 1/2 hour time limit is that the Fone CO. thinks that something is wrong after 1/2 an hour of ringing.

All parts are available Radio Shack. Using the least possible parts and arangement, the cost is $0.98 !!!! And that is parts for two of them! Talk about a deal! If you want to splurge then you can get a small PC board, and a switch. There are two schematics for this box, one is for most normal fones. The second one is for fones that don't work with the first. It was made for use with a Bell Trimline touch tone fone.

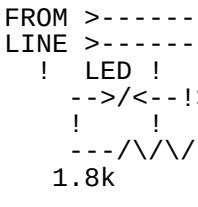
** Schematic 1 for most fones **
** LED ON: BOX ON **



Parts: 1 1.8k 1/2 watt resistor
1 1.5v LED
1 SPST switch

You may just have two wires which you connect together for the switch.

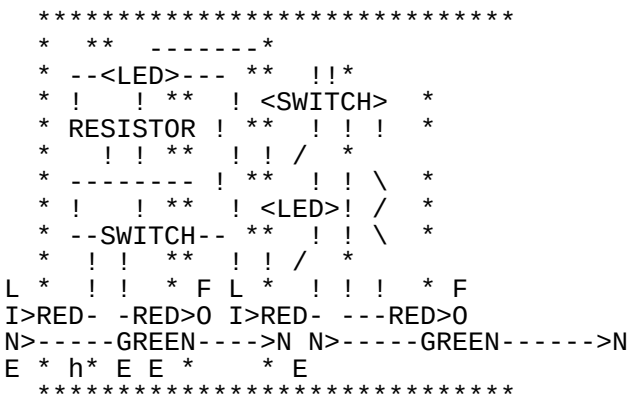
** Schematic 2 for all fones **
** LED ON: BOX OFF **



Parts: 1 1.8k 1/2 watt resistor
1 1.5v LED
1 DPST switch

Here is the PC board layout that I recommend using. It is neat and is very easy to hook up.

Schematic #1 Schematic #2



Once you have hooked up all the parts, you must figure out what set of wires go to the line and which go to the fone. This is because of the fact that LED's must be put in, in a certain direction. Depending on which way you put the LED is what controls what wires are for the line & fone.

How to find out:

Hook up the box in one direction using one set of wires for line and the other for fone.

NOTE For Model I switch should be OFF.
NOTE For Model][switch should be set to side connecting the led.

Once you have hooked it up, then pick up the fone and see if the LED is on. If it is, the LED will be lit. If is doesn't light then switch the wires and try again. Once you know which are which then label them. *NOTE* - If neither directions worked then your switch was in the wrong position. Now

lable the switch in its current position as BOX ON.

How to use it:

The purpose of this box is not to poeple who call you so it would make sence that it can only be used to receive! calls. When the box is *ON* then you may only recieve calls. Your fone will ring like normal and the LED on the box will flash. If you answer the fone now, then the LED will light and the caller will not be charged. Hang up the fone after you are done talking like normal. You will not be able to get a dial-tone or call when the box is on, so turn the box *OFF* for normal calls. I don't recommend that you leave it on all the time, as you don't want it to answer when Ma Bell calls!

from Plover-Net
(xxx) xxx-xxxx

```
 [=-================================-=]
  [=-=]   Presenting:[=-=]
  [=-=] The !BLAST! Box   [=-=]
  [=-=]An *ORIGINAL* Box, [=-=]
  [=-=]  Designed And Invented By   [=-=]
  [=-=]    (_> Shadow Hawk 1<_)[=-=]
  [=-================================-=]
  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 theese 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 espicially good for PBS
Subscription
  drives.

  Have Phun, and don't get caught!

  (_> Shadow Hawk 1 <_)
```

%+%+%+%+%+%+%+%+%+%+%+%+%+%+%
%HOW TO BUILD A BLOTO BOX+
%+%+%+%+%+%+%+%+%+%+%+%+%+%+%

Finally, it is here! What was first conceived as a joke to fool the inncoent phreakers around America has finally been concieved by the one phreak who is the expert on lines and voltage: The Traveler. Other boxes by the Traveler include the White Gold Box, the Aqua Box, The Diverti Box, and the Cold Box.
All of those plans will soon be available in a BBS/AE near you!

Well, for you people who are unenlightened about the Blotto Box, here is a brief summery of a legend.

--*-=> The Blotto Box <=-*--

For years now every pirate has dreamed of the Blotto Box. It was at first made as a joke to mock more ignorant people into thinking that the function of it actually was possible. Well, if you are The Voltage Master, it is possible. Originally conceived by King Blotto of much fame, the Blotto Box is finally available to the public.

NOTE: The Traveler can not be responcable 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!

All right, now that that is cleared up, here is the basis of the box and it's function.
The Blotto Box is every phreaks dream... you could hold AT&T down on it's knee's with this device. Because, quite simply, it can turn off the phone lines everywhere. Nothing. Blotto. No calls will be allowed out of an area code, and no calls will be allowed in. No calls can be made inside it for that matter. As long as the switchhing system stays the same, this box will not stop at a mere area code. It will stop at nothing. The electrical impulses that emit from this box will open every line. Every line will ring and ring and ring... the voltage will never be cut off until the box/ generator is stopped. This is no 200 volt job, here. We are talking GENERATOR. Every phone line will continue to ring, and people close to the box may be electricuted if they pick up the phone.

But, the Blotto Box can be stopped by merely cutting of the line or generator. If they are cut off then nothing will emit any longer. It will take

a while for the box to calm back down again, but that is merely a superficial aftereffect. Once again: Construction and use of this box is not advised! The Blotto Box will continue as long as thee is electricity to continue with.

OK, that is what it does, now, here are some interesting things for you to do with it...

--*-=> The Blotto Box Functions and Installation <=-*--

Once you have installed your Blotto, there is no turning back. The following are the instructions for construction and use of this box. Please read and heed all warnings in the above section before you attempt to construct this box.

Materials:
- A Honda portable generator or a main power outlet like in a stadium or some such place.
- A radio shack cord set for 400 volts that splices a female plug into a phone line jack.
- A meter of voltage to attach to the box itself.
- A green base (i.e. one of the nice boxes about 3' by 4' that you see around in your neighborhood. They are the main switch boards and would be a more effective line to start with.
  or: A regular phone jack (not your own, and not in your area code!
- A soudering iron and much souder.
- A remote control or long wooden pole.

Now. You must have guessed the construction from that. If not, here goes, I will explain in detail. Take the Honda Portable Generator and all of the other listed 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, sauder those lines together carefully. Wrap duck tape or insultation tape around all of the wires. Now, place the remote control right on to the startup of the generator. If you have the long pole,

make sure it is very long and stand back as far away as you can get and reach
the pole over. NOTICE: If you are going right along with this without reading
the file first, you sill 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 <=-*--

Original Idea: King Blotto.

Blue Box courtesy of the Jolly Roger

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---CO1-------TC1------TC2----CO2----B

A.... you
CO1=your central office
TC1.. your toll office.
TC2.. toll office in Amarillo.
CO2.. 806-258 central office.
B.... your friend (806-258-1234)

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 trunk 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	11	
700+1100	22	
900+1100	33	
700+1300	44	
900+1300	55	
1100+1300	66	
700+1500	77	
900+1500	88	
1100+1500	99	
1300+1500	00	

 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.

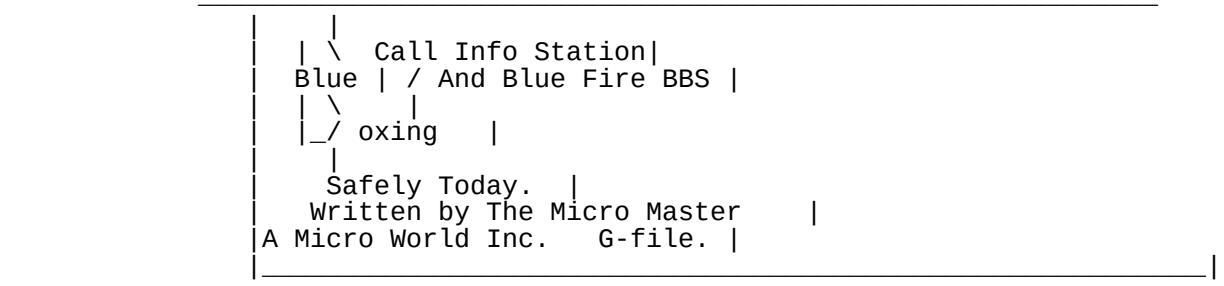
To complete a call using a blue box once seizure of a trunk has been accomplished by sending 2600Hz and pausing for the <beep><kerchunk>, one must first send a KP. This readies the register for the digits that follow.

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.



Blue Boxing: This file assmes you have made and/or know how to make a Blue Box, that you know how to use a Blue Box, and that you know what a Blue Box can do for you.

Blue Boxing at first:

When Blue Boxing first started At&t (called Bell at the time) was totaly unwary for this move. Blue Box tones where ordinginally created for the operator and the phone repair man. Using them phreaks used to tap lines, call anywhere for free, etc.

Then one dreaded day somebody at Bell caught on and BAM, people where busted like mad cause they thought blue box was safe.

Suddenly, people relized that it was not safe all the time, not safe sometimes, not safe at all. NEVER could you sue a Blue Box without being busted. But even after all this, Bell (and now At&t) still used Blue Box tone and they are still being
used today.

Now, how they got busted.

Every time a Blue Box tone is used, the number is came from is put on a list. This list contains all places where Blue Box tones came from in your area code. Now, just cause your name is on this list dosen't mean that your busted or anything, yo
ur still fine. However, at the end of the week another list is compared to the list of where the tones came from. If your NOT on this list you are in BIG trouble. Expect a vist to court.

Now, the trick of not getting busted.

The first thing is obvious. You must get on the second list mentioned above. Then your stumped, how do I get on that list?!?!?

Getting on a Blue Box tone list.

Alright, all operators are always on the list. So if you have a neighbor who is an operator, just put in a tap. No problem.

Now your saying "Oh great, all I have to do is move nextdoor to an operator. I read this whole G-file just to find that out!" Wrong. That's is the easiest way but by no means the only.

Another way: When a phone repair man comes to your house and either instals a new line, tests an old line, fixs a phone. Fixes a tine or works on your main Box (you know those big GREEN BOXS sitting in about every 8th house's yard. Then your nu
mber goes on the list.

By knowing a repair man you can get on this list or after having the line fixed, you can drag out your blue box and have some fun!

Finnaly. I have never succed in this but I know it DOES work.

Run a war dial of you area until you get a gold box (also called a diverter) tone. If you can find one go install a Gold Box somewhere. Now

scan again until you get your local At&t switching station. Call back through the diverter and hack unti
l you get a High level persons access. From a highlevel person access you can call in and edit the list of places where tones can come from. Now you can use the Blue Box. I personally have hacked a acount in At&t but it wasn't high enough to edit the l
ist but I could read it. From reading it I fround a bunch of good places to install a Gold Box.

  I be writing a G-phile on Gold boxing and then on on tapping a line.
   Look for more stuff soon.
L8R
   THE MICRO MASTER
 MICRO WORLD INC.

   The above was tested by The Micro Master, The Storyteller and someone else who dosen't have a modem but likes to call places free.

   The tests where done on At&t's Electronic Switching System (ESS) and no busts where even made so it is presumed safe.

    The Information Station   (xxx)xxx-xxxx
    The Fed's Reunion   (xxx)xxx-xxxx
    Ripco (xxx)xxx-xxxx
    The Blue Fire BBS   (xxx)xxx-xxxx
  Home of Micro World Inc.

