

## [In This Issue]

Intro Stuff // blakmac

The Little Brother Box // subterphuge

Wal-Mart Calling Cards – Avoiding the Payphone Surcharge // blakmac

Legacy – Satellite Systems: Reception // Black Axe

The Old Code

Letters

Linkage

## [Staff Members]

blakmac - editor in chief, webmaster

diversereality - resident genius, penetration specialist

Intro Stuff // blakmac [page33@mail.com]

Yes, we are back. I never thought I'd see the day when I could generate one, let alone three issues of a zine. Sadly, I'm still having to use old texts to fill out a decent size issue. We still need articles for both the zine and the website. As a matter of fact, we need some people on staff. Speaking of old texts, I've decided to add a new section to the zine called Legacy. In this section we will be featuring something older for your reading enjoyment. This time around, we are featuring an article from Phone Punx Magazine on satellites. It's interesting, really.

As of now, our tentative "to-do list" has several items on it, including a possible site re-design, finishing some rather lengthy articles that I am working on, finding new talent both for staff members and writers, as well as becoming better at doing the layout for this thing. I want it to look more like 2600 or Dig, but it's going to take a little bit of time. Also I suppose I need to find a good template for PageMaker, since I'm really not very good with it yet. (I'm digressing. Sorry.)

I have been toying with the idea of making some flyers to advertize the zine and site, as lots of other zines have done before. I'm not the most gifted when it comes to graphic design, so if anybody has any ideas and/or wants to help with

this, please let us know. Readership is important to any zine, and we will do lots of stuff (some of which may be very stupid) to get readers. I'm also considering taking out an ad in 2600, just to get a boost. Also, thanks to Majestic for linking me on his site, datutoday.tk, which is a great site (everyone should check it out).

Another wild idea has surfaced in my mind. Actually, this one happened quite some time ago. It would be nice to have some kind of conference in the Houston area. I know that there are some good ones out there, but for some of us, it's not that easy to just go to New York or Las Vegas, let alone overseas. And I realize that not everybody lives in the Houston area, but I do. Lots of us do. And almost everybody that I know around here would love to go to a big hacker conference, but can't for some reason or another. Ok, here's the deal – it would be cool if we (as a group, all of us) could brainstorm and think of ideas for setting up a conference around here.

Well, I think I've said enough for now. I'll leave you to digest this issue. We aren't responsible for the nausea, vomiting, and/or lower intestinal discomfort you may experience. Enjoy.

send articles/emails to:  
page 33 at mail dot com

Little Brother Box // subterphuge  
Dialup/POTS Data Interceptor  
Copyleft 1999 by Subterphuge  
All Wrongs Reserved.

>>>> A Dialup/POTS Modem Data Interception "Grey" Paper <<<<

Here's what you'll need:

(a) TWO MODEMS (internal highly recommended for covert operations)

- they \*must\* mute the "PHONE" jack once modem goes off-hook.

- you'll be limited to the lowest common demominator speed for throughput -- but faster modems than the target are sometimes handy for speedy remote downloading of captured logs.

(b) ANY SYSTEM BOX (old IBM-PC used throughout this doc for brevity)

- self-contained portables/laptops/lunchboxes recommended for covert operations, with either a single power cable connected

- to a power source, or (if appropriate) battery operations.

- you'll want enough disk space (either physical, or better

- yet RAM disk in case the box is compromised) to store data capture

- sessions, unless you program the control software to only log data after key phrases and capture only relevant data.

(c) CONNECTIVITY (RJ-11)

- custom-length phone cords to meet your requirements, small 3-inch cords are recommended for the modem-to-modem link.

