==Phrack Inc.==

Volume Three, Issue Thirty-five, File 1 of 13

Issue XXXV Index

P H R A C K 3 5

November 17,1991

˜Don't Tread on Me!˜

Phrack Inc. is going great! In fact so great that we already have enough material for the next two issues including the long-awaited sequel to Phrack 13 (the infamous joke issue released on April 1, 1987), Diet Phrack! That issue which will be number 36 is scheduled for release next month and will mark the end of Volume 3. If you have anything that is somewhat humorous, send it over to us at Phrack as soon as possible so we can include it.

Phrack Inc. celebrates its sixth birthday with the release of this issue. Exactly six years ago, sitting in front of an IBM PC known as Metal Shop Private, were Taran King and Knight Lightning releasing a soon to be famous publication called Phrack Inc. That first issue wasn't much, a small collection of eight files sent across the country to bulletin boards at 1200 baud. Six years is quite a long time in the hacker underground. Today we send Phrack to thousands of people at hundreds of Internet sites spanning the entire world. Phrack has become more than a magazine, it truly is an institution. Long Live Phrack!

Pay close attention to Phrack World News this issue for details on HoHo/ XMAScon and many other stories with serious ramifications to our way of life.

Special thanks to Twisted Pair (for the help in a jam), Amadeus, The Butler, and Black Kat for the great files. Thanks to the Great Gatsby, just because he is cool. It's people like you that keeps this magazine comming out so frequently.

This month we have had a ton of letters for Phrack Loopback. If your letter or question did not appear, we are sorry that it has to wait one more issue! The last issue really got some administrators (or wanna-be admins) steamed at us. Check out Phrack Loopback and PWN Quicknotes for details.

Your Editors,

Crimson Death and Dispater
phrack@stormking.com

Submissions: phrack@stormking.com
FTP Distribution: cs.widener.edu or eff.org

Phrack XXXV Table of Contents

1. Introduction to Phrack 34 by Crimson Death and Dispater
2. Phrack Loopback by Phrack Staff
3. Phrack Profile of Chris Goggans by S. Leonard Spitz
4. Telenet/Sprintnet's PC Pursuit Outdial Directory by Amadeus
5. Sting Operations by Sovereign Immunity
6. Social Security Numbers & Privacy by Chris Hibbert of CPSR
7. Users Guide to VAX/VMS Part 1 of 3 by Black Kat
8. A Beginners Guide to Novell Netware 386 by The Butler
9. Auto-Answer It by Twisted Pair
10. PWN/Part 1 by Dispater
11. PWN/Part 2 by Dispater
12. PWN/Part 3 by Dispater

13. PWN/Part 4 by Dispater

==Phrack Inc.==

Volume Three, Issue Thirty-five, File 2 of 13

[-=:< Phrack Loopback >:=-]

By Phrack Staff

Phrack Loopback is a forum for you, the reader, to ask questions, air problems, and talk about what ever topic you would like to discuss. This is also the place The Phrack Staff will make suggestions to you by reviewing various items of note; magazines, software, catalogs, hardware, etc.

What's on Your Mind

:: Hacking VMB's ::

From: Mr. Upsetter
To: phracksub@stormking.com
Subject: Phrack 34 VMB article

The article in Phrack 34 on voice mail hacking by Night Ranger was really good. It reminded me of some experiences I had with a cellular voice mail system a couple years ago in San Diego. I would bet there are similar systems in other cities.

These VMB's would automatically answer calls when the subscriber wasn't on the air. They worked just like standard VMB's. To access the box, the owner could dial his or her own cellular number, then hit * when it answered. Then the VMB would ask for a password.

Guess what the default password was? None! That meant all you had to do was dial up a cellular VMB and hit *, and you were in. How many VMB's still had the default password? About half...

To scan for cellular VMB's all you had to do was dial numbers in the cellular prefix. It was pretty fun...almost too easy.

Cheers,
Mr. Upsetter

- -

>From: Zoso Puda
>
>After reading PHRACK 34 I thought it was good. Especially the article on VMB >hacking. As a matter of fact I wrote a SALT script to help me do it.