[{-=:*> ASSORTED <*:=-}]
[{-=:*> BOX FREQUINCES <*:=-}]

(=)=(=)=(=)=(=)=(=)=(=)=(=)=(=)=(=)=(=)=(=)

BLUE BOX FREQUENCIES:

2600 HZ - USED TO GET ON/OFF TRUNK

TONE MATRIX TO USE AFTER 2600 HZ.

700:	1	2	4	7	11
900:	+	3	5	8	12
1100:	+	+	6	9	KP
1300:	+	+	+	10	KP2
1500:	+	+	+	+	ST

900	1100	1300	1500	1700

USE KP (1700+1100) TO START A CALL AND
ST (1500+1700) TO STOP. USE 2600 HZ TO
DISCONNECT.

RED BOX FREQS:

1700 HZ AND 2200 HZ MIXED TOGETHER

A NICKEL IS 66 MS ON (1 BEEP). A DIME IS 66MS ON, 66MS OFF, 66MS ON (2 BEEPS) A QUARTER IS 33MS ON, 33MS OFF REPEATED 5 TIMES. (MS= MILLISECOND). FOR THOSE OF YOU WHO DONT KNOW, A RED BOX SIMULATES MONEY BEING PUT INTO A PAY PHONE. YOU MUST PUT IN SOME MONEY FIRST THOUGH (THE OPERATOR CAN TELL IF MONEY WAS PUT IN BUT AS TO HOW MUCH, SHE LETS THE COMPUTER ANSWER THAT)

TASI LOCKING FREQ:

TASI (TIME ASSIGNMENT SPEECH INTERPOLATION) IS USED ON SATELITE TRUNKS, AND BASICALLY ALLOWS MORE THAN ONE PERSON TO USE A TRUNK BY PUTTING THEM ON WHILE THE OTHER PERSON ISNT TALKING. OF COURSE, YOU'D NEVER HEAR THE OTHER PERSON TALKING ON YOUR TRUNK.

WHEN YOU START TO TALK, HOWEVER, THE TASI CONTROLLER HAS TO FIND AN OPEN TRUNK FOR YOU. BECAUSE OF THIS, SOME OF YOUR SPEECH IS LOST(BECAUSE OF THE DELAY IN FINDING A TRUNK) THIS IS CALLED CLIPPING.

WELL, IF YOU WERE TRANSMITTING DATA OVER A TRUNK, CLIPPING WOULD REALLY FUCK UP THE DATA. SO THERE IS SOMETHING CALLED A TASI LOCKING FREQUENCY WHICH KEEPS THE TASI FROM PUTTING ANYONE ELSE ON YOUR TRUNK OR YOU ON ANYONE ELSES TRUNK. IN ANY CASE THE FREQ. IS 1850 HZ. SENT BEFORE THE

TRANSMISSION).

BLUE BOX PLANS

  NOTE TO ALL:THIS IS AN ORIGINAL PHILE
FROM THE OSUNY BBS(NOW DEFUNCT)...IT IS
STILL A VERY COMMONPLACE FILE, AND MANY
LAW ENFORCEMENT AGENCIES DO HAVE A
PRINTUP OF THIS FILE...IF YOU WERE EVER
CAUGHT WITH A COPY OF THIS PHILE, I
HAVE ABSOLUTELY NO IDEA NOR GRASP OF
WHAT THE CONSEQUENCES WOULD BE..ALSO
NOTE THAT IT IS AN OLD HARDWARE TYPE
FILE...UNLESS YOU ARE REALLY INTERESTED
IN BUILDING ONE, AND CAN ACCEPT THE
CONSEQUENCES OF BEING CAUGHT WITH A
HARDWARE BLUE BOX(OUTLINED ON D1'S
"PHREAKERS RIGHTS") THEN DO NOT TAKE
THIS FILE AND TRY TO USE IT...IT CAN
CERTAINLY MEAN NOTHING BUT TROUBLE
FOR YOU....

```
\-=-=-=-=-=-=-=-=-=-=/
\   /
\    THE ART AND   /
\    PRACTICE OF   /
\    BLUE BOXING   /
\   /
\=-=-=-=-=-=-=-=-=-=/
```

 =)>ORIGINALLY TYPED BY:<(=
^-NICKIE HALFLINGER-^
^- & MR. AMERICA -^
THIS IS THE TONE MATRIX FOR A BOX WHICH GENERATES
TONES THAT OPERATORS USE TO DIAL..ROTARY WORKS AS WELL,
ON OPERATOR LINES, BUT THIS IS TECHNOLOGICAL(!).
NOW I AGREE WITH THE OPINION OF A WELL KNOWN PHREAK
THAT 'BOXING' IS/WILL BE FOR THE MOST PART DEAD, BUT
THIS IS TRADITION... FIRST,YOU DIAL DIR.ASST, OR AN OPER. ETC,
THEN YOU BLAST THE LINE WITH A 2600HZ TONE. THIS GIVES YOU THE
LINE, THIS IS ALSO HOW MA BELL TRACKS DOWN BLUE BOXERS...
EVEN ON OLD #4 CROSSBARS... ONCE ON A OPER.TRUNK LINE,
YOU USE YOUR BLUE BOX/ROTARY TO DIAL...
SO, IF YOU USE 2600HZ, WHICH IS NECESSARY, UNLESS YOU
ARE *VERY* CAREFUL, YOU WILL BE SNAGGED.
FINALLY, THIS IS WHAT YOU READ!SO LONG AND HARD FOR:

```
700   :   1   :   2   :   4   :   7   :  11   :
900   :   +   :   3   :   5   :   8   :  12   :
1100  :   +   :   +   :   6   :   9   :  KP   :
1300  :   +   :   +   :   +   :  10   :  KP2  :
1500  :   +   :   +   :   +   :   +   :  ST   :
 :  900  : 1100  : 1300  :  1500 : 1700  :
```

USE KP TO START A CALL, AND ST TO STOP, WITH
THE BELOVED 2600HZ TONE TO DISCONNECT.
I ALSO HEAR THAT 2600HZ RESETS SPRINT NODES AND
GIVES YOU THEIR INITIAL TONE..
NOW, IF YOU'RE WONDERING ABOUT WHAT TO CALL FROM AN
OPERATOR TRUNK, HERE ARE SOME GOODIES TO HELP YOU OUT:
XXX+101 - TOLL SWITCHING
XXX+131 - INFORMATION
XXX+141 - RATE & ROUTE
XXX+181 - COIN REFUND OPERATOR
XXX+11501 - MOBILE OPERATOR
XXX+11521 - MOBILE OPERATOR
XXX+11511 - CONFERENCE OPERATOR

THESE WORK WITH ROTARY OR OPERATORS TONES, BUT ONLY ON OPER. TRUNK LINES...
THANKS FOR LISTENING!

BLUE BOXES, PART II

WHILE READING THE FINE ARTICLE ON THE BLUE BOX I SAW THAT THERE A LOT OF DATA LEFT OUT OF THE DOCUMENT. I HOPE THIS ADDS, IN SOME SMALL WAY, TO THE INFORMATION.
TIMING SPECS WERE NOT INCLUDED. THE TONE PAIRS ARE TO REMAIN ON FOR 1/10 SEC. WITH 1/10 SEC. OF SLIENCE BETWEEN DIGITS. THE 'KP' TONES SHOULD BE SENT FOR 2/10 SEC. A WAY TO DEFEAT THE 2600HZ TRAPS IS TO SEND ALONG WITH THE 2600HZ SOME PINK NOISE(MOST OF THE ENERGY IN THIS SIGNAL SHOULD BE ABOVE 3000HZ, THIS SIGNAL WON'T MAKE IT OVER THE TOLL NETWORK, BUT SHOULD CARRY AS FAR AS YOUR LOCAL TOLL CENTER) SO THAT THE TRAPS WON'T FIND 'PURE' 2600HZ ON THE TRUNK. THIS IS NOT A PERFECTLY SAFE WAY TO BOX, BUT IT SHOULD SLOW DOWN THE DISCOVERY.
AS TO USE, THE FIRST THING YOU NEED TO UNDERSTAND IS THAT THERE ARE TWO(2) TYPES OF TOLL COMPLETING TRUNK, INWARD AND OUTWARD. THE NAMES ARE REFERENCE TO THE OFFICE THAT IS SWITCHING THE CALL(THE TOLL CENTER THAT SERVES THE WATS LINE YOU CALLED) AND EACH TYPE OF TRUNK HAS A DIFFERENT CLASS OF SERVICE. FROM AN INWARD TOLL COMPLETING TRUNK, YOU CAN REACH THE DIFFERENT SERVICE OPERATORS, THE TOLL TEST BOARD, AND THE INWARD OPERATOR. SOME OFFICES ALSO ALLOW REMOTE TESTING AND IT IS IN THESE OFFICES THAT YOU CAN ACCESS THE OUTWARD TOLL COMPLETING TRUNKS. THE OUTWARD TRUNKS ALLOW YOU TO MAKE VERIFICATION(EMERGENCY) CALLS, DO BETWEEN LA AND NYC), ENABLE AND DISABLE TSPS POSITIONS, AND IN SOME CASES(ON SOME 4A'S) ISSUE TEMPORARY REROUTING INSTRUCTIONS(SEND ALL CALLS FROM LA TO NYC VIA MIAMI, BOSTON, OR ANY OTHER CLASS 5 OFFICE OR OFFICES). BOTH TYPE OF TRUNK ALLOW YOU TO PLACE A 'STANDARD' CALL WITH A BOX.
IN SOME OFFICES, MOSTLY THE SMALL ONES WITH A TOLL TEST BOARD THAT IS UNATTENDED AT NIGHT AND ON WEEKENDS, YOU CAN GET AN OUTWARD TOLL COMPLETING TRUNK AS WELL AS PERFORMING OTHER TEST AND ROUTING FUNCTIONS. YOU DO THIS BY USING THREE DIGIT CODES THAT ARE INVALID EXCHANGES(NOT OF THE PATTERN NNX[SEE NOTE 1]). DURING THE SIXITES THE CODES USED WERE FAIRLY STANDARD AND CONSISTENT, HOWEVER WHEN THE BOXES BECAME POPULAR AND THE PHREAKS STARTED DOING THINGS LIKE ROUTING ALL CALLS FROM DALLAS TO FT. WORTH VIA WASHINGTON D.C. MOTHER STARTED CHANGING THE TEST CODES ON A RANDOM(AS FAR AS I KNOW) BASIS. WHAT I WOULD SUGGEST IS THAT EVERYBODY INTERESTED IN DOING THIS SORT OF THING PICK OUT A NICE QUIET LITTLE OFFICE SOMEWHERE AND WORK ON DISCOVERING THE CODES ACCEPTABLE TO THAT OFFICE.
EACH NUMBERING PLAN AREA(NPA, ALSO KNOWN AS AREA CODE) HAS ALL OF THE OTHER TOLL OFFICES IN THE AREA AS WELL AS SERVING AS A CONCENTRATION POINT FOR MOST OUT OF AREA CALLS. TO ACCESS THE SERVICES OF A NON-MASTER OFFICE YOU NEED IT'S 'CITY CODE', THIS IS A THREE(3) DIGIT CODE THAT IS OF THE FORM 0XX, AND IS SENT AFTER THE AREA CODE[SEE NOTE 2]. AS AN EXAMPLE, THE 'CITY CODE' FOR CANTON, OHIO IS 042; THUS TO REACH THE INWARD OPERATOR IN CANTON, YOU WOULD SEND 'KP-216-042-121-ST' WHERE AS IF YOU WANTED THE INWARD OPERATOR IN CLEVELAND, YOU WOULD SEND 'KP-216-121-ST'. THE REASON THIS IS NECESSARY IS THAT THE OPERATOR IN CLEVELAND CAN'T VERIFY A NUMBER IN CANTON, SO IF YOU WANT TO VERIFY SOMEONE IN CANTON YOU NEED THE CITY CODE. ALSO, MOST AREA MASTER OFFICES HAVE DEDICATED DATA TRUNKS TO THE NETWORK CONTROL CENTER AND THUS DON'T ACCEPT TEST AND REROUTING COMMANDS OVER THE SWITCHED NET-

WORK.
IN CONCLUSION, THE SWITCHING NETWORK WILL DO A LOT MORE FOR YOU THEN CONNECT YOU TO PEOPLE AND THE SMALL OFFICES THAT REQUIRE A 'CITY CODE' ARE THE TYPE OF OFFICE TO TRY TO BREAK.
NICKIE HAFLINGER,
THE COVEN.
NOTE 1: THE NORMAL FORMAT FOR TELEPHONE NUMBERS IS AS FOLLOWS: NYN/NNX-XXXX. WHERE N=ANY DIGIT EXCEPT 1 AND 0; Y=0 OR 1, AND X=ANY DIGIT. YES I KNOW THAT IN SOME AREA CODES THE NNX FORMAT HAS CHANGED TO NXX. THIS IS A NEW OCCURRENCE AND ONLY OCCUR WHERE THERE HAS BE AN OUTRAGEOUS POPULATION INCREASE IN THE LAST FEW YEARS AND ALL OF THE FUNNY EXCHANGES ARE CONNECTED DIRECTLY TO MASTER OFFICES AND THUS DON'T CONFLICT WITH THE 'CITY CODE' FORMAT.

