===== Phrack Magazine presents Phrack 16 =====
===== File 1 of 12 : Phrack 16 Intro =====

Greetings, and welcome to Phrack #16, we are a bit late, but bigger then ever. I think you will find this issue very interesting. Enjoy and have Phun

Elric of Imrryr - Editor

Contents this issue:

Submission to Phrack may be sent to the following BBSes:

| | | | |
|---|---|---|---|
| Unlimited Reality | 313-489-0747 | Phrack | |
| The Free World | 301-668-7657 | Phrack Inc. | (*) |
| The Executive Inn | 915-581-5145 | Phrack | |
| Lunatic Labs UnLtd. | 415-278-7421 | Phrack | (*) |
| House of the Rising Sun | 401-789-1809 | Phrack | |

* You will get the quickest reply from these systems.

#### PHRACK PRESENTS ISSUE 16 ####
^*^*^*^Phrack World News, Part 3^*^*^*^
**** File 10 of 12 ****

[Ed's Note: Certain names have been change in the article to protect the author]

## The Flight of The Mad Phone-Man's BBS to a Friendly Foreign Country

Using my knowledge that the pigs grab your computer when they bust you,I got real worried about losing a BIG investment I've got in my IBM. I decide there's a better way.... Move it! But where? Where's safe from the PhBI? Well in the old days, to escape the draft, you went to Canada, why not expatriate my board.... Well the costs of a line are very high, let's see what's available elsewhere.

One afternoon, I'm working at a local hospital,(one I do telecom work for) and I ask the comm mgr if they have any links to Canada? He says why yes, we have an inter-medical link over a 23ghz microwave into the city just across the border. I ask to see the equipment. WOW! My dreams come true, it's a D4 bank (Rockwell) and it's only got 4 channel cards in it. Now, being a "nice" guy, I offer to do maintenance on this equipment if he would let me put up another channel...he agrees. The plot thickens.

I've got a satellite office for a business near the hospital on the other side, I quickly call up good ole Bell Canada, and have them run a 2 wire line from the equipment room to my office. Now the only thing to get is a couple of cards to plug into the MUX to put me on the air.

A 2 wire E&M card goes for bout $319, and I'd need two. Ilook around the state, and find one bad one in Rochester.... I'm on my way that afternoon via motorcycle. The card is mine, and the only thing I can find wrong is a bad voltage regulator. I stop by the Rockwell office in suburban Rochester and exchange the card, while I'm there, I buy a second one (Yeah, on my card) and drive home.... by 9pm that night the circuit is up, and we are on the air.

Results- Very good line, no noise, can be converted with another card for a modest fee if I want the bandwidth. So that's the story of how the board went to a "friendly foreign country."

The Mad Phone-Man

#### PHRACK PRESENTS ISSUE 16 ####
^*^*^*^Phrack World News, Part 4^*^*^*^
**** File 11 of 12 ****

## Shadow Hawk Busted Again

As many of you know, Shadow Hawk (a/k/a Shadow Hawk 1) had his home searched by agents of the FBI, Secret Service, and the Defense Criminal Investigative Services and had some of his property confiscated by them on September 4th.  We're not going to reprint the Washington Post article as it's available through other sources.  Instead, a summary:

In early July, SH bought an AT&T 3B1 ("Unix PC") with a 67MB drive for a dirt-cheap $525.  He got Sys V 3.5 for another $200 but was dissatisfied with much of the software they gave him (e.g. they gave him uucp version 1.1).

When he was tagged by the feds, he had been downloading software (in the form of C sources) from various AT&T systems.  According to reports, these included the Bell Labs installations at Naperville, Illinois and Murray Hill, New Jersey.  Prosecutors said he also gained entry to (and downloaded software from) AT&T systems at a NATO installation in Burlington, North Carolina and Robins AFB in Georgia.  AT&T claims he stole $1 million worth of software. Some of it was unreleased software taken from the Bell Labs systems that was given hypothetical price tags by Bell Labs spokespersons.  Agents took his 3B1, two Atari STs he had in his room, and several diskettes.

SH is 17 and apparently will be treated as a minor.  At the time of this writing, he will either be subject to federal prosecution for 'computer theft' or will be subject to prosecution only by the State of Illinois.

SH's lawyer,  Karen Plant, was quoted as saying that SH "categorically denies doing anything that he should not have been doing" and that he "had absolutely no sinister motives in terms of stealing property."  As we said, he was just collecting software for his new Unix PC.  When I talked to Ms. Plant on September 25th, she told me that she had no idea if or when the U.S. Attorney would prosecute. Karen Plant can be  reached at (312) 263-1355.  Her address is 134 North LaSalle, #306, Chicago, Illinois.

---------

On July 9th SH wrote:

So you see, I'm screwed. Oh yeah, even worse! In my infinite (wisdom || stupidity, take your pick 8-)) I set up a local AT&T owned 7300 to call me up and send me their uucp files (my uucp works ok for receive) and guess what. I don't think I've to elaborate further on THAT one... (holding my breath, so to type)

(_>Sh<_

---

```
                          #### PHRACK PRESENTS ISSUE 16 ####
                       ^*^*^*^Phrack World News, Part 5^*^*^*^
                               **** File 12 of 12 ****


        "Phone Companies Across U.S. Want Coins Box Thief's Number"
                 From the Tribune - Thursday, Nov. 5, 1987


SAN FRANCISCO  -  Seven  telephone  companies  across  the country, including
  Pacific Bell, are so frazzled  by a coin box thief that they are offering a
  reward of $25,000 to catch him.

He's very clever, telephone officials say,  and is the only known suspect  in
  the country  that is able to  pick the  locks on  coin boxes  in telephone
  booths with relative ease.

He is believed responsible for stealing hundreds of thousands of dollars from
  coin boxes in the Bay Area and Sacramento this year.

The  suspect  has  been  identified  by  authorities  as  James Clark, 47, of
  Pennisula,  Ohio,  a machinist  and  tool-and-die  maker,  who is believed
  responsible for coin box thefts in 24 other states.

Other companies  sharing in  the reward  are Ohio  Bell, Southern Bell, South
  Carolina Bell,  South Central  Bell, Southwestern  Bell, Bell  Telephone of
  Pennsylvania and U.S. West.

Clark  allegedly  hit  pay  phones  that  are  near  freeways and other major
  thoroughfares.  Clark, described  as 5  feet  9 inches tall, with shoulder
  length brown hair and gold-rimmed glasses, is reported to be driving a  new
  Chevrolet Astro van painted a dark metallic blue.

He was recently in Arizona but is believed to be back in California.

Written by a Tribune Staff Writer


Typed by the $muggler
```

===== Phrack Magazine presents Phrack 16 =====
===== File 2 of 12 =====

---

BELLCORE Information by The Mad Phone-man

---

So, you've broken into the big phone box on the wall, and are looking at a bunch of tags with numbers and letters on them. Which one is the modem line? Which one is the 1-800 WATS line? Which one is the Alarm line? Bell has a specific set of codes that enable you to identify what you're looking at. These are the same codes the installer gets from the wire center to enable him to set up the line, test it, and make sure it matches the customers order. Here are some extracts from the Bellcore book.