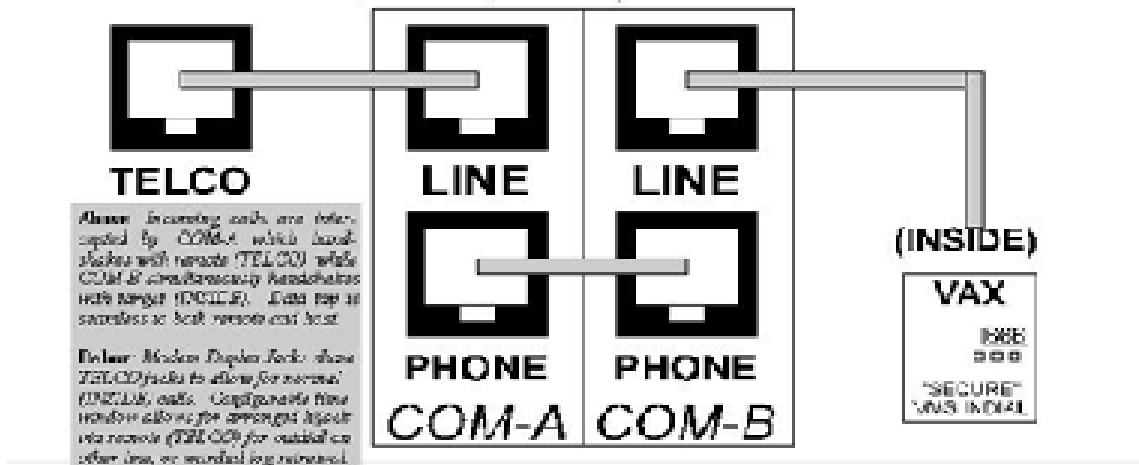
- any beige-box alligator-clip/wire jobs you may need for the particular situation -- you'll want an RJ-11 "lesbian" adapter

- or a female terminated cord for most newer telco interfaces, to connect to the male ("inside") plug on the target side.

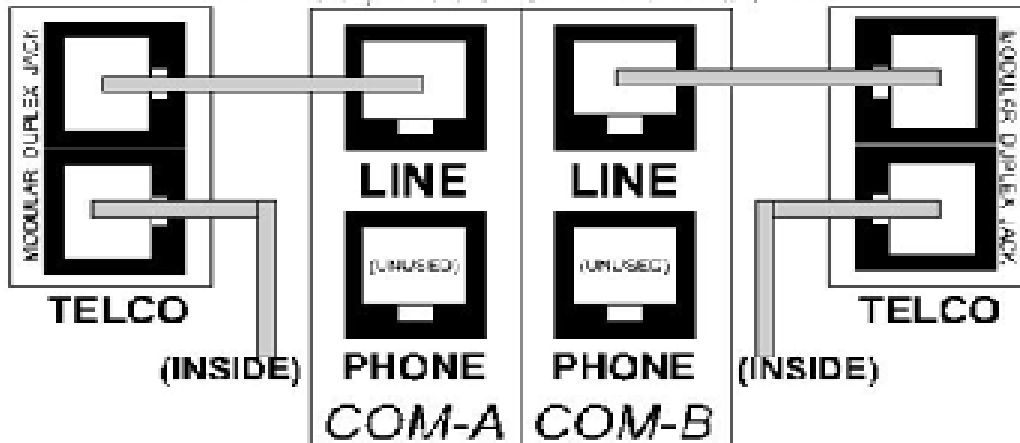
The following diagram should help:

# LITTLE BROTHER BOX

## DATA TAP SCHEMATIC



## OUTDIAL/WARDIAL SCHEMATIC



NOTE: It is imperative that you set up your wire connections this way and include the connector between the two VOICE/PHONE (as opposed to the TELCO/LINE) jacks on the modems. This is so that the incoming ring signal can be bypassed to the target without extra/special hardware being required, and so that those same jacks are also muted once the connections are being made, so that COM1 doesn't interfere with COM2, and vice versa.

I leave it to you to be clever enough to implement any beige wire connections on the TELCO or TARGET ends, if necessary. Most modern telco junction boxes have RJ-11 connectors though, so all you'll need is just normal phone cord, and probably an RJ-11 "lesbian" adapter or cord that is female-terminated on one end to connect to the plug. Usually, the female port on the junction boxes leads to the telco, and the male leads to inside of the target building/structure. You should always verify the telco side either by using a line tester LED indicator or just verifying a dial tone by connecting up a beige box.

If you haven't figured out the logistics of how it works yet, don't worry. Its devilishly simple. The key to it all is the software.

Just make sure you have the hardware setup down pat, and read on. The software should be able to support the following "features", outlined in brief:

- Intercept incoming call (ATA) and negotiate COM1 with remote.
- Same time make COM2 blind-dial (ATX1D) and negotiate with host.
- Once both are connected, capture user/password information to log.
- Include passworded time-window for secure remote log retrieval.