NOTE 2: YOU CAN OBTAIN THE 'CITY CODE' FOR A NUMBER BY CALLING RATE AND ROUTE AND ASKING FOR THE 'NUMBERS ROUTE' TO NYN/NNX(I.E. 914/725). OR IF YOU LEAVE ME A MESSAGE WITH THE AREA CODE AND FIRST THREE OF A NUMBER, I WILL GET YOU THE 'CITY CODE'.

THIS BULLETIN WILL DEAL ONLY WITH THE BASIC CONTRUCTION, WOULD LIKE TO KNOW THE SPECIFIC JOB OF ANY PART IN THE CIRCUIT JUST WRITE ME A MSG AND I WILL BE GLAD TO ANS-WER IT.

WE ALL KNOW THAT THE TOUCH TONES FREQUENCIES ARE COMPOSED OF TWO TONES (TWO DIFFERENT FREQS.) SO THAT IS THE REASON WHY WE HAVE 2 VCO'S (VOLTAGE CONTROLLED OSCILATORS). WE WILL CALL THESE VCO#1 AND VCO#2. IF YOU HAVE NOTICED VCO#1 ANS VCO#2 ARE EXACTLY THE SAME TYPE OF CIRCUITS. THAT IS WHY ONLY ONE WAS DRAWN. BUT REMEMBER THAT WHATEVER GOES FOR VCO#1 ALSO GOES FOR VCO#2. BOTH VCO'S ARE COMPOSED OF A HANDFULL OF PARTS. ONE CHIP TWO CAPACITORS 2 RESISTORS AND FIVE POTENTIOMETERS. ALL OF THIS WILL GIVE YOU (WHEN PROPERLY CALIBRATED) ONE OF THE FREQS. NECESSARY (THE OTHER ONE WILL COME FROM VCO#2) FOR THE OPERATION OF THE BB. BOTH OF THESE FREQS. WILL BE MIXED IN THE SPEAKER THUS FORMING THE REQUIRED TONE.

WHY?. BECAUSE OTHER DESIGNS WILL DRAIN THE BATTERY AFTER 10 - CALLS! THIS DESIGN WILL MAKE THEM LAST 10 MONTHS!!!!!!. BUT NEVER THE LESS DON'T FORGET TO PUT IN A SWITCH FOR ON AND OFF.
OK LET'S BUILD THE TWO VCO'S AND CALIBRATE THE UNIT BEFORE WE GET TO THE KEYBOARD CONTRUCTION.

VCO CONTRUCTION

TOOLS REQUIRED

1 OCILLISCOPE (RECOMENDED BUT NOT REQUIRED)
1 FREQ. COUNTER (REQUIRED)
1 VOLT METER " " "
ELECTRONICS TOOLS (PLIERS,DRILL, SCREWDRIVERS, ETC)

PARTS

R2 1K RESISTOR 5%

C1 .1UF ELECTROLYTIC CAPACITOR 16VDC
C2 .01UF ELECTROLYTIC CAPACITOR (MYLAR) 16VDC
IC1 2207 VCO CHIP BY EXAR ELECTRINICS
REMEMBER THE ABOVE IT IS ONLY FOR VCO#1 BUT THE SAME GOES FOR VCO#2.

R3-R4 150 OHM RESISTORS 5%
C3-C4 .1 UF ELECTROLITIC CAPACITOR 10VDC
P1-P10 200K TRIMMER POT - 20 TURNS
DIODES USED IN THE KEYBOARD ARE 1N914 TYPE (40 OF THEM)
AND 13 SWITCHES FOR THE KEYBOARD SPST. MOMENTARY.

SPKR= YOU CAN USE A TELEPHONE SPEAKER FOR THIS(IT WORKS BEST)
BUT REMEMBER TO TAKE OUT THE DIODE THAT IS CONNECTED
ACCROSS IT.

****

IMPORTANT NOTES

2 PINS 10,9,8 SHOULD BE TIED TOGETHER AND BE LEFT FLOATING.
3 ALL RESISTOR SHOULD BE 5%! NOTHING ELSE
4 A TELEPHONE SPEAKER GIVES THE BEST RESULTS

****

TROUBLE SHOOTING

BY NOW YOU SHOULD HAVE CONSTRUCTED THE TWO VCO'S ON A BREAD BOARD OR ANYTHING THAT PLEASES YOU.

CHECK FOR COLD SOLDER JOINTS, BROKEN WIRES, POLARITY OF THE BATTERY, ETC.....

BEFORE WE APPLY POWER TO THE VCO'S WE HAVE TO ADJUST THE POTS FOR THEIR HALF WAY TRAVEL POINT. THIS IS DONE BY TURNING THEM 21 TURNS TO THE RIGHT AND THEN 10 TURNS TO THE LEFT. DO THE SAME FOR ALL TEN OF THEM.

IN THE CHIPS BY PUTTING THE POSITIVE LEAD OF YOUR VOLT METER ON PIN 7 AND THE NEGATIVE LEAD ON PIN 12. IF YOU DON'T HAVE ANYTHING THERE TURN OFF THE UNIT ANT RECHECK THE WIRING.

WHEN YOU GET THE RIGHT VOLTAGES ON THE CHIPS, CONNECT A DIODE TO A PIECE OF WIRE (LOOK AT FIG. 2 FOR THE ORIENTATION OF THE DIODE) FROM GROUND TO ANY POT AT POINT T (LOOK CAREFULLY AT THE SCHEMATIC FOR POINT T IT IS LABELED T1-T10 FOR ALL POTS)
YOU SHOLD BE ABLE TO HEAR A TONE, IF NOT DISSCONNECT THE LEAD AND PLACE THE SPEAKER CLOSE TO YOUR EAR AND IF YOU HEAR A CHIRP LIKE SOUND, THIS MEANS THAT THE TWO VCO'S ARE WORKING IF YOU DON'T, IT MEANS THAT EITHER ONE OR BOTH OF THE VCO'S IS DEAD.
SO IN THIS CASE IT IS ALLWAYS GOOD TO HAVE AN OCILLOSCOPE ON HAND.

DISCONNECT THE SPEAKER FROM THE CIRCUIT AND HOOKUP THE OCILLISCOPE TO ONE OF THE LEADS OF THE SPEAKER AND THE GROUND FROM THE SCOPE TO THE GROUND OF THE BATTERY. CONNECT AGAIN THE GROUND LEAD WITH THE DIODE CONNECTED TO IT FROM GROUND TO ANY POT ON THE VCO THAT YOU ARE CHECKING AND YOU SHOULD SEE A TRIANGLE WAVE UNTIL YOU SEE IT. WHEN YOU DO SEE IT DO THE THE SAME FOR THE OTHER VCO TO MAKE SURE IT IS WORKING. (AMPLITUDE IS ABOUT 2VAC)

WHEN YOU GET THE TWO VCO'S WORKING YOU ARE SET FOR THE ADJUSTMENT OF THE INDIVIDUALS POTS...

ADJUSTMENT

DISCONNECT THE SPEAKER FROM THE CIRCUIT AND CONNECT A FREQ. COUNTER (THE POSITIVE LEAD OF THE COUNTER TO ONE OF THE SPEAKERS LEADS THAT BELONGS TO VCO#1 OR CONNECT IT TO PIN 14).

CONNECT THE NEGATIVE LEAD TO THE BATTERY NEGATIVE AND CONNECT THE JUMPER LEAD WITH THE DIODE FROM GROUND TO POT NUMBER 1 T1 .(THE FIRST POT NUMBER 1 POINT T1)
IF YOU GOT IT WORKING YOU SHOULD HEAR A TONE AND GET A READING ON THE COUNTER. ADJUST THE POT FOR A FREQ. OF 1700HZ AND CONTINUE DOING THE SAME FOR POTS 2-5 EXCEPT THAT THEY GET DIFFERENTS FREQS.

P1= 1700HZ
P2= 1300HZ
P3= 1100HZ
P4= 900HZ
P5= 1500HZ

NOW DISCONNECT THE FREQ. COUNTER FROM THE SPEAKER LEAD OF VCO#1 OR FROM PIN 14 (WHICH EVER YOU HAD IT ATTACHED TO AT THE BEGINNING) AND CONNECT IT TO THE SPEAKER LEAD OF VCO#2 OR TO PIN 14 OF VCO#2 AND PERFORM THE SAME ADJUSTMENTS TO P6-10.

P6= 1100HZ
P7= 700HZ
P8= 900HZ
P9= 2600HZ MAGIC NUMBER!!!!!
P10= 1500HZ

WHEN YOU FINISH DOING ALL OF THE POT GO BACK AND RECHECK THEM

KEYBOARD
IF YOU LOOK AT FIG-2 YOU WILL SEE THAT THE KEYS ARE SIMPLE SWITCHES CONNECTED TO GROUND AND TWO DIODES ON THE OTHER END. THESE DIODES ARE USED TO SIMPLIFY THE CONSTRUCTION OF THE KEYBOARD BECAUSE OTHERWISE THE DISTRIBUTION OF THE GROUND SIGNAL FOR BOTH VCO'S WOULD HAVE BEEN DONE MECHANICALLY. ONE DIODE WILL GO TO VCO#1 AND THE OTHER WILL GO TO VCO#2. FIG-3 SHOWS THE ARRANGEMENT OF THE KEYS ON THE KEYBOARD.

BELOW IS A TABLE THAT WILL HELP YOU CONNECT
THE KEYS TO REQUIRED VCO'S POTS.

KEY	TOTO POT ON VCO1	FREQ OUT POT ON VCO2	PIN 14 VCO1	PIN 14 VCO
C1	6	1700	1100	
02	10	1300	1500	
E1	10	1700	1500	
23	7	1100700		
33	8	1100900		
42	7	1300700		
52	8	1300900		
62	6	1300	1100	
75	7	1500700		
85	8	1500900		
95	6	1500	1100	
X-	9	----	2600	

****
* REMEMBER THAT FIG-2 IT IS THE SAME FOR EACH KEY EXCEPT THE "X" WHICH*
* ONLY TAKES ONE DIODE. *
****

AS A FINAL WORD YOU CAN BUILD THIS IN ANY TYPE OF ENCLOSURE AND SHOULD NEVER BE USED TO MAKE FREE CALLS USING THE TELEPHONE LINES. I HOPE THIS BULLETIN WILL CLEAR ANY QUESTION YOU MAY

IF YOU HAVE ANY QUESTION PLEASE
LEAVE ME A MSG. AND I WILL BE VERY GLAD TO
ANSWER IT.