First lets take a hypothetical line number I'm familiar with:
64FDDV 123456

```
----------------------------------------------------------
The serial number format:

        Prefix +  service code + modifier +   serial number +
digits: 1,2      3,4       5,6  7,8,9,10,11,12    continued
----------------------------------------------------------------------------

         Suffix +  CO assigning circuit number +   segment
digits: 13,14,15            16,17,18,19       20,21,22
----------------------------------------------------------------------------
```

The important shit is in the 3rd thru 6th digit.

SERVICE CODES Intra or Inter LATA Block 1-26

-------------

AA- Packet analog access line
AB- Packet switch trunk
AD- Attendant
AF- Commercial audio fulltime
AI- Automatic identified outward dialing
AL- Alternate services
AM- Packet, off-network access line
AN- Announcement service
AO- International/Overseas audio (full time)
AP- Commercial audio (part time)
AT- International/Overseas audio (part time)
AU- Autoscript
BA- Protective alarm (CD)
BL- Bell & lights
BS- Siren control
CA- SSN Access
CB- OCC Audio facilities
CC- OCC Digital facility-medium speed
CE- SSN Station line
CF- OCC Special facility
CG- OCC Telegraph facility
CH- OCC Digital facility high-speed
CI- Concentrator Identifier trunk
CJ- OCC Control facility
CK- OCC Overseas connecting facility wide-band
CL- Centrex CO line
CM- OCC Video facility
CN- SSN Network trunk
CO- OCC Overseas connecting facility
CP- Concentrator identifier signaling link
CR- OCC Backup facility
CS- Channel service
CT- SSN Tie trunk
CV- OCC Voice grade facility
CW- OCC Wire pair facility
CZ- OCC Access facility
DA- Digital data off-net extension
DB- HSSDS 1.5 mb/s access line

```
DF- HSSDS 1.5 mb/s hub to hub
DG- HSSDS 1.5 mb/s hub to earth station
DH- Digital service
DI- Direct-in dial
DJ- Digit trunk
DK- Data link
DL- Dictation line
DO- Direct-out dial
DP- Digital data-2 4 kb/s
DQ- Digital data-4 8 kb/s
DR- Digital data-9.6 kb/s
DW- Digital data-56  kb/s
DY- Digital service (under 1 mb/s)
EA- Switched access
EB- ENFIA II end office trunk
EC- ENFIA II tandem trunk
EE- Combined access
EF- Entrance facility-voice grade
EG- Type #2 Telegraph
EL- Emergency reporting line
EM- Emergency reporting center trunk
EN- Exchange network access facility
EP- Entrance facility-program grade
EQ- Equipment only-(network only) assignment
ES- Extension service-voice grade
ET- Entrance facility-telegraph grade
EU- Extension service-telegraph grade
EV- Enhanced Emergency reporting trunk
EW- Off network MTS/WATS equivalent service
FD- Private line-data
FG- Group-supergroup spectrum
FR- Fire dispatch
FT- Foreign exchange trunk
FW- Wideband channel
FV- Voice grade facility
FX- Foreign exchange
HP- Non-DDS Digital data 2.4 kb/s
HQ- Non-DDS Digital data 4.8 kb/s
HR- Non-DDS Digital data 9.6 kb/s
HW- Non-DDS Digital data 56  kb/s
IT- Intertandem tie trunk
LA- Local area data channel
LL- Long distance terminal line
LS- Local service
LT- Long distance terminal trunk
MA- Cellular access trunk 2-way
MT- Wired music
NA- CSACC link (EPSCS)
NC- CNCC link (EPSCS)
ND- Network data line
OI- Off premises intercommunication station line
ON- Off network access line
OP- Off premises extension
OS- Off premises PBX station line
PA- Protective alarm (AC)
PC- Switched digital-access line
PG- Paging
PL- Private line-voice
PM- Protective monitoring
PR- Protective relaying-voice grade
PS- MSC constructed spare facility
PV- Protective relaying-telegraph grade
PW- Protective relaying-signal grade
PX- PBX station line
PZ- MSC constructed circuit
QU- Packet asynchronous access line
QS- Packet synchronous access line
RA- Remote attendant
RT- Radio landline
SA- Satellite trunk
```

SG- Control/Remote metering signal grade
SL- Secretarial line
SM- Sampling
SN- Special access termination
SQ- Equipment only-customer premises
SS- Dataphone select-a-station
TA- Tandem tie-trunk
TC- Control/Remote metering-telegraph grade
TF- Telephoto/Facsimile
TK- Local PBX trunk
TL- Non-tandem tie trunk
TR- Turret or automatic call distributor (ACD) trunk
TT- Teletypewriter channel
TU- Turret or automatic call distributor (ACD) line
TX- Dedicated facility
VF- Commercial television (full time)
VH- Commercial television (part time)
VM- Control/Remote metering-voice grade
VO- International overseas television
VR- Non-commercial television (7003,7004)
WC- Special 800 surface trunk
WD- Special WATS trunk (OUT)
WI- 800 surface trunk
WO- WATS line (OUT)
WS- WATS trunk (OUT)
WX- 800 service line
WY- WATS trunk (2-way)
WZ- WATS line (2-way)
ZA- Alarm circuits
ZC- Call and talk circuits
ZE- Emergency patching circuits
ZF- Order circuits, facility
ZM- Measurement and recording circuits
ZP- Test circuit, plant service center
ZQ- Quality and management circuits
ZS- Switching, control and transfer circuits
ZT- Test circuits, central office
ZV- Order circuits, service

SERVICE CODES FOR LATA ACCESS
---------------------------------------------------
HC- High capacity 1.544 mb/ps
HD- High capacity 3.152 mb/ps
HE- High capacity 6.312 mb/ps
HF- High capacity 6.312
HG- High capacity 274.176 mb/s
HS- High capacity subrate
LB- Voice-non switched line
LC- Voice-switched line
LD- Voice-switched trunk
LE- Voice and tone-radio landline
LF- Data low-speed
LG- Basic data
LH- Voice and data-PSN access trunk
LJ- Voice and data SSN access
LK- Voice and data-SSN-intermachine trunk
LN- Data extension, voice grade data facility
LP- Telephoto/Facsimile
LQ- Voice grade customized
LR- Protection relay-voice grade
LZ- Dedicated facility
MQ- Metallic customized
NQ- Telegraph customized
NT- Protection alarm-metallic
NU- Protection alarm
NV- Protective relaying/Telegraph grade
NW- Telegraph grade facility-75 baud
NY- Telegraph grade facility- 150 baud
PE- Program audio, 200-3500 hz
PF- Program audio, 100-5000 hz

| | |
|---|---|
| PJ- | Program audio, 50-8000 hz |
| PK- | Program audio, 50-15000 hz |
| PQ- | Program grade customized |
| SB- | Switched access-standard |
| SD- | Switched access-improved |
| SE- | Special access WATS-access-std |
| SF- | Special access WATS access line improved |
| SJ- | Limited switched access line |
| TQ- | Television grade customized |
| TV- | TV Channel one way 15khz audio |
| TW- | TV Channel one way 5khz audio |
| WB- | Wideband digital, 19.2 kb/s |
| WE- | Wideband digital, 50 kb/s |
| WF- | Wideband digital, 230.4 kb/s |
| WH- | Wideband digital, 56 kb/s |
| WJ- | Wideband analog, 60-108 khz |
| WL- | Wideband analog 312-552 khz |
| WN- | Wideband analog 10hz-20 khz |
| WP- | Wideband analog, 29-44 khz |
| WR- | Wideband analog 564-3064 khz |
| XA- | Dedicated digital, 2.4 kb/s |
| XB- | Dedicated digital, 4.8 kb/s |
| XG- | Dedicated digital, 9.6 kb/s |
| XH- | Dedicated digital 56. kb/s |