The value of running from a RAM disk is two-fold, in case your box is compromised at deployment site: 1) you don't have to worry about any incriminating data being recovered (once the power goes, the RAM is wiped); 2) you can physically remove the floppy drive after you've booted your program, saving valuable hardware from being confiscated.

Today we are looking at a flaw with the "billing" system of Wal-Mart prepaid phone cards. These cards are very handy to have in emergency situations (i.e., broken down on the highway, locked out of the house, emergency pizza delivery to a random unsuspecting person, long distance prank calling, etc.). But what happens when you run low on minutes? If you are calling from a home or office phone, you can use your last few minutes without problems. But assume for a minute that you are stranded somewhere. The problem is that Wal-Mart cards charge a 9-minute surcharge when calling from payphones. This can seriously put a damper on your calling if you have a card with a low amount of minutes to begin with. However, there is a way to avoid the surcharge, for those that are so inclined.

The solution to the problem is simple, and any decent phone phreak should be able to guess what I'm eluding to, however, this is for the newbies out there. The answer – op divert. Op diverting (for those that do not know) means using an operator (or something similar) to cause an ANI fail on the line, thereby hiding both the origin of the call and the type of line being called from. Here's the play-by-play:

First, op-divert by dialing 10-10-288-0. This connects you to

AT&T. At the prompt, enter the 800 number listed on the back of the card. It will connect you to the calling card system, which will ask you for the calling card number, and the number you are wanting to dial. If done correctly, it will connect your call without the 9-minute surcharge notification. When dialed without op-diverting, it will notify you of the surcharge and deduct 9 minutes from the account.

So far, I've had luck on SBC payphones with this technique. The local COCOTS all connect you to an Opticom operator when you try to op divert, and they will not dial the toll free number (in my experience). Perhaps a gifted social engineer could get them to comply better than I could. As a matter of fact, when I dialed 10-10-288-0 from the COCOT, instead of hearing AT&T's music, it said something like "Thank you for choosing Opticom".

Armed with this new knowledge, you can now squeeze every last minute out of Wal-Mart prepaid calling cards. I have not tested this method on other cards, but it is likely that some may have this same flaw. If anybody finds any other cards that this works on, let everybody know. Maybe a good project idea would be to purchase lots of different cards and try this trick on all of them and document the results.

#### [LEGACY]

##### Satellite Systems: Reception // Black Axe

*from: Phone Punx Magazine #2, Aug. 7, 1999*

Ever look up at the sky, and wonder what's up there? Ever watch someone's satellite TV and wonder, "gee, maybe if I turned the dial and swung the dish around a bit, I could see what else is up there.."? Hopefully, this article can help inform the reader about the most common and easily intercepted forms of satellite communication.

Before we begin, there are a few important concepts, that we must cover. If you know anything about satellites, this part should bore you. All satellites orbit the earth. Some of those satellites orbiting the earth are put into such an orbit that they appear motionless to an earth-based station; in layman's terms, they don't go anywhere. These types of satellites are referred to as geosynchronous. Other satellites will orbit the earth. Because they move in perspective to the earth-based observer, that observer must keep track of where exactly the satellite is at any given time (usually for purposes of antenna calibration). Keplerian Elements, readily available for most (non-spy) satellites, can be entered into a variety of different freeware, shareware, and commercial programs to track the satellites. Some programs can even orient your antennas or dishes for you, to get the best possible signal as the satellite moves across the horizon.

These topics having been covered, let us delve deeper into what our dishes and antennas can fish out of the cosmos.

#### **Amateur Radio Satellites**

One of the easiest types of signals to receive from space is from amateur (Ham) satellites. Most amateur satellites use uplinks and downlinks in the VHF and UHF bands, making antenna requirements easy to fulfill. Most of the time, a properly oriented telescoping whip is all that is needed. Operating modes vary; CW (Morse code) is often used. Other operating modes include SSB (Single Sideband), various digital modes, and FM voice (specifically, the AO-29 satellite). The interesting part about amateur satellites is that not only does one have the ability to listen in, but also the ability to use these satellites for their own communications. Some digital satellites even house entire BBS systems.