TXS
MR. AMERICA

PS. I WOULD LIKE TO THANK MY KEYBOARD, MY FINGERS, AND ME FOR HELPING ME WRITTE THIS BULLETTIN. WITHOUT THEIR HELP I WOULD HAVE NEVER FINISH THIS PROJECT.

BLUE BOXING
[==========]

This is the tone matrix for a box which generates tones that operators use to dial..rotary works as well, on operator lines, but this is technological (!). now i agree with the opinion of a well known phreak that 'boxing' is/will be for the most part dead, but this is tradition... first,you dial dir.asst, or an oper. etc , then you blast the line with a 2600 hz tone. this gives you the line, this is also how many bell tracks down blue boxers... there are 2600hz detectors systems, and even on old #4 cross bars... once on a oper.trunk line, you use your blue box/rotary tdo dial...

so, if you use 2600hz, which is necessary, unless you are *very* careful, you will be snagged. finally, this is what you read! so long and hard for:

```
700   :   1   :   2   :   4 :   7   : 11   : 900   :   +   :   3
:   5 :   8   : 12   : 1100  :   +   :   +   :   6 :   9   : KP
: 1300  :   +   :   +   :   + :  10   : KP2  : 1500  :   +
: +   :   + :   +   : ST   : :  900  : 1100  : 1300 : 1500 : 1700
```

use kp to start a call, and st to stop, with the beloved 2600hz tone to disconnect. i also hear that 2600hz resets sprint nodes and gives you their initial tone..

now, if you're wondering about what to call from an operator trunk, here are some goodies to help you out:

XXX+101 - TOLL SWITCHING
XXX+121 - LOCAL OPERATOR
XXX+131 - INFORMATION
XXX+141 - RATE ROUTE
XXX+181 - COIN REFUND OPERATOR
XXX+11501 - MOBILE OPERATOR
XXX+11521 - MOBILE OPERATOR
XXX+11511 - CONFERENCE OPERATOR

---CONCERNING ABOVE

First the tones. while all the information is correct, the timing specs were not included . the tone pairs are to remain on for 1/10 sec. with 1/10 sec. of silence between digits. the 'kp' tones should be sent for 2/10 sec. a way to defeat the

2600 hz traps is to send a long with the 2600hz some pink noise(most of the en
ergy in this signal should be above 3000hz, this signal won't make it over the
toll network, but should carry as far as your local toll center) so that the tr
aps won't find
'pure' 2600 hz on the trunk. this is not a perfectly safe way to box, but it sho
uld slow down the discovery.

as to use, the first thing you need to understand is that there are two (2)
types of toll completing trunk, inward and outward. the names are reference to t
he office that is switching the call(the toll center that serves the watsline yo
u called) and e
ach type of trunk has a different class of service. from an inward toll completi
ng trunk, you can reach the different service operators, the toll test board, an
d the inward operator. some offices also allow remote testing and it is in these
offices that y
ou can access the outward toll completing trunks. the out wardtrunks allow you
to make verification(emergency) calls, do service monitoring(tapping), stack tru
nks(busy out all trunks between la and nyc), enable and disable tsps positions,
and in some cas

es(on some 4a's) issue temporary rerouting instructions(send all calls from la t
o nyc via miami, boston, or any other class 5 office or offices). both type of t
runk allow you to place a 'standard' call with a box.
in some offices, mostly the small ones with a toll test board that is unatt
ended at night and on weekends, you cange to an outward toll completing trunk as
well as performing other test and routing functions. you do this by using three
digit codes th
at are invalid exchanges (not of the pattern nnx[see note 1]). during the sixite
s the codes used were fairly standard and consistent, however when the boxes bec
ame popular and the phreaks started doing things like routing all calls from dal
las to ft. wort
h via washington d.c. others started changing the test codes on a random (as far
as i know) basis. what i would suggest is that everybody interested in doing th
is sort of thing pick out a nice quiet little office somewhere and work on disco
vering the code
s acceptable to that office.
each numbering plan area (npa, also known as area code)has an office design
ated as its master office. this office controls all of the other toll offices in

the area as well asserving as a concentration point for most out of area calls.
to access the s
ervices of a non-masteroffice you need it's'city code', this is a three (3) digit
code that is of the form 0xx, and is sent after the area code [see note 2]. as

an example, the 'city code' for canton, ohio is 042; thus to reach the inward o
perator in cant
on, you would send 'kp-216-042-121-st' where as if you wanted the inward operato
r in cleveland, you would send 'kp-216-121- st'. the reason this is necessary is
that the operator in cleveland can't verify a number in canton, so if you want
to verify someo
ne in canton you need the city code. also, most area master offices have dedicat
ed data trunks to the network control center and thus don't accept test and rero
uting commands over the switched net-work.

in conclusion, the switching network will do a lot more for you then connec
t you to people and the small offices that require a 'city code' are the type of
office to try to break.

note 1: the normal format for telephone numbers is as follows: nyn/nnx-xxxx
. where n=any digit except 1 and 0;y=0 or 1, and x=any digit. yes i know that in
some area codes the nnx format has changed to nxx. this is a new occurrence and
only occur whe
re there has be an outrageous population increase in the last few years and all
of the funny exchanges are connected directly to master offices and thus don't c
onflict with the 'city code' format.

note 2: you can obtain the 'city code' for a number by calling rate and rou
te and asking for the 'numbers route' to nyn/nnx(i.e. 914/725). or if you leave
me a message with the area code and first three of a number, i will get you the'
city code'.

blue box plans

```
$ BLUE BOX PLANS! $
$   This file will explain the   $
$ construction, troubleshooting, and  $
$ adjustment of a Blue Box. $
$  $
$   We all know that the touch tone   $
```

```
$ frequencies are composed of 2 tones $
$ (2 different freqs.) so that is the $
$ reason why we have 2 VCO's (Voltage $
$ Controlled Oscilators). We'll call  $
$ them VCO#1 and VCO#2. If you have   $

$ noticed VCO#1 and VCO#2 are exactly $
$ the same type of circuits. That is  $
$ why only 1 was drawn. But remember  $
$ that whatever goes for VCO#1 also   $
$ goes for VCO#2. Both VCO'S are $
$ composed of a handfull of part. One $
$ chip, two capacitors, 2 resistors   $
$ and five potentiometers. All of$
$ this will give you (when properly   $
$ calibrated) one of the freqencies   $
$ necessary (the other one will come  $
$ from VCO#2) for the operation of    $
$ the Blue Box. Both of these freqs.  $
$ will be mixed in the speaker to$
$ form the required tone.   $
$  $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$  $
$   This is one of the most $
$ sophisticated designs I have ever   $
$ made. Why?. Because other designs   $
$ will drain the battery after 10$
$ calls. This design will make them   $
$ last 10 months!!!!!!. But never the $
$ less, don't forget to put in a $
$ switch for on and off. Ok let's$
$ build the two VCO'S and calibrate   $
$ the unit before we get to the  $
$ keyboard construction.    $
$  $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
!  !
!VCO CONSTRUCTION !
!=== ============ !
!  !
! TOOLS REQUIRED  !
! ----- --------  !
!  !
! 1 ocilliscope(optional but not req) !
! 1 Freq. counter   (REQUIRED)   !
! 1 Volt meter  "  "  "!
!   Electronics tools  (Pliers,drll,  !
!   screwdrivers, etc.)!
!  !

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
.......................................
.  .
. ! $-PARTS-$ !   .
. -------------   .
.  .
. R1  1.5K RESISTOR  5%.
. R2  1K   RESISTOR  5%.
. C1 .1uf ELECTROLYTIC CAPACITOR 16VDC.
. C2 .01uf    "   "  (MYLQR)16VDC.
.IC1 2207 VCO CHIP BY EXAR ELECTRONICS.
.    Remember the above only says.
.    VCO#1 but the same is for VCO#2  .
```

. R3-R4 150 OHM RESISTORS 5%   .
. C3-C4 .1 uf ELECTROLITIC CAPACITOR .
. 10VDC.
. P1-P10 200K TRIMMER POT - 20 TURNS .
. DIODES USED IN THE KEYBOARD   .
. ARE 1N914 TYPE (40 OF THEM) .
. 13 SWITCHES FOR THE KEYBOARD .
. SPST MOMENTARY..
. SPKR=YOU CAN USE A TELEPHONE SPEAKER.

. FOR THIS (IT WORKS BEST) BUT   .
. REMEMBER TO TAKE OUT THE DIODE .
. THAT IS CONNECTED ACCROSS IT. .
****
*   ---------------------   *
*   ! *IMPORTANT NOTES* !   *
*   ---------------------   *
* 1. DO NOT USE ANYTHING ELSE OTHER *
*THAN A MYLAR CAPACITOR FOR C2. *
* 2. PINS 10,9,8 SHOULD BE TIED *
*TOGETHER AND BE LEFT FLOATING. *
* 3. ALL RESISTORS SHOULD BE 5%!*
*NOTHING ELSE!   *
* 4. A TELEPHONE SPEAKER GIVES THE   *
*BEST RESULTS.   *
****
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%   --------------------   %
%   ! TROUBLE SHOOTING !   %
%   --------------------   %
%   By now you should have constructed%
% the two VCO'S on a bread board or   %

% anything that pleases you.%
% Check for cold solder joints, broken%
% wires, polarity of the battery, etc.%
% Before we apply power to the VCO'S %
% we have to adjust the pots for their%
% half way travel point. This is done %
% by turning them 21 turns to the%
% right and then 10 turns to the left.%
% Do the same for all ten of them.   %
%-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-%
%   Now apply power to the unit check %
% to see that you have power in the   %
% chips by putting the positive lead %
% of your volt meter on pin 7 and the %
% negative lead on pin 12. If you do %
% not have anything there turn off   %
% the unit and RECHECK THE WIRING.   %
%-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-%
%   When you get the right voltages   %
% on the chips, connect a diode to a %
% piece of wire (look at fig. 2 for   %
% the orientation of the diode) from %