Now the last two positions of real importance, 5 & 6 translate thusly:

Modifier Character Position 5
------------------------------

| INTRASTATE | INTERSTATE | |
|---|---|---|
| A | B | Alternate data & non data |
| C | | Customer controlled service |
| D | E | Data |
| N | L | Non-data operation |
| P | | Only offered under intra restructured private line (RPL) tariff |
| S | T | Simultaneous data & non-data |
| F | | Interexchange carriers is less than 50% |
| | G | Interstate carrier is more than 50% usage |

MODIFIER CHARACTER POSITION 6
-------------------------------------------------------------------

| TYPE OF SERVICE | Intra LATA | |
|---|---|---|
| ALL EXCEPT US GOVT | US GOVERNMENT | |
| T | M | Circuit is BOC customer to BOC customer all facilities are TELCO provided |
| C | P | Circuit is BOC/BOC and part of facilities or equipment is telco provided |
| A | J | Circuit is BOC/BOC all electrically connected equip is customer provided |

```
       L                    F      Circuit terminates at interexchange
                                       carrier customers location
---------------------------------------
       Z                               Official company service
---------------------------------------
                           Interlata
       S                    S      Circuit terminates at interexchange
                                       carriers point of term (POT)
---------------------------------------
       V                    V      Circuit terminates at an interface of a
                                       radio common carrier (RCC)
---------------------------------------
       Z                               Official company service
---------------------------------------

                            Corridor
       Y                    X      Corridor circuit
---------------------------------------
                            International
       K                    H      Circuit has at least 2 terminations in
                                       different countries
---------------------------------------
                            Interexchange carrier
       Y                    X      Transport circuit between interexchange
                                       carrier terminals.
-----------------------------------------
```

So 64FDDV would be a private line data circuit terminating at a radiocommon carrier.  Other examples can be decoded likewise.

Enjoy this information as much as I've had finding it.

    -= The Mad Phone-man =-

```
                ===== Phrack Magazine presents Phrack 16 =====
                           ===== File 3 of 12 =====

==========================================
====    Cosmos Kid Presents...     ====
====   A Hacker's Guide To:  PRIMOS   ====
====            Part I        ====
====    (c) 1987 by Cosmos Kid  ====
==========================================
```

## Author's Note:

This file is the first of two files dealing with PRIMOS and its operations. The next file will be in circulation soon so be sure to check it out at any good BBS.

## Preface:

This file is written in a form to teach beginners as well as experienced Primos users about the system. It is written primarily for beginners however. PRIMOS, contrary to popular belief can be a very powerful system if used correctly. I have outlined some VERY BASIC commands and their use in this file along with some extra commands, not so BASIC.

## Logging On To A PRIMOS:

A PRIMOS system is best recognized by its unusual prompts. These are: 'OK', and 'ER!'. Once connected, these are not the prompts you get. The System should identify itself with a login such as:

```
Primenet V2.3
-or-
Primecom Network
```

The system then expects some input from you,preferably: LOGIN. You will then be asked to enter your user identification and password as a security measure. The login onto a PRIMOS is as follows:

```
CONNECT
Primenet V 2.3 (system)
LOGIN<CR>      (you)
User id?       (system)
AA1234   (you)
Password?      (system)
KILLME   (you)
OK,         (system)
```

Preceding the OK, will be the systems opening message. Note that if you fail to type login once connected, most other commands are ignored and the system responds with:

```
Please Login
ER!
```

## Logging Off Of A PRIMOS:

If at any time you get bored with Primos, just type 'LOGOFF' to leave the system. Some systems have a TIMEOUT feature implemented meaning that if you fail to type anything for the specified amount of time the system will automatically log you out, telling you something like:

```
Maximum Inactive Time Limit Exceeded
```

## System Prompts:

As stated previously, the prompts 'ER!' and 'OK,' are used on Primos. The 'OK,' denotes that last command was executed properly and it is now waiting for your next command. The 'ER!' prompt denotes that you made an error in typing your last command. This prompt is usually preceded by an error message.

## Special Characters:

Some terminals have certain characteristics that are built in to the terminal.
key

CONTROL-H
Deletes the last character typed.

## Other Special Characters:

RETURN: The return key signals PRIMOS that you have completed typing a command and that you are ready for PRIMOS to process the command.

BREAK/CONTROL-P: Stops whatever is currently being processed in memory and will return PRIMOS to your control. To restart a process, type:
START (abbreviated with S).

CONTROL-S: Stops the scrolling of the output on your terminal for viewing.

CONTROL-Q: Resumes the output scrolling on your terminal for inspection.

SEMICOLON ';': The logical end of line character. The semicolon is used to enter more than one command on one line.

## Getting Help:

You can get on-line information about the available PRIMOS commands by using the 'HELP' command. The HELP system is keyword driven. That is, all information is stored under keywords that indicate the content of the help files. This is similar to VAX. Entering the single command 'HELP' will enter the HELP sub-system and will display an informative page of text. The next page displayed will provide you with a list of topics and their keywords. These topics include such items as PRIME, RAP, MAIL, and DOC. If you entered the MAIL keyword, you would be given information concerning the mail sub-system available to users on P simply enter PRIME to obtain information on all PRIMOS commands. You could then enter COPY to obtain information on that specific topic.

## Files And Directories:

The name of a file or sub-directory may have up to 32 characters. The filename may contain any of the following characters, with the only restriction being that the first character of the filename may not be a digit. Please note that BLANK spaces are NOT allowed ANYWHERE:

```
A-Z .....alphabet
0-9 .....numeric digits
&   .....ampersand
#   .....pound sign
$   .....dollar sign
-   .....dash/minus sign
*   .....asterisk/star
.   .....period/dot
/   .....slash/divide sign
```

## Naming Conventions:

There are very few restrictions on the name that you may give a file. However, you should note that many of the compilers (language processors) and commands on the PRIME will make certain assumptions if you follow certain guidelines. File name suffixes help to identify the file contents with regard to the language the source code was written in and the contents of the file. For instance, if you wrote a PL/1 program and named the file containing the source code 'PROG1.PL1' (SEGmented loader) would take the binary file, link all the binary libraries that you specify and produce a file named 'PROG1.SEG', which would contain the binary code necessary to execute the program. Some common filename suffixes are: F77, PAS, COBOL, PL1G, BASIC, FTN, CC, SPIT (source files). These all denote separate languages and get into more advanced programming on PRIMOS. (e.g. FTN=Fortran).