#### **MIR and SAREX**

One can also communicate with the Russian space station, MIR, and (at certain times) the American Space Shuttle (SAREX). Cosmonauts aboard the space station MIR operate voice and a packet (digital) system onboard in the 144-mHz amateur band. The American Space Shuttle's SAREX (Space Amateur Radio Experiment) is a more clandestine operation, consisting of a handheld radio and a window-mounted antenna. FM voice is used on a number of different frequencies in the 144mHz band. Amateur radio operators are EXTREMELY competitive in making a SAREX contact, usually just for the nice postcard (QSL) that NASA sends.

## Inmarsat

Now we delve into more of a "grey area" of satellite monitoring. The Inmarsat system consists of four geosynchronous satellites serving the entire surface of the Earth with satellite telephone service. Ridiculously expensive, Inmarsat service is generally only used by well-funded people and organizations. Some Inmarsat traffic is digital. However, there is still an abundance of voice traffic to be intercepted. Transmission mode is companded FM, meaning that signal strength varies with the noise level (used to conserve power consumption); set your squelch accordingly. To intercept Inmarsat traffic, a receiver capable of covering 1500mHz is required, along with a dish and a directional antenna (Yagi). Orient the Yagi (tuned for the band) towards the dish, and affix it to the dish's LNB. Find the satellites in the sky (this will be left as an exercise for the reader); tune the receiver to 1537mHz to find a constant signal transmitted by the satellites. Modulation mode is Narrow FM; steps of 25kHz. Have a tape recorder ready; you never know what you'll hear.

## TVRO

TVRO stands for TeleVision Receive Only. Basically, it is what is known as satellite TV. Although many pay services are common nowadays, it is still possible to intercept a great deal of analog video traffic from TVRO satellites. Basically, what is required is a TV (of course), a satellite receiver, a dish with an LNB (Low Noise Block converter), and rotors to spin the dish around. What's out there, you say? Of course, there's regular network TV, and many other less-common broadcast services. By far, the most interesting part of TVRO is "wild feeds", that is, live video being transmitted from various locations to broadcast studios. For example, during the conflict at Waco, there were four live and uncensored feeds coming out of Waco, 24 hours a day. You'll get to see all the blood and guts that are edited out of the network broadcast, along with reporters you'll recognize very well bitching before a broadcast, smoking a quick cigarette, etc. The world of TVRO is vast and ready for exploration.



## [THE OLD CODE]

*I found this program on some qBasic site. It's simple, but handy. I know there are better encryption tools out there, but hey, this is just for your enjoyment. So enjoy // blakmac*