% ground to any pot at point T (look %
% carefully at the schematic for %
% point T it is labeled T1-T10 for   %
% all pots). You should be able to   %
% hear a tone, if not disconnect the %
% lead and place the speaker close to %
% your ear and if you hear a%
% chirp-like sound, this means that   %

```
% the two VCO'S are working if you    %
% don't, it means that either one or  %
% both of the VCO'S are dead. So in   %
% this case it is always good to have %
% an ocilloscope on hand.   %
% Disconnect the speaker from the%
% circuit and hook the ocilliscope to %
% 1 of the leads of the speaker  the %
% ground from the scope to the ground %
% of the battery. Connect again the   %
% ground lead with the diode connected%
% to it from ground to any pot on the %
% VCO that you are checking and you   %
% should see a triangle wave if not   %

% turn the pot in which you are  %
% applying the ground to until you see%
% it. When you do see it do the the   %
% same for the other VCO to make sure %
% it is working. (amplitude is about  %
% 2VAC). When you get the two VCO's   %
% working you are set for the    %
% adjustment of the individuals pots. %
%  %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
:  -------------- :
:  ! ADJUSTMENT ! :
:  -------------- :
:   DISCONNECT THE SPEAKER FROM THE   :
: CIRCUIT AND CONNECT A FREQ. COUNTER :
: (THE POSITIVE LEAD OF THE COUNTER TO:
: ONE OF THE SPEAKERS LEADS THAT :
: BELONGS TO VCO#1 OR CONNECT IT TO   :
: PIN 14).   :
:-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-:
:   CONNECT THE NEGATIVE LEAD TO THE  :
: BATTERY NEGATIVE AND CONNECT THE    :

: JUMPER LEAD WITH THE DIODE FROM:
: GROUND TO POT NUMBER 1.T1.:
: ( THE FIRST POT NUMBER 1 POINT T1)  :
: IF YOU GOT IT WORKING YOU SHOULD    :
: HEAR A TONE AND GET A READING ON    :
: THE COUNTER. ADJUST THE POT FOR A   :
: FREQ. OF 1700hz AND CONTINUE DOING  :
: THE SAME FOR POTS 2-5 EXCEPT THAT   :
: THEY GET DIFFERENTS FREQS. WHICH ARE:
:  $$$$$$$$$$$$$ :
:  $ P1= 1700hz $ :
:  $ P2= 1300hz $ :
:  $ P3= 1100hz $ :
:  $ P4=  900hz $ :
:  $ P5= 1500hz $ :
:  $$$$$$$$$$$$$ :
:   NOW DISCONNECT THE FREQ. COUNTER  :
: FROM THE SPEAKER LEAD OF VCO#1 OR   :
: FROM PIN 14 (WHICH EVER YOU HAD IT  :
: ATTACHED TO AT THE BEGINNING) AND   :
: CONNECT IT TO THE SPEAKER LEAD OF   :
: VCO#2 OR TO PIN 14 OF VCO#2 AND:

: MAKE THE SAME ADJUSTMENTS TO P6-10. :
:  $$$$$$$$$$$$$:
:  $ P6=  1100hz $:
```

```
:  $ P7=   700hz $:
:  $ P8=   900hz $:
:  $ P9=  2600hz $:
:  $ P10= 1500hz $:
:  $$$$$$$$$$$$$$:
:   WHEN YOU FINISH DOING ALL OF THE  :
: POTS GO BACK AND RE-CHECK THEM.:
::::::::::::::::::::::::::::::::::::
<   --------=---  >
<   ! KEYBOARD !  >
<   ------------  >
<   IF YOU LOOK AT FIG-2 YOU WILL SEE >
< THAT THE KEYS ARE SIMPLE SWITCHES.  >
< CONNECTED TO A GROUND AND TWO  >
< DIODES ON THE OTHER END. THESE >
< DIODES ARE USED TO SIMPLIFY THE>
< CONSTRUCTION OF THE KEYBOARD   >
< BECAUSE OTHERWISE THE DISTRIBUTION  >
< OF THE GROUND SIGNAL FOR BOTH VCO'S >

< WOULD HAVE BEEN DONE MECHANICALLY.  >
< THE DIODE WILL GO TO VCO#1 AND THE  >
< OTHER WILL GO TO VCO#2. FIG-3 SHOWS >
< THE ARRANGEMENT OF THE KEYS ON THE  >
< KEYBOARD.  >
z5ujj-=-=->-=-=-=-=-=-=-?
<   BELOW IS A TABLE THAT WILL HELP   >
< YOU CONNECT THE KEYS TO THE    >
< REQUIRED VCO'S POTS. >
<-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=->
<    (-FIG 2-)    >
<-----!-----!--------!--------!------->
<!!   !   !  >
< TO  ! TO  !  FREQ  !  FREQ  !  KEY  >
< POT ! POT !  OUT:  !  OUT:  !  >
< ON  ! ON  !   !   !  >
< VCO1! VCO2!   !   !  >
<-----!-----!--------!--------!------->
<  1  !  06 ! 1700hz ! 1100hz !   C   >
<  2  !  10 ! 1300hz ! 1500hz !   0   >
<  1  !  10 ! 1700hz ! 1100hz !   E   >
<  4  !  07 ! 0900hz ! 0700hz !   1   >

<  3  !  07 ! 1100hz ! 0700hz !   2   >
<  3  !  08 ! 1100hz ! 0900hz !   3   >
<  2  !  07 ! 1300hz ! 0700hz !   4   >
<  2  !  08 ! 1300hz ! 0900hz !   5   >
<  2  !  06 ! 1300hz ! 1100hz !   6   >
<  5  !  07 ! 1500hz ! 0700hz !   7   >
<  5  !  08 ! 1500hz ! 0900hz !   8   >
<  5  !  06 ! 1500hz ! 1100hz !   9   >
<  -  !  09 ! ------ ! 2600hz !   X   >
<-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=->
<   REMEMBER THAT IN FIG-2 IT'S THE   >
< SAME FOR EACH KEY EXCEPT THE "X"    >
< KEY, WHICH ONLY TAKES ONE DIODE.    >
*******************************.*******
```

few KEYS to the diagram:

Cx is capacitor #x Denoted by: ---| |---

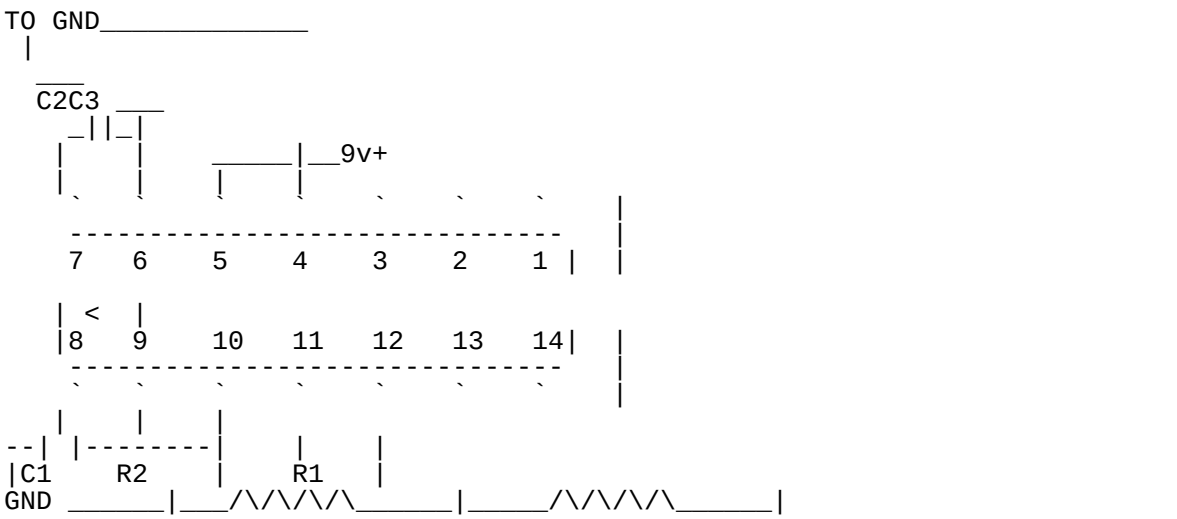
Px is Pot or Variable resistor #x Denoted by :/

```
  \

  /<--
 \
```
Rx is resistor #x Denoted by /\/\/\/\

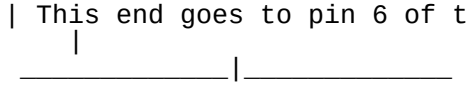
Schematics

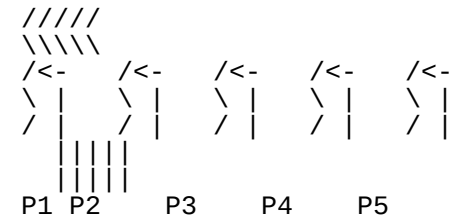
The XR-2207 chip is a Voltage-Controlled Oscillator and a 14 pin device thus you must be very careful when soldering the parts to this device. It is
a little dificult to actually draw a schematic on an 80 character screen
using limited graphics, but I will give it a try.



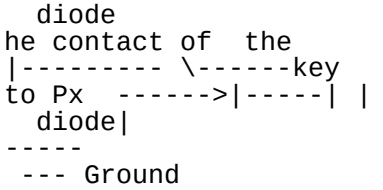
is is a diagram of how to locate the different pins on the chip.
Please notice that pin one (1) is the closest to the notch on top of the chip.
The first thing we'll do is to connect power to the chip (remember that you
need to build two (2) of these to get a complete system) this is accomplished
by connecting the positive wire of the battery lead to pin#1 one leg of R1
and R2 is soldered to pin#11. The other leg of R1 goes to pin 1 or to the d. C1 goes
between pin 10 and ground. The timing capacitor or C2 goes between pins 2 and 3 of the chip. Pins 8 and 9 should be grounded to ground. Pin 14 is the
output and this is where one leg of C4 (C3 goes on the other VCO) in series
with R3 (the same goes for the other VCO) and to one lead of the speaker.

The trimmer pots P1 to P10 should be grouped in groups of 5 pots each.
The way you group it is by soldering one end of the pot to each other leaving
the wiper and the other end free.





And finally this is the way each key should be wired.



Note to sysops: You are welcome to download this file and use it on your system, providing you DO NOT remove the credits for Mark Tabas or KAOS. In other words, try to act like a human being!

The Mark Tabas encounter series presents:

-=-

Better Homes and Blue Boxing

Part I

Theory of Operation

=-=

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 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 Armarillo, Texas). For ease, we'll assume that you are on #5 Crossbar switching and not in the 806 area. Your central office (CO) would recognize that 806 is a foreign NPA, so it would route the call to the toll centre that serves you. [For the sake of accuracy here, and for the more experienced readers, note that the CO in question is a class 5 with LAMA that uses out-of-band SF supervisory signalling]. Depending on where you are in the country, the call would leave your toll centre (on more trunks) to another toll centre, or office of higher "rank". Then it would be routed to central office 806-258 eventually and the call would be completed. Illustration:

```
A---CO1-------TC1------TC2----CO2----B

A=you  CO1=your central office
TC1=your toll office.
TC2=toll office in Amarillo.
CO2=806-258 central office.
B=your friend (806-258-1234)
```

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 too much. 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 (806-258-1234) so you send a 2600Hz down the line. This tone travels down the line to your friend's central office (CO2) where it is detected. However, that CO thinks that the 2600Hz is originating from Bell equipment, indicating to it that you've hung up, and thus the trunks are once again idle (with 2600Hz present on them). But actually, you

have not hung up, you have fooled the equipment at your friend's CO into thinking you have. Thus,it disconnects him and resets the equipment to prepare for the next call. All this happens very quickly (300-800ms for step-by-step equipment and 150-400ms for other equipment).

When you stop sending 2600Hz (after about a second), the equipment thinks that another call is coming towards it (e.g. it thinks the far end has come "off-hook" since the tone has stopped. It could be thought of as a toggle switch: tone --> 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 dinosaur , 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 signalling consists of 7 frequencies, beginning with 700Hz and separated by 200Hz. A different set of two of the 7 frequencies represent the

digits 0 thru 9, plus an additional 5 special keys. The frequencies and uses are as follows:

Frequencies (Hz)	Domestic	Int'l
700+900	11	
700+1100	22	
900+1100	33	
700+1300	44	
900+1300	55	
1100+1300	66	
700+1500	77	
900+1500	88	
1100+1500	99	
1300+1500	00	
700+1700	ST3p	Code 11
900+1700	STp	Code 12
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 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 a 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 2 seconds while a trunk is seized.

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 area 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 dialed).

This has been Part I of Better Homes and Blue Boxing. I hope you enjoyed and learned from it. If you have any questions, comments, threats or insults, please fell free to drop me a line. If you have noticed any errors in this text (yes, it does happen), please let me know and perhaps a correction will be in order. Part II will deal mainly with more advanced principles of blue boxing, as well as routings and operators.

Note 1: other highly trunkable areas include: 816,305,813,609,205. I personally have excellent luck boxing off of 609-953-0000. Try that if you have any trouble.

.....
 Mark Tabas
.....
$$LODLODLODLODLODLODLODLODLOD$

```
   ----------------------
   :    Written for:    :
   ::
   : K.A.O.S. :
   ::
   :   at:
   ::
   :    215-xxx-xxxx    :
   ::
   ----------------------
```

Go To Part 2
Go To Part 3

The Mark Tabas encounter series
presents...