BIN=the binary code produced by the compiler
LIST=the program listing produced by the compiler
SEG=the linked binary code produced by SEG

Some files which do not use standard suffixes may instead use the filename prefixes to identify the contents of the file. Some common filename prefixes are:

B  Binary code produced by the compiler
L  source program Listing
C  Command files
$  Temporary work files (e.g. T$0000)
#  Seg files

Commands For File Handling:
---------------------------

PRIMOS has several commands to control and access files and file contents. These commands can be used to list the contents of files and directories, and to copy, add, delete, edit, and print the contents of files. The capitalized letters of each are deleted. A LIST must be enclosed in parenthesis.

```
Close arg       ....Closes the file specified by 'arg'.  'Arg' could also be
                 a list of PRIMOS file unit numbers, or the word 'ALL' which
                 closes all open files and units.

LIMITS          ....Displays information about the login account, including
                 information about resources allocated and used, grantor, and
                 expiration date.

Edit Access     ....Edits the Access rights for the named directories and
                 files.

CName arg1 arg2 ....Changes the Name of 'arg1' to 'arg2'.  The arguments can
                 be files or directories.

LD              ....The List Directory command has several arguments that
                 allow for controlled listing format and selection of entries.

Attach arg      ....allows you to Attach to the directory 'arg' with the
                 access rights specified in the directory Access Control List.

DOWN <arg>      ....allows you to go 'DOWN into' a sub-ufd (directory).  You
                 can specify which one of several sub-ufds to descend into
                 with the optional 'arg'.

UP <arg>         ....allows you to go 'UP into' a higher ufd (directory).  You
                 can specify which one of several to climb into with the
                 optional 'arg'.

WHERE           ....Displays what the current directory attach point is and
                 your access rights.

CREATE arg      ....CREATES a new sub-directory as specified by 'arg'.

COPY arg1 arg2  ....COPIES the file or directory specified by 'arg1' into a
                 file by the same name specified by 'arg2'.  Both 'arg1' and
                 'arg2' can be filename with the SPOOL command, whose format
                 is:
```

```
SPOOL filename -AT destination
                 where filename is the name of the file you want printed, and
                 destination is the name of the printer where you want the
                 file printed.  For example if you want the file 'HACK.FTN'
                 printed at the destination 'LIB' type:

SPOOL HACK.FTN -AT LIB
```

PRIMOS then gives you some information telling you that the file named was SPOOLed and the length of the file in PRIMOS records. To see the entries in the SPOOL queue, type:

```
SPOOL -LIST
```

PRIMOS then lists out all the files waiting to be printed on the printers on your login system. Also included in this information will be the filename of the files waiting to print, the login account name of the user who SPOOLed the file, the time that the file was SPOOLed, the size of the file in PRIMOS records, and the printer name where the file is to print.

Changing The Password Of An Account:
------------------------------------
If you wish to change the password to your newly acquired account you must use the 'CPW' command (Change PassWord).  To do this enter the current password on the command line followed by RETURN.  PRIMOS will then prompt you for your desired NEW password and then ask you to confirm your NEW password.  To change your password of 'JOE' to 'SCHMOE' then type:

```
OK,             (system)
CPW JOE         (you)
New Password?   (system)
```

You can save a copy of your terminal session by using the COMO (COMmand Output) command.  When you type:

```
COMO filename
```

Everything which is typed or displayed on your terminal is saved (recorded) into the filename  on the command line (filename).  If a file by the same name exists, then that file will be REPLACED with NO WARNING GIVEN!  When you have finished doing whatever it was you wanted a hardcopy of, you type:

```
COMO -End
```

which will stop recording your session and will close the COMO file. You can now print the COMO file using the SPOOL command as stated earlier.

Conclusion:
-----------
This  concludes this  first  file on PRIMOS.  Please  remember this  file  is written primarily for beginners, and some of  the text may have seemed BORING! However, this filewaswrittenin  a verbose fashion to FULLYINTRODUCEPRIMOS to beginners.  Part II will deal with more the several languages on PRIMOS and some other commands.

Author's Endnote:
-----------------
I would like to thank the following people for the help in writing this file:

AMADEUS (an oldie who is LONG GONE!)
The University Of Kentucky
State University Of New York (SUNY) Primenet

And countless others.....

Questions, threats, or suggestions to direct towards me, I can be found on any of the following:

| | |
|---|---|
| The Freeworld ][......... | 301-668-7657 |
| Digital Logic............ | 305-395-6906 |
| The Executive Inn........ | 915-581-5146 |
| OSUNY BBS................ | 914-725-4060 |

-=*< Cosmos Kid >*=-

========================================

```
                ===== Phrack Magazine presents Phrack 16 =====
                             ===== File 4 of 12 =====
```

Hacking the Global Telecommunications Network
Researched and written by:  The Kurgan
Compiled on 10/5/87

## Network Procedure Differences

The Global Telecommunications Network (GTN) is Citibanks's international data network, which allows Citicorp customers and personnel to access Citibank's worldwide computerized services.

Two different sign on procedures exist: Type A and Type B.  All users, except some in the U.S., must use Type B.  (U.S. users: the number you dial into and the Welcome Banner you receive determine what sign-on procedure to follow.)  Welcome banners are as follows:

```
TYPE A:
WELCOME TO CITIBANK. PLEASE SIGN ON.
XXXXXXXX

@
PASSWORD =

@

TYPE B:
PLEASE ENTER YOUR ID:-1->
PLEASE ENTER YOUR PASSWORD:-2->

CITICORP (CITY NAME). KEY GHELP FOR HELP.
  XXX.XXX
 PLEASE SELECT SERVICE REQUIRED.-3->
```

## Type A User Commands

User commands are either instructions or information you send to the network for it to follow.  The commands available are listed below.

```
User Action:  Purpose:

@ (CR)  To put you in command mode (mode in which you can put
         your currently active service on hold and ask the network
         for information, or log-off the service).  (NOTE: This
         symbol also serves as the network prompt; see Type A
         messages.)

BYE (CR)  To leave service from command mode.

Continue (CR)  To return to application from command mode (off hold)

D (CR)                  To leave service from command mode.

ID                      To be recognized as a user by the network (beginning of
                        sign on procedure), type ID, then a space and your
                        assigned network ID.  (Usually 5 or 6 characters long)

Status (CR)             To see a listing of network address (only from @
                        prompt).  You need this address when "reporting a
                        problem."
```

## Type A messages

The network displays a variety of messages on your screen which either require a user command or provide you with information.

```
Screen shows:  Explanation:

@   Network prompt -- request for Network ID.

BAD PASSWORD  Network does not except your password.

<address> BUSY          The address is busy, try back later.


WELCOME TO CITIBANK.    Network welcome banner. Second line provides address
PLEASE SIGN ON.         # to be used when reporting "problems."
XXX.XXX

<address> ILLEGAL       You typed in an address that doesn't exist.

<address> CONNECTED     Your connection has been established.

DISCONNECTED            Your connect has been disconnected.

NOT CONNECTED           You're not connected to any service at the time.

NUI REQUIRED            Enter your network user ID.

PASSWORD =              Request for your assigned password.

STILL CONNECTED         You are still connected to the service you were using.

?                       Network doesn't understand your entry.
```