'File Crypt v001.01.01

'by Eric McCormick

```
DECLARE SUB CT (CTEXT$)
DECLARE SUB INKEY ( )
DECLARE SUB PL (LN, TEXT$)
DECLARE SUB S ( )

' $STATIC
DIM DC(1 TO 10) AS INTEGER
DIM EC(1 TO 10) AS INTEGER
DIM FB(1 TO 10) AS INTEGER

ON ERROR GOTO ER
SCREEN 12
MENU:
CLOSE
TempFile$ = "~!@##@!~.tmp"
OPEN TempFile$ FOR BINARY AS #1
CLOSE
KILL TempFile$
FOR L = 1 TO 10
RANDOMIZE TIMER
REC = INT(RND * 500) + 1
EC(L) = REC - 255
NEXT L
ERASE FB, DC
S
CT "File Crypt Version 1.0"
PL 10, "1. Encrypt File"
PL 11, "2. Decrypt File"
PL 13, "3. Exit File Crypt"
PL 20, "Type MENU at any prompt to go to this menu."
PL 22, "File Crypt by Eric McCormick"
PL 17, "Your choice(1-4) ?"
```

```

MC$ = INPUT$(1)
IF MC$ = "1" THEN GOTO EF
IF MC$ = "2" THEN GOTO DF
IF MC$ = "3" THEN CLS : END
GOTO MENU

EF:
S
CT "Encrypt File"
PL 9, "Type the filename of the file to encrypt:"
LOCATE 10, 15: INPUT "", SourceFile$
IF SourceFile$ = "MENU" THEN GOTO MENU
OPEN SourceFile$ FOR BINARY AS #1
IF LOF(1) = 0 THEN
CLOSE
KILL SourceFile$
PL 12, "The file you have typed cannot be found."
PL 13, "Type another filename."
PL 15, "PRESS ANY KEY TO CONTINUE"
INKEY
GOTO EF
END IF
PL 12, "Type the destination filename:"
PL 21, "To write encryption to the same file,"
PL 22, "type OVERWRITE."
LOCATE 13, 15: INPUT "", DestinationFile$
IF DestinationFile$ = "MENU" THEN GOTO MENU
DCom$ = "DIFFFILE"
IF DestinationFile$ = SourceFile$ OR DestinationFile$ = "OVERWRITE" THEN DCom$ = "OVERWRITE"
OPEN TempFile$ FOR BINARY AS #2
PL 15, "Password (optional, 5-10 characters):"
PL 21, "If you want, type a password for this file"
PL 22, "which will be need upon decrypting."
COLOR 0
GETPASS:
LOCATE 16, 15: INPUT "", Pass$
IF Pass$ = "MENU" THEN GOTO MENU
IF Pass$ = "" THEN Pass = 0 ELSE Pass = 1
IF Pass = 1 AND (LEN(Pass$) < 5 OR LEN(Pass$) > 10) THEN GOTO GETPASS
COLOR 15
PL 21, " "
PL 22, " "
IF Pass = 1 THEN
PL 16, "Confirm your password:"
PL 22, "Retype your password to confirm."
COLOR 0
LOCATE 17, 15: INPUT "", Confirm$
COLOR 15
IF Confirm$ = "MENU" THEN GOTO MENU
IF Pass$ <> Confirm$ THEN PL 21, "Passwords don't match. Try again.": PL 22, "PRESS ANY KEY TO CONTINUE"
": INKEY: CLOSE : GOTO EF
IF LEN(Pass$) <> 10 THEN AddOn$ = MID$(Pass$, 1, 10 - LEN(Pass$)): Pass$ = Pass$ + AddOn$
END IF
PL 22, " "
PL 19, "Encryption in progress....."
PL 21, "File Size: " + LTRIM$(STR$(LOF(1))) + " bytes"
IF Pass = 1 THEN
FOR L = 1 TO 10
EC(L) = ASC(MID$(Pass$, L, 1))
NEXT L
END IF
FP& = 0: L = 1
DO
A$ = " "
GET #1, , A$
ASCV = ASC(A$)
IF ASCV + EC(L) > 255 THEN A$ = CHR$((ASCV + EC(L)) - 256): GOTO BYE
IF ASCV + EC(L) < 0 THEN A$ = CHR$((ASCV + EC(L)) + 256): GOTO BYE
A$ = CHR$(ASCV + EC(L))
BYE:
IF FP& >= 0 AND FP& < 10 THEN FB(L) = ASC(A$)
PUT #2, , A$
IF L = 10 THEN L = 0
L = L + 1
FP& = FP& + 1
IF FP& / 250 = INT(FP& / 250) THEN LOCATE 22, 15: PRINT "Encrypted: "; FP&; "bytes"
LOOP UNTIL FP& = LOF(1)
IF Pass = 1 THEN A$ = "=PASSWORD ACCESS $$ ": PUT #2, , A$
IF Pass = 0 THEN
FOR L = 1 TO 10
ASCSAV& = (FB(L) + (-EC(L) + FB(L)) - (EC(L) + 1))