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Better Homes and Blue Boxing
Part ii
Practical Applications
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

(It is assumed that the reader has read and understood Part i of this series).

The essential purpose of blue boxing in the beginning was merely to receive toll services free of charge. Though this can still be done, blue boxing has essentially outlived its usefulness in this area. Modern day "extenders" and long distance services provide a safer and easier way to make free fone calls. However, you can do things with a blue box that just can't be done with anything else. For ordinary toll-fraud, a blue box is impractical for the following reasons:

1. Clumsy equipment required (blue box or equivalent)
2. Most boxed calls must be made through an extender. Not for safety reasons, but for reasons I'll explain later.
3. Connections are often sacrificed because considerable distances must be dialed to cross a seizable trunk, in addition to awkward routing.

As stated in reason #2, boxed calls are usually made through an extender. This is for billing reasons. If you recall from Part i, 2600Hz is used as a "supervisory" signal. That is, it signals the status of a trunk-- "on-hook" or "off-hook." When you seize a trunk (by briefly sending 2600Hz), your end (the CALLING end) goes on hook for the duration of the 2600Hz and then goes off-hook once again when the 2600Hz is terminated. The CALLED end recognizes that a call is on the way and attaches a register, which inerprets the digits which are to be sent. Now, understand that even though your end has come off-hook (no 2600Hz present), the other end is still on-hook. You may wonder then, why, if the other end (the CALLED end) is still on-hook, there is no 2600Hz coming the other way on the trunk, when there should be. This is correct. 2600Hz *IS* present on the trunk when you seize it and afterwards, but you cannot hear it because of a Band

Elimination Filter (BEF) at your central office.

Back to the problem. Remember that when you seize a trunk, 2600Hz is indeed coming the other way on the trunk because the CALLED end is still on-hook, but you don't actually hear it because of a filter. However, the Bell equipment knows it's there (they can "hear" it). The presence of the 2600Hz is telling the billing equipment that your call has not yet been completed (i.e., the CALLED end is still on-hook). When finally you do connect with your boxed call, the 2600Hz from the called end terminates. This tells the billing equipment that someone picked up the fone at the CALLED end and you should begin to be billed. So you do start to get billed, but for the call to the trunk, NOT the boxed call. Your billing equipment thinks that you've connected with the number you used to seize the trunk.

Illustration:

1. You call 1+806-258-2222 (directly)
2. Status of trunks:

```
<----------------------------------->
(You)806-258-2222
No 2600Hz-------> <------------2600Hz
```

When you seize a trunk (before the number you called answers) there is no affect on your billing equipment. It simply thinks that you're still waiting for the call to complete (the CALLED end is still on-hook; it is ringing, busy, going to recorder or intercept operator.

Now, let's say that you've sezied a trunk (806-258-2222) and for example, KP+314+949+1705+ST. The call is routed from the tandem you seized to: 314-949-1705.

Illustration:

```
<------------------>O<--------------->
(You)    806    314-949
  tandem
No 2600Hz----------> <----------2600Hz
```

Note that the entire path towards the right (the CALLED end) has no 2600Hz present and is therefore "off-hook." The entire path towards the left (the CALLING end) does have 2600Hz present on it, indicating that the CALLED end has not picked up (or come "off-hook"). When 314-949-1705 answers,

"answer supervision" is given and the 2600Hz towards the left (the CALLING end) terminates. This tells your billing equipment, which thinks that you're still waiting to be connected with 806-258-2222, that you've finally connected. Billing then begins to 806-258-2222. Not exactly an auspicious beginning for an aspiring young phone phreak.

To avoid this, several actions may be taken. As previously mentioned, one may avoid being charged for the number called to seize a trunk by using an extender (in which case the extender will get billed). In some areas, boxing may be accomplished using an 800 number, generally in the format of 800-858-xxxx (many Amarillo numbers) or 800-NN2-xxxx (special intra-state class in-WATS numbers). However, boxing off of 800 numbers is impossible in many areas. In my area, Denver, I am served by #1A ESS and it is impossible for me to box off of any 800 number.

Years ago, in the early days of blue boxing (before my time), phreaks often used directory assistance to box off of because they were "free" long distance calls. However, because of competetive long distance companies, directory assistance surcharges are now $0.50 in many areas. It is additionally advised that directory assistance numbers not be used to box from because of the following:

Average DA calls last under 2 minutes. When you box a call, chances are that it will last considerably longer. Thus, the Bell billing equip-ment will make a note of calls to directory assistance that last a long time. A call to a directory assistant lasting for 4 hours and 17 minutes may appear somewhat suspicious.

Although the date, time, and length of a DA call do not appear on the bill, it is recorded on AMA tape and will trip a trouble report if it were to last too long. This is how most phreaks were discovered in the old days. Also, sometimes too many calls lasting too long to one 800 number may raise a few eyebrows at the local security office.

Assuming you can complete a blue box call, the following are listed routings for various Bell internal operators. These are in the format of KP+NPA+ special routing+1X1+ST, which I will explain later. The 1X1 is the actual operator routing, and NPA and NPA+ special routing are used for out-of-

area code calls and out-of-area code calls requiring special routing, respectively.

KP+101+ST ..... toll test board
KP+121+ST ..... inward op
KP+131+ST ..... directory assistance
KP+141+ST ..... was rate & route. Now only works in 312, 815, 717, and a few others. It has been replaced with a univer-sal rate & route number, 800+141+1212.
KP+151+ST ..... overseas completion operator (inbound). Works only in certain NPAs, such as 303.
KP+181+ST ..... in some areas, toll station for small towns

Thus, if you seize a trunk in 806 NPA and wanted an inward (in 806), then you would dial KP+121+ST. If you wanted a 312 inward and were dialing on an 806 trunk, an area code would be required. Thus, you would dial KP+312+121+ST. Finally, some places in the network require special routing, in addition to an area code. An example is Franklin Park, Ill. It requires a special routing of 032. For this, you would dial KP+312+032+121+ST for a Franklin Park inward operator.

Special routings are in the format of 0XX. They are used primarily for load balance, so that traffic flow may be evenly distributed. About half of the exchanges in the network require special routing. Note that special routings are NEVER EVER EVER used to dial normal telephone numbers, only operators.

Operator functions:

TOLL TEST BOARD- Generally a cordboard position that assists in trunk testing. They are not used by operators, only switchmen.

INWARD- Assists the normal TSPS (0+) operator in completing calls out of the TSPS's area. Also, inwards perform emergency inerrupts when the number to be interrupted is out of the area code of the original (TSPS) operator. For example, a 303 operator has a customer that needs an emergency interrupt on 215-647-6969. The 303 operator gets the routing for the inward that covers 215-647, since she cannot do the interrupt herself. The routing is found to be only 215+ (no special routing required). So, the 303 operator

keys KP+215+121+ST. An inward answers and the 303 says to her, "Inward, this is Denver. I need an emergency interrupt on 215-647-6969. My customer's name is Mark Tabas." The inward will then do the interrupt (off the line, of course). If the number to be interrupted had required special routing, such as, say, 312-456-1234 (spec routing 032), then the 303 operator would dial KP+312+032+121+ST for the inward to do that interrupt.

DIRECTORY ASSISTANCE- These are the normal NPA+555+1212 operators that assist customers with obtaining telefone directory listings. Not much toll-fraud potential here, except maybe $0.50.

RATE AND ROUTE- These operators are reached by dialing KP+800+141+1212+ST. They assist normal (TSPS) operators with rates and routings (thus the name). The only uses I typically have for them are the following:

1. Routing information. In the above example, when the 303 operator needed to dial an inward that served 215-647, she needed to know if any special routing was required and, if so, what it was. Assuming she would use rate and route, she would dial them and say nicely, "Operator's route, please, for 215-647." Rate & route would respond with "215 plus." This means that the operator would dial KP+215+121+ST to reach the inward that serves 215-647. If there were special routing required, such as in 312-456, rate & route would respond with "312 plus 032 plus." In that case, the operator would dial KP+312+032+ST for the inward that serves 312-456.
  It is good practice to ask for "operator's route" specifically, as there are also "numbers route" and "directory routes." If you do not specifically ask for operator's route, rate & route will generally assume that is what you want anyway.
  "Numbers" route refers to overseas calls. Example, you want to know how to reach a number in Geneva, Switzerland (and you already have the number). You would call routing and say "Numbers route, please, Geneva, Switzerland." The operator would respond with: "Mark 41+22. 011+041+ST (plus) 041+22" The "Mark 41+22" has to do with billing, so disregard it. The 011+041 is access to the overseas gateway (to be discussed in Part iii) and the 041+

22+ is the routing for Geneva from the overseas sender.

"Directory" routings are for directory assistance overseas. Example: you want a DA in Rome, Italy. You would call rate & route and say, "Directory routing please, for Rome, Italy." They would respond with "011+039+ST (plus) 039+1108 STart." As in the previous example, the 011+039 is access to the overseas gateway. The 039+1108 is a directory assistant in Rome.

2. Nameplace information. Rate & Route will give you the location of an NPA+ exchange. Example: "Nameplace please, for 215-648." The operator would respond with "Paoli, Pennsylvania." This isn't especially useful, since you can get the same information (legally) by dialing 0, but using rate & route is often much faster and it avoids having to hang up when you are already on a trunk.

*NOTE on Rate & Route: As a blue boxer, always ask for "IOTC" routings. (e.g., "IOTC operator's route", "IOTC numbers route", etc.) This tells them that you want cordboard-type routings, not TSPS, because a blue boxer is actually just a cordboard position (that Bell doesn't know about).

OVERSEAS COMPLETION OPERATOR (inbound)- These operators (KP+151+ST) assist in the completion of calls coming in to the United States from overseas. There are KP+151+ST operators only in a few NPAs in the country (namely 303). To use one, you would seize a trunk and dial KP+303+151+ST. Then you would tell the operator, for example, "This is Bangladesh calling. I need U.S. number 215-561-0562 please." [in a broken Indian accent]. She would connect you, and the bill would be sent to Bangladesh (where I've been billing my KP+151+ST calls for two years).

Other internal Bell Operators.

KP+11501+ST ..... universal operator
KP+11511+ST ..... conference op
KP+11521+ST ..... mobile op
KP+11531+ST ..... marine op
KP+11541+ST ..... long distance terminal
KP+11551+ST ..... time & charges op
KP+11561+ST ..... hotel/motel op
KP+11571+ST ..... overseas (outbound) op

These 115X1 operators are identical in routing to the 1X1 operators listed previously, with one exception. If special routing is required (0XX), then the trailing 1 is left off.

Examples:

A 312 universal op ... KP+312+11501+ST
A Franklin Park (312-456) universal op (special routing 032 required).... ..... KP+312+032+1150+ST
[The trailing 1 of 11501 is left off].

Purposes of 115X1 operators.

UNIVERSAL- Used for collect/callback calls to coin stations.

CONFERENCE- This is a cordboard conference operator who will set up a conference for a customer on a manual operation basis.

MOBILE- Assists in completion of calls to mobile (IMTS) type telefones

MARINE- Assists in completion of calls to ocean going vessels.

LONG DISTANCE TERMINAL- Now obsolete. Was used for completion of long distance calls.

TIME & CHARGES- Will give exact costs of calls. Used to time calls and inform customer of exactly how much it cost.

HOTEL/MOTEL- Handles calls to/from hotels and motels.

OVERSEAS COMPLETION (outbound)- assists in completion of calls to overseas points. Only works in some, if any NPAs, because overseas assistance has been centraized to IOCC (covered in Part iii).

Note that all KP+1X1+ST and KP+115X1+ST operators automatically assume that you are a TSPS or cordboard operator assisting a customer with a call. DO NOT DO ANYTHING TO JEOPARDIZE THIS! If you do not know what to do, don't call these operators! Find out what to do first.