Type B User Commands and Messages

Since the Type B procedure is used with GTN dial-ups, it requires fewer commands to control the network. There is only 1 Type B command. Break plus (CR) allows you to retain connection to one service, and connect with another.

```
Screen Shows:  Explanation:

CITICORP (CITY NAME).   Network Welcome banner. Type in service address.
 PLEASE SELECT SERVICE

COM   Connection made.

DER   The port is closed out of order, or no open routes are
      available.

DISCONNECTED  You have disconnected from the service and the network.

ERR   Error in service selected.

INV   Error in system.

MOM   Wait, the connection is being made.

NA    Not authorized for this service.

NC    Circuits busy, try again.

NP    Check service address.

OCC   Service busy, try again.
```

Sign-on Procedures:

  There are two types of sign on procedures.  Type A and Type B.

Type A:

To log onto a system with type A logon procedure, the easiest way is through Telenet. Dial your local Telenet port. When you receive the "@" prompt, type in the Type-A service address (found later in the article) then follow the instructions from there on.

Type-B:
Dial the your GTN telephone #, then hit return twice. You will then see:

"PLEASE ENTER YOUR ID:-1->"

Type in a network ID number and hit return.

You will then see

"PLEASE ENTER YOUR PASSWORD:-2->"

Type in Network Password and hit return.

Finally you will see the "CITICORP (city name)" welcome banner, and it will ask you to select the service you wish to log onto. Type the address and hit return. (A list of addresses will be provided later)

Trouble Shooting:

If you should run into any problems, the Citicorp personnel will gladly help their "employees" with any questions. Just pretend you work for Citibank and they will give you a lot. This has been tried and tested. Many times, when you attempt to log on to a system and you make a mistake with the password, the system will give you a number to call for help. Call it and tell them that you forgot your pass or something. It usually works, since they don't expect people to be lying to them. If you have any questions about the network itself, call 305-975-5223. It is the Technical Operations Center (TOC) in Pompano, Florida.

Dial-Ups:

The following list of dial-ups is for North America. I have a list of others, but I don't think that they would be required by anyone. Remember: Dial-ups require Type-B log-on procedure. Type-A is available on systems accessible through Telenet.

| | | | |
|---|---|---|---|
| Canada | Toronto | 416-947-2992 | (1200 Baud V.22 Modem Standard) |
| U.S.A. | Los Angeles | 213-629-4025 | (300/1200 Baud U.S.A. Modem Standard) |
| | Jersey City | 201-798-8500 | |
| | New York City | 212-269-1274 | |
| | | 212-809-1164 | |

Service Addresses:

The following is a VERY short list of just some of the 100's of service addresses. In a later issue I will publish a complete list.

| Application Name: | Type-A | Type-B |
|---|---|---|
| CITIADVICE | 2240001600 | CADV |
| CITIBANKING ATHENS | 2240004000 | :30 |
| CITIBANKING PARIS | 2240003300 | :33 |
| CITIBANKING TOKYO | 2240008100 | :81 |
| CITICASH MANAGER | | |
| INTERNATIONAL 1 (NAFG CORP) | 2240001200 | CCM1 |
| INTERNATIONAL 7 (DFI/WELLS FARGO) | 2240013700 | CCM7 |
| COMPMARK ON-LINE | 2240002000 | CS4 |
| ECONOMIC WEEK ON-LINE | 2240011100 | FAME1 |
| INFOPOOL/INFOTEXT | 2240003800 | IP |

EXAMPLE OF LOGON PROCEDURE:

THE FOLLOWING IS THE BUFFERED TEXT OF A LOG-ON TO CITIBANKING PARIS THROUGH TELENET.

```
CONNECT 1200
TELENET
216 13.41

TERMINAL=VT100

@2240003300

223 90331E CONNECTED

ENTER TYPE NUMBER OR RETURN

TYPE B IS BEEHIVE DM20
TYPE 1 IS DEC VT100
TYPE A IS DEC VT100 ADV VIDEO
TYPE 5 IS DEC VT52
TYPE C IS CIFER 2684
TYPE 3 IS LSI ADM 3A
TYPE L IS LSI ADM 31
TYPE I IS IBM 3101
TYPE H IS HP 2621
TYPE P IS PERKIN ELMER 1200
TYPE K IS PRINTER KEYBOARD
TYPE M IS MAI BASIC 4
TYPE T IS TELEVIDEO 9XX
TYPE V IS VOLKER CRAIG 4404
TYPE S IS SORD MICRO WITH CBMP
RELEASE BSC9.5 - 06JUN85
FOR 300 BAUD KEY ! AND CARRIAGE RETURN
CONFIG. K1.1-I11H-R-C-B128
ENTER TYPE NUMBER OR RETURN K

CONNECTED TO CITIBANK PARIS - CBP1 ,PORT 5
```

Have fun with this info, and remember, technology will rule in the end.

===== Phrack Magazine presents Phrack 16 =====
===== File 5 of 12 =====

# The Laws Governing Credit Card Fraud

Written by Tom Brokaw
September 19, 1987

Written exclusively for:
Phrack Magazine

(A Tom Brokaw/Disk Jockey Law File Production)

## Introduction:

In this article, I will try to explain the laws concerning the illegal use of credit cards. Explained will be the Michigan legislative view on the misuse and definition of credit cards.

## Definition:

Well, Michigan Law section 157, defines a credit card as "Any instrument or device which is sold, issued or otherwise distributed by a business organization identified thereon for obtaining goods, property, services or anything of value." A credit card holder is defined as: 1) "The person or organization who requests a credit card and to whom or for whose benefit a credit card is subsequently issued" or 2) "The person or organization to whom a credit card was issued and who uses a credit card whether the issuance of the credit card was requested or not." In other words, if the company or individual is issued a card, once using it, they automatically agree to all the laws and conditions that bind it.

## Stealing, Removing, Retaining or Concealment:

Michigan Law states, that it is illegal to "steal, knowingly take or remove a credit card from a card holder." It also states that it is wrongful to "conceal a credit card without the consent of the card holder." Notice that it doesn't say anything about carbons or numbers acquired from BBSes, but I think that it could be considered part of the laws governing the access of a persons account without the knowledge of the cardholder, as described above.

## Possession with Intent to Circulate or Sell

The law states that it is illegal to possess or have under one's control, or receive a credit card if his intent is to circulate or sell the card. It is also illegal to deliver, circulate or sell a credit card, knowing that such a possession, control or receipt without the cardholders consent, shall be guilty of a FELONY. Notice again, they say nothing about possession of carbons or numbers directly. It also does not clearly state what circulation or possession is, so we can only stipulate. All it says is that possession of a card (material plastic) is illegal.

## Fraud, forgery, material alteration, counterfeiting.

However, it might not be clearly illegal to possess a carbon or CC number. It IS illegal to defraud a credit card holder. Michigan law states that any person who, with intent to defraud, forge, materially alter or counterfeit a credit card, shall be guilty of a felony.