```

```

LT = 100
DO
IF ASCSAV& > 255 THEN ASCSAV& = ASCSAV& - 256: LT = LT + 1
IF ASCSAV& < 0 THEN ASCSAV& = ASCSAV& + 256: LT = LT - 1
IF ASCSAV& >= 0 AND ASCSAV& <= 255 THEN EXIT DO
LOOP
A$ = CHR$(ASCSAV&) + CHR$(LT)
PUT #2, , A$
NEXT L
END IF
LOCATE 22, 15: PRINT "Encrypted: "; FP&; "bytes"
CLOSE
IF DCom$ = "DIFFFILE" THEN
OPEN DestinationFile$ FOR BINARY AS #1
CLOSE
KILL DestinationFile$
NAME TempFile$ AS DestinationFile$
END IF
IF DCom$ = "OVERWRITE" THEN
KILL SourceFile$
NAME TempFile$ AS SourceFile$
END IF
PL 19, "Encryption successful!           "
INKEY
GOTO MENU

DF:
S
CT "Decrypt File"
PL 9, "Type the filename of the file to decrypt:"
LOCATE 10, 15: INPUT "", SourceFile$
IF SourceFile$ = "MENU" THEN GOTO MENU
OPEN SourceFile$ FOR BINARY AS #1
IF LOF(1) = 0 THEN
CLOSE
KILL SourceFile$
PL 12, "The file you have typed cannot be found."
PL 13, "Type another filename."
PL 15, "PRESS ANY KEY TO CONTINUE"
INKEY
GOTO DF
END IF
PL 12, "Type the destination filename:"
PL 21, "To write decryption to the same file,"
PL 22, "type OVERWRITE."
LOCATE 13, 15: INPUT "", DestinationFile$
IF DestinationFile$ = "MENU" THEN GOTO MENU
DCom$ = "DIFFFILE"
IF DestinationFile$ = SourceFile$ OR DestinationFile$ = "OVERWRITE" THEN DCom$ = "OVERWRITE"
OPEN TempFile$ FOR BINARY AS #2
PL 21, "           "
PL 19, "Decryption in progress....."
FOR L = 1 TO 10
A$ = " "
GET #1, , A$
FB(L) = ASC(A$)
NEXT L
A$ = "           "
GET #1, LOF(1) - 19, A$
IF A$ = "=PASSWORD ACCESS $$ " THEN Pass = 1 ELSE Pass = 0
IF Pass = 0 THEN
FOR L = 1 TO 10
A$ = " "
GET #1, (LOF(1) - 21) + (L * 2), A$
DC(L) = (((ASC(MID$(A$, 1, 1)) + ((ASC(MID$(A$, 2, 1)) - 100) * 256) + 1)) - (FB(L) * 2)) / -2
NEXT L
END IF
CLOSE #1
IF Pass = 1 THEN
PL 15, "Password:"
PL 21, "This file requires a password to decrypt "
PL 22, "it. Type the password now.           "
COLOR 0
NEEDPASS:
LOCATE 16, 15: INPUT "", Pass$
IF Pass$ = "MENU" THEN GOTO MENU
IF LEN(Pass$) < 5 OR LEN(Pass$) > 10 THEN GOTO NEEDPASS
COLOR 15
PL 21, "           "
PL 22, "           "
PL 16, "Confirm your password:"

```

```

PL 22, "Retype your password to confirm."
COLOR 0
LOCATE 17, 15: INPUT "", Confirm$
COLOR 15
IF Confirm$ = "MENU" THEN GOTO MENU
IF Pass$ <> Confirm$ THEN PL 21, "Passwords don't match. Try again.": PL 22, "PRESS ANY KEY TO CONTINUE"
": INKEY: CLOSE : GOTO DF
IF LEN(Pass$) <> 10 THEN AddOn$ = MID$(Pass$, 1, 10 - LEN(Pass$)): Pass$ = Pass$ + AddOn$
FOR L = 1 TO 10
DC(L) = ASC(MID$(Pass$, L, 1))
NEXT L
END IF
PL 22, " "

OPEN SourceFile$ FOR BINARY AS #1
PL 21, "File Size: " + LTRIM$(STR$(LOF(1) - 20)) + " bytes"
FP& = 0: L = 1
DO
A$ = " "
GET #1, , A$
ASCV = ASC(A$)
IF ASCV - DC(L) > 255 THEN A$ = CHR$((ASCV - DC(L)) - 256): GOTO BYD
IF ASCV - DC(L) < 0 THEN A$ = CHR$((ASCV - DC(L)) + 256): GOTO BYD
A$ = CHR$(ASCV - DC(L))
BYD:
PUT #2, , A$
IF L = 10 THEN L = 0
L = L + 1
FP& = FP& + 1
IF FP& / 250 = INT(FP& / 250) THEN LOCATE 22, 15: PRINT "Decrypted: "; FP&; "bytes"
LOOP UNTIL FP& = LOF(1) - 20
LOCATE 22, 15: PRINT "Decrypted: "; FP&; "bytes"
CLOSE
IF DCom$ = "DIFFILE" THEN
OPEN DestinationFile$ FOR BINARY AS #1
CLOSE
KILL DestinationFile$
NAME TempFile$ AS DestinationFile$
END IF
IF DCom$ = "OVERWRITE" THEN
KILL SourceFile$
NAME TempFile$ AS SourceFile$
END IF
PL 19, "Decryption successful! "
INKEY
GOTO MENU

ER:
CLOSE
S
PL 7, "File Crypt has performed an illegal operation"
PL 8, "and will be restarted."
PL 10, "Error " + LTRIM$(STR$(ERR)) + " at line " + LTRIM$(STR$(ERL)) + " ."
INKEY
RUN

SUB CT (CTEXT$)
LOCATE 7, 41 - (LEN(CTEXT$) / 2): PRINT CTEXT$
END SUB

SUB INKEY
DO: LOOP WHILE INKEY$ = ""
END SUB

SUB PL (LN, TEXT$)
LOCATE LN, 15: PRINT TEXT$
END SUB

SUB S
CLS
PAINT (0, 0), 1
LINE (100, 80)-(540, 360), 4, B
LINE (99, 81)-(541, 359), 4, B
LINE (98, 82)-(542, 358), 4, B
LINE (97, 83)-(543, 357), 4, B
LINE (96, 84)-(544, 356), 4, B
LINE (101, 85)-(539, 355), 0, BF
END SUB