This concludes Part iii. There is one final part in which I will explain overseas dialing, IOCC (International Overseas Completion Centre), RQS (Rate/Quote System), and some basic scanning.

.....
(c) February 6, 1900 Mark Tabas
.....

Go To Part 1
Go To Part 3

The Mark Tabas encounter series
presents...

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Better Homes and Blue Boxing
Part iii
Advanced Signalling

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

(It is assumed that the reader has read and$understood parts i & ii before proceeding to this part).

In parts i & ii, I covered basic theory and domestic singalling and operators. In this part I will explain overseas direct boxing, the IOCC, the RQS, and some basic scanning methods.

Overseas Dipect Boxing.

Calling outside of the United States and Canada is accomplished by using an "overseas gateway." There are 7 overseas gateways in the Bell System, and each one is designated to serve a certain region of the world. To initiate an overseas call, one must first access the gateway that the call is to be sent on. To do this automatically, decide which country you are calling and find its country code. Then, pad it to the left with zeros as required so it is three digits. [Add 1, 2, or 3 zeros as required].

Examples:

Luxembourg (352) is 352 (stays the same)
Spain (34)   becomes 034 (1 zero added)
U.S.S.R. (7) becomes 007 (2 zeros added)

Next, seize a trunk and dial KP+011+CC+ST. Note that CC is the three digit padded country code that you just determined by the above method. [For Luxembourg, dial KP+011+352+ST, Spain KP+011+034+ST, and the U.S.S.R. KP+011+007+ST]. This is done to route you to the appropriate overseas gateway that handles the country you are dialing. Even though every gateway will allow you to dial every dialable country, it is good practice to use the gateway that is designated for the country you are calling.

After dialing KP+011+CC+ST (as CC is defined above) you should"be connected to an overseas gateway. It will acknowledge by sending a wink (which is audible as a <beep><kerchink> and a dial tone. Once you receive international dial tone, you may route your

call one of two ways: a) as an operator-originated call, or b) as a customer-originated call. To go as a operator-originated call, key KP+ country code (NOT padded with zeros)+ city code+number+ST. You will then be connected, providing the country you are calling can receive direct-dialed calls. The U.S.S.R. is an example of a country that cannot.

Example of a boxed int'l call:

To make a call to the Pope (Rome, Italy), first obtain the country code, which is 39. Pad it with zeros so that it is 039. Seize a trunk and dial KP+011+039+ST. Wait for sender dial tone anf then dial KP+39+6+6982+ST. 39 is the country code, 6 is the city code, and 6982 is the Pope's number in Rome. To go as an operator-originated call, simply place a zero in front of the country code when dialing on the gateway. Thus, KP+0+39+6+6982+ST woulf be dialed at sender dial tone. Routing your call as operator-originated does not affect much unless you are dialing an operator in a foreign country

To dial an operator in a foreign country, you must first obtain the operator routing from rate & route for that country. Dial rate & route and if you're trying to get an operator in Yugoslavia, say nicely, "IOTC Operator's route, please, for Yugoslavia." [In larger countries it may be necessary to specify a city]. Rate & route will respond with, "38 plus 11229". So, dial your over-seas gateway, KP+011+038+ST, wait for sender dial tone, and key KP+0+38+ 11029+ST. You should then get an operator in Yugoslavia. Note that you must prefix the country code on the sender with a 0 because presumably only an operator here can dial an operator in a foreign country.

When you dial KP+011+CC+ST for an overseas gateway, it is translated to a 3-digit sender code of the format 18X, depending on which sender is designated to handle the country you are dialing. The overseas$gateways and their 3-digit codes are listed below.

182 ..... White Plains, NY
183 ..... New York, NY
184 ..... Pittsburg, PA
185 ..... Orlando, FL
186 ..... Oakland, CA
187 ..... Denver, CO
188 ..... New York, NY

Dialing KP+182+ST would get you the sender in White Plains, and KP+183+ST would get the sender in NYC, etc., but the KP+011+CC+ST is highly suggested (as previously mentioned). To find out what sender you were routed to after dialing KP+011+CC+ST, dial (at int'l dial tone): KP+0020000+ST.

If you have difficulty in reaching a sender, call rate and route and ask for a numbers route for the country you're dialing. Sometimes, KP+011+ padded country code+ST will not work. I have found this in many 3-digit country codes. Lexembourg, country code 352, for example, should be KP+011+352+ST theoretically. But it is not. In this case, dial KP+011+ 003+ST for the overseas gateway. If you have trouble, try dialing KP+00+ first digit of country code+ST, or call rate The IOCC.

Sometimes when"you call rate and route and ask for an "IOTC numbers route" or "IOTC operators route" for a foreign country, you will get something like "160+700" (as in the case of the Soviet Union). This means that the country is not dialable directly and must be handled through the International Overseas Completion Centre (IOCC). For an IOCC routing, pad the country code to the RIGHT with zeros until it is 3 digits. Then KP+160 is dialed, plus the padded country code, plus ST.

Examples:

The U.S.S.R. (7) ..... KP+160+700+ST
Japan (81) ..... KP+160+810+ST
Uraguay (598) ..... KP+160+598+ST

You will then be routed to the IOCC in Pittsburg, PA, who will ask for country, city, and number being dialed. Many times they will ask for a ringback [thanks to Telenet"Bob] so have a loop ready. They will then place the call and call you back (or sometimes put you through directly). Some calls, such as to Moscow, take several hours.

The Rate Quote System (RQS).

The RQS is the operator's rate/quote system. It is a computer used by TSPS (0+) operators to get rate and route information without having to dial the rate and route operator. In Part ii, I discussed getting an inward routing for dialing-assistance and emergency interrupts from the rate and route

operators (KP+800+141+1212+ST). The same information is available from RQS. Say you want the inward routing for 305-994. You would sieze a trunk and dial KP+009+ST (to access the RQS). Sometimes, if you seize a trunk in an NPA not equipped with RQS, you need to dial an NPA that is equipped with RQS first, such as 303. Anyway, after you dial KP+009+ST or KP+303+009+ST, you will receive a wink (<beep><kerchink>) and then RQS dial tone. At RQS dial tone, for an inward routing for 305-994 you would dial KP+06+305+994+ST. That is, KP+06+NPA+exchange+ST. RQS will respond with "305 plus 033 plus". This means you would dial KP+305+033+121+ST for an inward that services 305-994. If no special routing were required, RQS would have responded with "305 plus" and you would simply dian: KP+305+121+ST for an inward.

Another RQS feature is the echo feature. You can use it to test your blue box. Dial RQS (KP+009+ST) and then key KP+07+1234567890+ST. RQS will respond with voice identification of the digits it recognized, between the KP+07 and ST.

RQS can also be used for rates and directory routings, but those are seldom needed, so they have been omitted here.

Simple Scanning.

If you're interested in scanning, try dialing on a trunk, routings in the format of KP+11XX1+ST. Begin with"11001 and scan to 11991. There are lots of interesting things to be found there, as Doctor Who (413 area) can tell you. Those 11XX1 routings can also be prefixed with an NPA, so if you want to scan area code 212, dial KP+212+ 11XX1+ST.

There, now you know as much about blue boxing as most phreaks. If you read and understand the material, and put aside preconceived ideas of what blue boxing is that you may have aquired from inexperienced people or other bulletin boards, you should be well on you way to an enlightening career in blue boxing. If you follow the guidelines in Part i to box, you should have no problem with the fone company. Comments made by "phreaks" on bulletin boards that proclaim "tracing" of blue boxers are nonsense and should be ignored (except for a passing chuckle).

NOTE 1: CCIS and the downfall of blue boxing.

CCIS stands for Common Channel Inter-office Signalling. It is a signalling method used between electronic switching systems that eminiates the use of 2600Hz and 3700Hz"supervisory signals, and MF pulsing. This is why many places cannot be boxed off of; they employ CCIS, or out-of-band signalling, which will not respond to any tones that you generate on the line. Eventually, all existing toll equipment will be upgraded or replaced with CCIS or T-carrier. In this case, we'll all be boxing with microwave dishes. Until then (about 1995 by current BOC/AT&T estimates), have fun!

If you have ANY questions about this text, please feel free to drop me a line. I will respond to anl mail, messages, etc. Insults are also welcomed. And if you discover anything interesting scanning, be sure to let me know.

Mark Tabas
LOD

This text was prepared in full by Mark Tabas for:

K.A.O.S.
Philadelphia, PA.
[215-xxx-xxxx].

Technical acknowledgements:

Karl Marx, X-Man, High-Rise Joe, Telenet Bob, Lex Luthor, TUC, John Doe, Doctor Who (413 area), The Tone Sweep, Mr. Silicon, K00L KAT, The Glump.

References:

1. Notes on the BOC Intra-LATA Networks
   Bell System publication, 1983.
2. Notes on the Network
   Bell System publication, 1983.
3. Engineering and Operations in the
   Bell System
   Bell System publication, 1983.
4. Notes on Distance Dialing
   Bell System publication, 1968.
5. Early Medieval Architecture.

.....

.....

Call 1-305-xxx-xxxx now.

Go To Part 1
Go To Part 2

```
/-/-/-/-/-/-\-\-\-\-\-\
<:-\-Brown Box Plans-/-:>
 \-\-\-\-\-\-/-/-/-/-/-/
```

(>Introduction<)

This is a fairly simple modification that can be made to any phone. All it does is allow you to take any 2 lines in your house and create a party line. So far I have not heard of any problems with it from my friends that have set one up and I ha

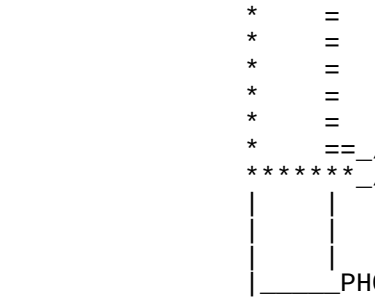
I think that the convenience of having two people on line at any one time will make up for the minor volume loss.

(>Phone Modification Instructions<)

Here is the diagram:

KEY:

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



In some houses the black and yellow are already wired in others you will have to go out to your box and rewire it. A good way to figure out which line is which is to take the phone you are looking for off the hook. Then you only need to take the red and green wires entering your phone and hook them to the different pairs of red and green going into the house. You can't hurt anything in the phone or telephone by probeing. When you find the pair that you want take the black from your line and attach it to the red of the other line then take the yellow and attach it to the green line. Now you are all set to go. For people with rotary phones you can have one person call you then place the second call out to the other person. Though not phreakers tool, the brown box can be phun.

-END-

```
 @!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@
  !@@!
  @!!@
  !@@!
  @!  The Bud Box  !@
  !@  -----------  @!
  @!!@
  !@@!
  @! Revision 1.0  !@
  !@By: Dr. D-Code & The Pimp@!
  @!   Of The High Mountain Hackerz    !@
  !@ HMH Inc. AE line.....xxx-xxx-xxxx @!
  @! HMH Inc. CS/CF.......xxx-xxx-xxxx !@
  !@  Both lines 10 megz and 2 drives  @!
  @!  AE password.....BOMB   !@
  !@@!
  @!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@!@
```

Necessary Materials

Four alligator clips
One Telephone
Some telephone wire

Instructions
----

1) Find a neighbor's house that has a little gray box on the side. This box should have a Bell logo on it (the gay little bell in a circle).

2) Apply pressure underneath the box and the front should come right off. Pull the end off of the length of the telephone wire. Then strip the ends of all the different colored wires inside. These should be green, red, yellow and black. Attach an alligator clip to each of the wires. Then clip the clips to the same colors in the box. Yellow to yellow, red to red and so on.