## Revoked or cancelled card, use with intent to defraud.

This states that "Any person who knowingly and with intent to defraud for the purpose of obtaining goods, property or services or anything of value on a credit card which has been revoked or cancelled or reported stolen by the issuer or issuee, has been notified of the cancellation by registered or certified mail or by another personal service shall be fined not more than $1,000 and not imprisoned not more than a year, or both. However, it does not clearly say if it is a felony or misdemeanor or civil infraction. My guess is that it would be dependant on the amount and means that you used and received when you defraud the company. Usually, if it is under $100, it is a misdemeanor but if it is over $100, it is a felony. I guess they figure that you should know these things.

## The People of The State of Michigan vs. Anderson (possession)

On April 4, 1980, H. Anderson attempted to purchase a pair of pants at Danny's Fashion Shops, in the Detroit area. He went up to the cashier to pay for the pants and the cashier asked him if he had permission to use the credit card. He said "No, I won it last night in a card game". The guy said that I could purchase $50 dollars worth of goods to pay back the debt. At the same time, he presumed the card to be a valid one and not stolen. Well, as it turned out it was stolen but he had no knowledge of this. Later, he went to court and pleased guilty of attempted possession of a credit card of another with intent or circulate or sell the same. At the guilty hearings, Mr. Anderson stated that the credit card that he attempted to use had been acquired by him in payment of a gambling debt and assumed that the person was the owner. The trial court accepted his plea of guilty. At the sentencing, Mr. Anderson, denied that he had any criminal intent. Anderson appealed the decision stating that the court had erred by accepting his plea of guilty on the basis of insufficient factual data. Therefore, the trial court should not have convicted him of attempted possession and reversed the charges.

## The People of the State of Michigan vs. Willie Dockery

On June 23, 1977, Willie Dockery attempted to purchase gas at a Sears gas station by using a stolen credit card. The attendant noticed that his driver's license picture was pasted on and notified the police. Dockery stated that he had found the credit card and the license at an intersection, in the city of Flint. He admitted that he knowingly used the credit card and driver's license without the consent of the owner but he said that he only had purchased gasoline on the card. It turns out that the credit card and driver's license was stolen from a man, whose grocery store had been robbed. Dockery said that he had no knowledge of the robbery and previous charges on the cardwhich totalled$1,373.21. He admitted that he did paste his picture on the driver's license. Butagain the court screws up, they receive evidence that the defendant had a record of felonies dating back to when he was sixteen and then assumed that he was guilty on the basis of his prior offenses. The judge later said that the present sentence could not stand in this court so the case was referred to another court.

## Conclusion

I hope that I have given you a better understanding about the law, that considers the illegal aspects of using credit cards. All this information was taken from The Michigan Compiled Laws Annotated Volume 754.157a-s and from The Michigan Appeals Report.

In my next file I will talk about the laws concerning Check Fraud.

```
                                              -Tom Brokaw
```

```
                 ===== Phrack Magazine presents Phrack 16 =====
                            ===== File 6 of 12 =====

*******************************************************************************
*                                                                             *
*                        Tapping Telephone Lines                              *
*                                                                             *
*                             Voice or Data                                *
*                                                                             *
*                       For Phun, Money, and Passwords                     *
*                                                                             *
*                  Or How to Go to Jail for a Long Time.                      *
*                                                                             *
*******************************************************************************
```

Written by Agent Steal 08/87

Included in this file is...

* Equipment needed

* Where to buy it

* How to connect it

* How to read recorded data

But wait!!  There’s more!!

* How I found a Tymnet node

* How I got in

```
*************
THE EQUIPMENT
*************
```

First thing you need is an audio tape recorder. What you will be recording, whether it be voice or data, will be in an analog audio format. >From now on, most references will be towards data recording. Most standard cassette recorders will work just fine. However, you are limited to 1 hour recording time per side. This can present a problem in some situations. A reel to reel can also be used. The limitations here are size and availability of A.C. Also, some reel to reels lack a remote jack that will be used to start and stop the recorder while the line is being used. This may not present a problem. More later. The two types of recorders I would advise staying away from (for data) are the micro cassette recorders and the standard cassette recorders that have been modified for 8 to 10 hour record time. The speed of these units is too unstable. The next item you need, oddly enough, is sold by Radio Shack under the name "Telephone recording control" part # 43-236 $24.95. See page 153 of the 1987 Radio Shack catalog.

```
****************
HOW TO CONNECT IT
****************
```

The Telephone recording control (TRC) has 3 wires coming out of it.

#1 Telco wire with modular jack.  Cut this and replace with alligator clips.

#2 Audio wire with miniature phone jack (not telephone).  This plugs
into the microphone level input jack of the tape recorder.

#3 Audio wire with sub miniature phone jack.  This plugs into the "REM" or remote control jack of the tape recorder.

Now all you need to do is find the telephone line, connect the alligator clips, turn the recorder on, and come back later. Whenever the line goes off hook, the recorder starts. It's that simple.

****************
READING THE DATA
****************

This is the tricky part. Different modems and different software respond differently but there are basics. The modem should be connected as usual to the telco line and computer. Now connect the speaker output of the tape player directly to the telephone line. Pick up the phone and dial the high side of a loop so your line doesn't make a lot of noise and garble up your data. Now, command your modem into the answer mode and press play. The tape should be lined up at the beginning of the recorded phone call, naturally, so you can see the login. Only one side of the transmission between the host and terminal can be monitored at a time. Going to the originate mode you will see what the host transmitted. This will include the echoes of the terminal. Of course the password will be echoed as ####### for example, but going to the answer mode will display exactly what the terminal typed. You'll understand when you see it. A couple of problems you might run into will be hum and garbage characters on the screen. Try connecting the speaker output to the microphone of the hand set in your phone. Use a 1 to 1 coupling transformer between the tape player input and the TRC audio output. These problems are usually caused when using A.C. powered equipment. The common ground of this equipment interferes with the telco ground which is D.C. based.

I was a little reluctant to write this file because I have been unsuccessful in reading any of the 1200 baud data I have recorded. I have spoke with engineers and techs. Even one of the engineers who designs modems. All of them agree that it IS possible, but can't tell me why I am unable to do this. I believe that the problems is in my cheap ass modem. One tech told me I needed a modem with phase equalization circuitry which is found in most expensive 2400 baud modems. Well one of these days I'll find $500 lying on the street and I'll have nothing better to spend it on! Ha! Actually, I have a plan and that's another file.....

I should point out one way of reading 1200 baud data. This should work in theory, however, I have not attempted it.

Any fully Hayes compatible modem has a command that shuts off the carrier and allows you to monitor the phone line. The command is ATS10. You would then type either answer or originate depending on who you wanted to monitor. It would be possible to write a program that records the first 300 or so characters then writes it to disk, thus allowing unattended operation.

**************
HOW CRAZY I AM
**************

PASSWORDS GALORE!!!!