```



[LETTERS]

---

-----  
I have read alot on phreaking and phone systems and don't know where to start i think i read to much and am confused i really wanna know and do much help please

joanix

*Ah! Our first letter! I know everybody hears questions like this all the time, and most of the responses are generally in the style of something derogatory. It sounds like you have a desire to actually learn, but one thing is for sure, you can NEVER read too much. Keep in mind that it takes not only reading, but experimenting. Also, it would help to get in with some people in your area that share your interests. Also, be aware that Google is your friend. Odds are if you want to learn something, it's probably out there.*

---

Please remove my number from your call database. 301-675-2458.

Thank you

J Mertz

*Um...that number isn't in our call database, so it cannot be removed. Sorry for the inconvenience.*

---

[LINKAGE]

This section is where we will add links that we find very worthy of perusal by the masses. Feel free to submit your links too. If we like them, odds are they will end up here. Enjoy.

**<http://www.telcodata.tk>** // Home of the famous NPA.php!

**[bbs.icecastle.com](http://bbs.icecastle.com)** // A BBS that I get on occaisionally. Based in Houston.

**<http://www.gbppr.org>** // Green Bay Professional Packet Radio. They don't like alot of people, but they are intellegent.

[END NOTES]

Thanks: Majestic (for the linkage), lowtec (for the good advice)

Disclaimer // The information contained in this magazine is protected by the first amendment of the Constitution of the United States. It is intended for educational use only. We do not endorse illegal activities. We do not take any responsibility for the misuse of any information contained herein. May contain peanuts.

Article Submission // We will review all articles submitted. Please email them in plaintext to [topage33@mail.com](mailto:topage33@mail.com). Alternately, you can send us a link to your article, and we will review it. Articles should be related to hacking, phreaking, programming, and any other technical information. Please don't bother submitting rants, they will not be printed. Any articles not used in the zine may be used on the site at our discretion.

Releases // Page 33 has no set release dates currently. Please check the website for the latest releases. Our target is one issue every 2-4 months for now, however we cannot guarantee this. The more articles we receive, the faster the issues will roll out.

Distribution // Feel free to mirror our zine archive on your website, but please post a link to our main page at <http://page33.port5.com>, or <http://www.page33.tk>. Feel free to print out hardcopy (use the .doc files for best results) and distribute them as desired.

Copyright 2004 Page 33. Individual articles are are property of the author and used with permission. Please feel free to distribute this zine, but please do not modify any of the articles. It's a free zine, so please don't charge more than the cost of reproduction. You may reprint these articles either in another zine or on your website, but please let us know.

[<http://page33.port5.com>]

[[page33@mail.com](mailto:page33@mail.com)]