3) Then run the wire across the street back to your house and then plug a phone into the other end of the wire.
4) Now you can dial out and receive the neighbors calls. Great for tapping the phones and then blackmailing them. You can also stop phreaking because any outgoing calls will be charged to the neighbors!   Great eh?

All sysops may use these plans if they do not change them in any way at all.

- The Marshals of Dynamic Discord -
- Present -

The Chartreuse Box (or any other obnoxious color)

- By: Wonko The Sane -

Intro

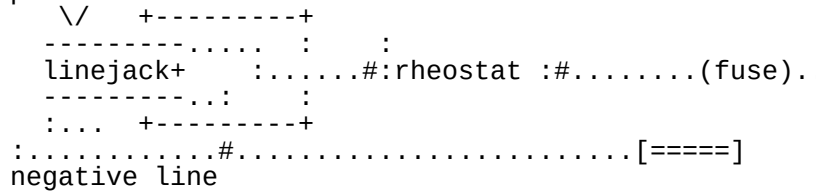
The Chartreuse Box, so named because this is an obnoxious box and chartreuse is an obnoxious color, is designed to take advantage of the thousands of dollars Ma Bell pays to the electric company each day. As you know, your telephone line is a constant power source. The chart box is designed to allow you to tap that power source for whatever sicko purposes you might have in mind.

Parts

[1]- 1 four prong to modular phone adapter (the rectangular beige boxes with phone line jacks at one end and four prongs out the other.)
[2]- 1 low power broad range rheostate.
[3]- some wire
[4]- a soldering iron
[5]- some electric tape
[6]- a 70 vlt. DC fuse (optional)
[7]- 1 SPST switch

Assembly

Plug the adapter into a phone line, and use a multitester to note which posts are charged. Use a magic marker to mark the positive and negative poles. Do this first.
Take the adapter, and turn it upside down. You should observe that the bottom fits into the top. Use a pocketknife, small screwdriver, battle axe etc. to remove the bottom. Don't break it.
Detach the two wires not connected to charged poles, and scrap em. Detach the other two wires as well. Take your rheostat, and mount it on the outside of the box, drilling a small hole in the box, to run wires through.
Run wire from the charged connections from the line jack, through the rheostat, to the charged poles. (see diagram).



Key: # - Rheostate poles
. - Wiring path
[=]- Outside posts

Attach the fuse somewhere in the line if you feel like it.
When the phone rings 90 volts of pulsing DC power get shot down

your line, and can really fuck up whatever you have the chart box hooked up to. Therefore, the fuse is a good idea.
You can also hook a switch up to the wiring, to give you more control over when power starts to flow. Once all the wiring is complete, push the wires and the fuse into the casing, and reclose it. Then tape around the side of the box, to hold the wires that come out to the rheostat down. I highly recommend that you mark the charged posts with a marker, so you can easily identify them.

Use

To use the chart box, hook it up to a phone line, and grab a multitester or voltmeter. Use the voltmeter to read off the voltage from your chart box. You can get up to 12 volts (more if you use a transformer) from the box, but you can use the rheostat to calibrate the box for whatever voltage you need. Once the voltage is set, remove the box from the line, hook your device up to the charged poles, and plug the box back in. If you're really in a constructive mood, build a switch into the box. Now leech Ma Bell's precious energy to your hearts content.

Footnote

This device has other potential uses. One of the most obvious, and least useful (at least to my view) is as a volume control for your phone. Maybe you have an aunt that talks REAL LOUD!!!!! Also, you can use this device to set up a feedback loop to mess up someone else's phone line. Finally, it may be possible to use the chart box to tone down your connection, and provide a little background noise, so that ESS doesn't pick up on your blue boxing. This is not a guaranteed method, but if you do it just right, you can make the 2600 blast sneak by the ESS detection code.
Naturally, the main purpose of the chart box is to leech Ma Bell just like she leeches you.

Hail Discordia!

Naturally, the main purpose of the chart box is to leech Ma Bell!

$$$$$$$$$$-=>Making Your Phone<=-$$$$$$
$$$$$$$$$$-=>Into a Cheesebox <=-$$$$$$

/=\Typed by:Sir Knight/=\

A Cheesebox(named for the type ofbox 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 Inter-cept 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 gener- ate 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 phoneand not get traced...

```
  \ \ \ \ \ \ \ \ \ \ \ \ \ \
  \[_____________________________[_    \  /
  \[ The Chrome Box   [_A Portable Self-Contained Device
  \[   14-JUN-88 [_    /  to Manipulate Traffic Signals \
  \[   Outlaw Telecommandos[_ /by Remote Control  \
  \[Modem Free Earth  [_ /  \
  \[\\\\\\\\\\\\\\\\\\\\\\\\\\\\\[_  -=p*p=-
```

Emergency vehicles in many cities are now using devices called OptoComs.

OptoComs are a system of sensors on traffic lights that detect a pattern of flashes from vehicle-mounted strobe lights.

This flash pattern varies from city to city depending on the manufacturer of the equipment used. Often the sensors are installed only at major intersections. Nevertheless, the Chrome Box, which simulates these strobe patterns can often be used to give your car the same priority as an ambulance, paramedic van, firetruck or police car.

Because of the varying patterns on different systems this phile will outline a general procedure for making the Chrome Box.

Decoding Flash Patterns:

First, you need to observe an emergency vehicle in action. You can wait until you encounter one by chance, running out to see when you hear a siren, or when you pull over in your car to let one pass by. You might wait near a fire station for the next emergency to occur. Or, if you are very impatient, you can summon one by calling in a false alarm (not recommended in areas with limited services - that could divert attention from a real emergency). If the OptoComs in your area are the kind with a pattern of single flashes at a steady rhythm, you have merely to buy a strobe light at Radio Shack & adjust the flash rate until you can induce a traffic light to change.

If the flash pattern is more complex, you can videotape the emergency vehicle & then play back the tape in single-frame mode, counting the number of frames between each flash. Each video frame is 1/30 of a second, using this you can calculate the time between flashes in the pattern. Another way is to count the number of flashes (or flash-groups) in one minute and use that to compute the rate. Counting video frames will give you a good idea of the spacing of the flashes in a complex pattern. For really accurate information, call the fire station & ask them, or write to the manufacturer for a service manual, which will include a schematic diagram that you can use to build one. A good cover story for this is that you are a consultant &

one of your clients asked you to evaluate Optocom systems, or you could pose as a free-lance journalist writing an article.

Modifying the Strobe Light:

You may not have to modify the strobe at all. But if you need a faster flash rate than your strobe allows, open it up & find the large capacitor inside. Capacitors are marked in microfarads, abbreviated as mf,mfd or ufd. By replacing the capacitor with one of the same voltage-rating (usually 250 volts or more) and a SMALLER value in microfarads, you can increase the flash rate. Halving the microfarads doubles the rate.

The other component that can be changed is the potentiometer (the speed control device with the knob on it). Using a smaller value (measured in ohms or Kilohms, abbrevaited with the greek letter 'omega' or the letter K) will speed up the strobe. There may also be a resistor (small cylinder with several colored stripes on it, and wires coming out of each end). Replacing this resistor with one of smaller value will also speed up the strobe.

To generate a complex pattern, you will either have to design and build a triggering circuit using IC chips, or rig up a mechanical device with a multiple-contact rotary switch and a motor. It HAS been done.

To modify the strobe for mobile operation the simplest thing is to get a 110-volt inverter that will run off of a car battery by plugging into the cigarette lighter & run the strobe from that. Or, you can figure out (or find in a hobby electronics magazine) a strobe circuit that will run from batteries.

Battery-powered strobes may also be availble, either assembled or as kits.

Stealth Technology:

Most light sensors and photocells are more sensitive in the infrared area of the light spectrum. Infrared (IR) is invisible to the human eye. Putting an infrared filter over the strobe light may allow the Chrome Box to operate in traffic undetected by police or other observers. IR filters can be obtained from military surplus sniperscope illuminators, or from optical supply houses like Dow-Corning or Edmunds Scientific Co.

Using the Chrome Box:

Mounted on your car, the Chrome Box can guarantee you green lights at major intersections in cities that have OptoComs. Handheld Chrome Boxes may be used to create gridlock by interfering with the normal flow of traffic. If

you have access to a window overlooking a traffic light, you can play pranks
by switching the signals at inappropriate moments, or you can plug the strobe into an exposed outlet at a laundromat or gas station.

Some Decoded Patterns:

Torrance, California
Standard large Radio Shack strobe lights are used. Moderately fast rate.
* * * * * * * *

Manhattan Beach,CA
Flash-pairs in a 4:1 ratio, at a rate of 2 flash-pairs per second.
* * * * * * * *
<------ 1 sec ----->

****
* Please add any new patterns or info you discover to this Phile *
****

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 dont require payment until after the connection is established. You pick up the fone, get a dial tone, dial your number, and then insert your money after the person answers.If you dont deposit the money then you can not speak to the person on the other end- because your mouth peice 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 ould be plugged into the out- put of the amplifier and a microphone would be hooked to the input. So when the party that is being called answers, the caller could speak through the little microphone instead. His voice then goes through the amplifier and out the induction coil, and into the back of the reciever where it would then be broadcast through the phone lines and the other party would be able to hear the caller. The Clear Box thus 'clears up' the problem of not being heard. Luckily, the line will not be cut-off after a certain amount of time because it will wait forever for the coins to be put in.The biggest advantage for all of us about this new clear box is the 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 doesnt require any special equipment, (for the phone company)This payphone will work on any phone line. Ususally a payphone line is different, but this is a regular phone line and it is set up so the phone does all the charging, not the company.

CLEAR BOXING

The idea for the Clear box comes from an article in the newsletter 2600.

The clear box works on 'post pay' coin phones, pay phones that require money only after the connection has been made. The way this works is: After the connection is made the mouthpiece of the phone is muted but not the earpiece, free calls to dial-it services can be made with these phones.

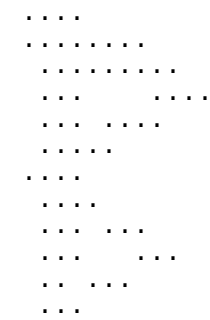
In order to talk to the person you called without paying (NOTE: It is against the law to do this!!) Take yourself down to your nearby electronics store and get a four transistor amplifier and a telephone suction cup inductive pick-up. Put the pick-up on the earpiece and plug it into the output of the amplifier, and plug a microphone into the input. You then talk into your microphone and listen normally through the earpiece.

Radio Shack sells an item that wont need much modification,and that should work the same as the above construction. It is their 'Portable snap-on handset amplifier' (Part # 43-238) Their description says to put it on the earpiece and it will boost the callers voice to five times the normal level.
In order to make this function like a clear box one would have to take the amplifier apart and remove the internal speaker, in it's place, connect the suction cup inductive pickup. Place the pick-up (which is now the speaker) to the earpiece of the payphone, and talk into the microphone of the amplifer.

The line will not cut off, and will wait forever for you to put the coins in.
Note also that these types of payphones are not connected to the TSPS in the same way as normal payphones. The phone does all the charging and not the Central Office. It is because of this, that a phone connected to the lines BEFORE the payphone would act just like a normal phone. So get out your smallest phone, cut off the jack and strip the wires. connect the wires to two alligator clips. Then you can clip onto the payphone's wires BEFORE they connect to the payphone, you then have a normal telephone line that you dont pay the bills on!

R e n e g a d e L e g i o n
T e c h n i c a l R e p o r t s

Technical Report #2



February 1991

Report Number: 4.0

COCOTS: Uses for privatly operated public telephones. How to make free calls
use their maintenance features, and plans for a tone dialer to fool COCOT security systems.

Compiled : 03/25/91
Author : Count Zero
System : COCOT Payphones
Uses: Free calling to most of the world