After numerous calls to several Bell offices, I found the one that handled Tymnet's account. Here's a rough transcript:

Op:  Pacific Bell priority customer order dept. How may I help you?
Me:  Good Morning, this is Mr. Miller with Tymnet Inc.  We're interested in
     adding some service to our x town location.
Op:  I'll be happy to help you Mr. Miller.
Me:  I need to know how many lines we have coming in on our rotary and if we
     have extra pairs on our trunk.  We are considering adding ten additional
     lines on that rotary and maybe some FX service.
Op:  Ok....What's the number this is referenced to?
Me:  xxx-xxx-xxxx (local node #)
Op:  Hold on a min....Ok bla, bla, bla.

Well you get the idea. Anyway, after asking her a few more unimportant questions I asked her for the address. No problem, she didn't even hesitate. Of course this could have been avoided if the CN/A in my area would give out addresses, but they don't, just listings. Dressed in my best telco outfit, Pac*Bell baseball cap, tool belt and test set, I was out the door. There it was, just an office building, even had a computer store in it. After exploring the building for awhile, I found it. A large steel door with a push button lock. Back to the phone. After finding the number where the service techs were I called it and talked to the tech manager.

Mgr: Hello this is Joe Moron.
Me: Hi this is Mr. Miller (I like that name) with Pacific Bell. I'm down here at your x town node and we're having problems locating a gas leak in one of our Trunks. I believe our trunk terminates pressurization in your room.
Mgr: I'm not sure...
Me: Well could you have someone meet me down here or give me the entry code?
Mgr: Sure the code is 1234.
Me: Thanks, I'll let you know if there's any trouble.

So, I ran home, got my VCR (stereo), and picked up another TRC from Trash Shack. I connected the VCR to the first two incoming lines on the rotary. One went to each channel (left,right). Since the volume of calls is almost consistent, it wasn't necessary to stop the recorder between calls. I just let it run. I would come back the next day to change the tape. The VCR was placed under the floor in case a tech happened to come by for maintenance. These nodes are little computer rooms with air conditioners and raised floors. The modems and packet switching equipment are all rack mounted behind glass. Also, most of the nodes are unmanned. What did I get? Well a lot of the logins were 1200, so I never found out what they were. Still have 'em on tape though! Also a large portion of traffic on both Tymnet and Telenet is those little credit card verification machines calling up Visa or Amex. The transaction takes about 30 secs and there are 100's on my tapes. The rest is as follows:

```
   Easylink       CompuServe    Quantumlink     3Mmail
   PeopleLink   Homebanking       USPS          Chrysler parts order
   Yamaha           Ford              Dow Jones
```

And a few other misc. systems of little interest. I'm sure if I was persistent, I'd get something a little more interesting. I spent several months trying to figure out my 1200 baud problem. When I went back down there the code had been changed. Why? Well I didn't want to find out. I was out of there! I had told a couple of people who I later found could not be trusted. Oh well. Better safe than sorry.

**************************************

Well, if you need to reach me,try my VMS at 415-338-7000 box 8130. But no telling how long that will last. And of course there's always P-80 systems at 304-744-2253. Probably be there forever. Thanks Scan Man, whoever you are. Also read my file on telco local loop wiring. It will help you understand how to find the line you are looking for. It should be called Telcowiring.Txt

<<< AGENT STEAL >>>

```
                 ===== Phrack Magazine presents Phrack 16 =====
                            ===== File 7 of 12 =====

------------------------------------------------------------------------
-                         The Disk Jockey                             -
-                            presents:                           -
-                                                                      -
-                    Reading Trans-Union Reports:                     -
-                       A lesson in terms used                    -
-                       (A 2af presentation)                       -
------------------------------------------------------------------------
```

This file is dedicated to all the phreaks/hacks that were busted in the summer of 1987, perhaps one of the most crippling summers ever for us.

Preface:
-------

Trans-Union is a credit service much like CBI, TRW or Chilton, but offers more competitive rates, and is being used more and more by many credit checking agencies.

Logging in:
----------

Call one of the Trans Union dial-ups at 300,E,7,1, Half Duplex. Such a dial-up is 314-XXX-XXXX. After connecting, hit Ctrl-S. The system will echo back a 'GO ' and then awaits you to begin the procedure of entering the account and password, then mode, i.e.: S F1111,111,H,T. The system will then tell you what database you are logged on to, which is mostly insignificant for your use. To then pull a report, you would type the following: P JONES,JIM* 2600,STREET,CHICAGO,IL,60604** <Ctrl-S>. The name is Jim Jones, 2600 is his street address, street is the street name, Chicago is the city, IL is the state, 60604 is the zip.

The Report:
----------

The report will come out, and will look rather odd, with all types of notation. An example of a Visa card would be:

```
SUB NAME/ACCT#  SUB#    OPEND   HICR DTRP/TERM BAL/MAX.DEL PAY.PAT   MOP

CITIBANK         B453411  3/87  $1000   9/87A   $0       12111     R01
4128XXXXXXXXX           $1500           5/87    $120
```

Ok, Citibank is the issuing bank. B453411 is their subscriber code. 3/87 is when the account was opened. HICR is the most that has been spent on that card. 9/87 is when the report was last updated (usually monthly if active). $1000 is the credit line. $0 is the current balance. 12111 is the payment pattern, where 1=pays in 30 days and 2=pays in 60 days. R01 means that it is a "Revolving" account, meaning that he can make payments rather than pay the entire bill at once. 4128-etc is his account number (card number). $1500 is his credit line. 5/87 is when he was late on a payment last. $120 is the amount that he was late with.

Here is a list of terms that will help you identify and understand the reports better:

ECOA Inquiry and Account Designators
------------------------------------

I Individual account for sole use of applicant
C Joint spousal contractual liability
A Authorized user of shared account
P Participant in use of account that is neither C nor A
S Co-signer, not spouse
M Maker primarily liable for account, co-signer involved
T Relationship with account terminated
U Undesignated
N Non-Applicant spouse inquiry

Remarks and FCBA Dispute Codes

```
------------------------------
AJP Adjustment pending
BKL Bankruptcy loss
CCA Consumer counseling account
CLA Placed for collection
CLO Closed to further purchases
CTS Contact Subscriber
DIS Dispute following resolution
DRP Dispute resolution pending
FCL Foreclosure
MOV Moved, left no forwarding address
ND  No dispute
PRL Profit and loss write-off
RFN Account refinanced
RLD Repossession, paid by dealer
RLP Repossession, proceeds applied towards debt
RPO Repossession
RRE Repossession, redeemed
RS  Dispute resolved
RVD Returned voluntarily, paid by dealer
RVN Returned voluntarily
RVP Returned voluntarily, proceeds go towards debt
RVR Returned voluntarily, redeemed
SET Settled for less than full balance
STL Plate (card) stolen or lost
TRF Transferred to another office

Type of Account
---------------
O Open account (30 or 90 days)
R Revolving or option account (open-end)
I Installment (fixed number of payments)
M Mortgage
C Check credit (line of credit at a bank)

Usual Manner of Payment
-----------------------
00 Too new to rate; approved, but not used or not rated
01 Pays (or paid) within 30 days of billing, pays accounts as agreed
02 Pays in more than 30 days, but not more than 60 days
03 Pays in more than 60 days, but not more than 90 days
04 Pays in more than 90 days, but not more than 120 days
05 Pays in 120 days or more
07 Makes payments under wage earner plan or similar arrangement
08 Repossession
8A Voluntary repossession
8D Legal repossession
8R Redeemed repossession
09 Bad debt; placed for collection; suit; judgement; skip
9B Placed for collection
UR Unrated
UC Unclassified

Kinds of Business Classification
-------------------------------
A Automotive
B Banks
C Clothing
D Department and variety
F Finance
G Groceries
H Home furnishings
I Insurance
J Jewelry and cameras
K Contractors
L Lumber, building materials
M Medical and related health
N National credit card
O Oil and national credit card
P Personal services other than medical
```

Q Mail order houses
R Real estate and public accommodations
S Sporting goods
T Farm and garden supplies
U Utilities and fuel
V Government
W Wholesale
X Advertising
Y Collection services
Z Miscellaneous

Type of Installment Loan
------------------------

AF Appliance/Furniture
AP Airplane
AU Automobile
BT Boat
CA Camper
CL Credit line
CM Co-maker
CO Consolidation
EQ Equipment
FH FHA contract loan
FS Finance statement
HI Home improvement
IN Insurance
LE Leases
MB Mobile home
MC Miscellaneous
MT Motor home
PI Property improvement plan
PL Personal loan
RE Real estate
ST Student loan
SV Savings bond, stock, etc.
US Unsecured
VA Veteran loan

Date Codes
----------

A Automated, most current information available
C Closed date
F Repossessed/Written off
M Further updates stopped
P Paid
R Reported data
S Date of last sale
V Verified date

Employment Verification Indicator
---------------------------------

D Declined verification
I Indirect
N No record
R Reported, but not verified
S Slow answering
T Terminated
V Verified
X No reply

Hope this helps. Anyone that has used Trans-Union will surely appreciate this, as the result codes are sometimes hard to decipher.

-The Disk Jockey

#### PHRACK PRESENTS ISSUE 16 ####
^*^*^*^Phrack World News, Part 1^*^*^*^
**** File 8 of 12 ****

>From the 9/16 San Francisco Chronicle, page A19:

GERMAN HACKERS BREAK INTO NASA NETWORK (excerpted)

Bonn

A group of West German computer hobbyists broke into an international computer network of the National Aeronautics and Space Administration and rummaged freely among the data for at least three months before they were discovered, computer enthusiasts and network users said yesterday.

An organization in Hamburg called the Chaos Computer Club, which claimed to be speaking for an anonymous group that broke into the network, said the illicit users managed to install a "Trojan horse," and gain entry into 135 computers on the European network.

A "Trojan Horse" is a term for a permanent program that enables amateur computer enthusiasts [as opposed to professionals?], or "hackers," to use a password to bypass all the security procedures of a system and gain access to all the data in a target computer.

[Actually, this type of program is a ’back door’ or a ’trap door.’ The group may very well have *used* a Trojan horse to enable them to create the back door, but it probably wasn’t a Trojan horse per se. A Trojan horse is a program that does something illicit and unknown to the user in addition to its expected task. See Phrack xx-x, "Unix Trojan Horses," for info on how to create a Trojan horse which in turn creates a trap door into someone’s account.]

The NASA network that was broken into is called the Space Physics Analysis Network [ooh!] and is chiefly designed to provide authorized scientists and organizations with access to NASA data. The security system in the network was supplied by an American company, the Digital Equipment Corp. [Probably DECNET. Serves them right.] Users said the network is widely used by scientists in the United States, Britain, West Germany, Japan and five other countries and does not carry classified information.

A Chaos club spokesman, Wau Holland, denied that any data had been changed. This, he said, went against "hacker ethics."

West German television reports said that computer piracy carries a penalty of three years in prison in West Germany. The government has not said what it plans to do.

The Chaos club clearly views its break-in as a major coup. Holland, reached by telephone in Hamburg, said it was "the most successful running of a Trojan horse" to his knowledge, and the club sent a lengthy telex message to news organizations.

It said the "Trojan horse" was spotted by a user in August, and the infiltrating group then decided to go public because "they feared that they had entered the dangerous field of industry espionage, economic crime, East-West conflict...and the legitimate security interests of high-tech institutions."

The weekly magazine Stern carried an interview with several anonymous hobbyists who showed how they gained access to the network. One described his excitement when for the first time he saw on his screen, "Welcome to the NASA headquarters VAX installation."

According to Chaos, the hobbyists discovered a gap in the Digital VAX systems 4.4 and 4.5 and used it to install their "Trojan Horse."

[Excerpted and Typed by Shooting Shark. Comments by same.]

#### PHRACK PRESENTS ISSUE 16 ####
^*^*^*^Phrack World News, Part 2^*^*^*^
**** File 9 of 12 ****

[Ed's Note: CertainThings in the article have been blanked (XXXXX) at the request of the author]

The Story of the Feds on XXXXXXX BBS
By The Mad Phone Man

Returninghome one afternoon with a friend, I knew something wasn't right when I walked into the computer room. I see a "Newuser" on the board... and the language he's using is... well "Intimidating"...

"I want you all to know I'm with the OCC task force and we know who you are... we are going to have a little get-together and 'talk' to you all."

Hmmm... a loser?... I go into chat mode... "Hey dude, what's up?" I ask. "Your number asshole" he says.... Well, fine way to log on to a board if I do say.... "Hey, you know I talked to you and I know who you are.." "Oh yeah...Who am I?." he hesitates and says... "Well uh.. you used to work for Sprint didn't you?"

I say, "No, you've got me confused with someone else I think, I'm a junior in high school."

"Ohyeah?.. You got some pretty big words for a high school kid," he says....

"Well, in case you didn't know, they teach English as a major these days...."

He says... "Do you really want to know which LD company I'm with?"

I say "NO, but if it will make you happy, tell me."

He says MCI. (Whew! I don't use them)... "Well you're outta luck asshole, I pay for my calls, and I don't use MCI." He's dumbfounded.

I wish him the worst as he asks me to leave his rather threatening post up on my board and we hang up on him.

Now, I'm half paralyzed... hmmm.... Check his info-form... he left a number in 303... Denver.... I grab the phone and call it.. It's the Stromberg Telephone company... Bingo.. I've got him.

I search my user files and come up with a user called "Cocheese" from there, and I voice validated him, and he said he worked for a small telco called Stromberg... I'm onto him now.

Later in the week, I'm in a telco office in a nearby major city, I happen to see a book, marked "Confidential Employee Numbers for AT&T." I thumb thru and lo and behold, an R.F. Stromberg works at an office of AT&T in Denver, and I can't cross reference him to an office. (A sure sign he's in security). Well, not to be out-done by this loser... I dial up NCIC and check for a group search for a driver's licence for him... Bingo. Licence number, cars he owns, his SS number, and a cross reference of the licence files finds his wife, two kids and a boat registered to him.

I've never called him back, but If I do have any trouble with him, I'm gonna pay a little visit to Colorado....