This is exactly what we like to see. People actually getting basic information and building on it.

- -

ZoSoft Telix VMB Hacker

written by: Zoso Puda

First words

After reading Night Ranger's article (see PHRACK 34), I decided to make a VMB hacking program. Night Ranger provided good insight into how to hack VMB systems but some VMBs are hard to crack. What I came up with is a program to help me hack some of the harder systems. The ones that don't use the defaults are tough. Also my phone has the buttons and earpiece in one unit and I had to dial then put the phone to my ear and listen, look at the buttons to dial a number and put the phone back to my ear to listen. It soon became tiresome.

What I finally came up with was a program to let me run all the phone functions from the keyboard. My modem speaker is loud enough to hear clearly so it seemed like the perfect thing to do. I also automated certain features like incrementing the password or box number. The program is not fully automated however. You must run this program manually. It's main purpose is to allow you to run normal phone functions via the keyboard. If you cannot hear clearly through your modem speaker then pick up the phone after the program dials the VMB phone # and hang up the phone before hanging up the modem.

What follows is a brief description on how to use the program, compile the program, and run the program. A working knowledge of VMB systems is expected.

Parameter details

VMB phone number : If you don't know this, give it up.

Setup sequence : This code is used for systems that require a '9' or '#' or '*' to be pressed before the box number. Up to 3 characters can be in this string.

Valid Box # : This would be a known valid box or the box you will be attempting to hack. This value remains constant.

Codefile filename: You may use a file to get 'default' or your favorite passwords from. You must include the extension.

Starting box/code: Box # or code to start checking. This value will increase automatically upon pressing [F7].

Using the function keys

[F1]	Dials the VMB system (see params).
[F2]	Hangs-up the modem.
[F3]	Closes the current codefile.(see params).
[F4]	Lets you set the current code/box #.
[F5]	Dials the Setup sequence (see params).
[F6]	Dials the current code.
[F7]	Makes the next code current.
[F8]	Dials the valid box (see params).
[F9]	Allows you to re-set the parameters.
[F10]	Hangs-up and quits the program.
[0 - 9]	These keys will dial 0 - 9 respectively.
[*, #]	These keys will dial * and #.
[/]	Used as a substitute # for the keypad.

Basic Insructions

Codefiles should be stored in the same directory as your Telix program.

A sample codefile should look like this:

```
1111
2222
3333
etc...
```

I suggest you make seperate codefiles for the number of digits in each code. For example, all 3 digit codes should be in a file called 3DIGIT.COD, or something similar.

During parameter entry, if you enter a codefile and it exists, you will NOT be prompted for a 'Starting box/code'. When the codefile is finished, the current code will set itself to 1000.

If you enter a blank for the codefile or the name you entered doesn't exist then you will be prompted for a 'Starting Box/Code'.

Compiling

Save the program within the 'CUT HERE' lines as VMBHACK.SLT. Copy the file

VMBHACK.SLT into the directory where your Telix scripts are. Compile using CS.EXE. (example: CS VMBHACK.SLT) To run the program, load Telix and press Alt-G followed by the program name (VMBHACK).

```
//----------------------------<CUT HERE>-------------------------------------
//                    ZoSoft VMB Hacker Version 1.4
//                     Code by: Zoso, November 1991
//
//           See PHRACK 34 for more information on VMB systems.
//
// NOTE: Do not remove the credits of the original author, modified versions
//       you may add credits, but please do not remove any.
//
str code[10],                           // Global Variables
    codes[10],
    reset[1],
    vmb_number[15],
    borc[1],
    valid[10],
    setup[3];
str filename[12],
    fstatus[10];
int f;
int fflag = 0;
init_modem()                            // Modem initialization
{
cputs("AT X3 S6=0 S7=0 S11=105 M1 L3"); // X must be 3, L is Loudness on
cputs("^M");                            // some modems, you may have to
waitfor("OK",20);                       // alter this. See you modem
manual.
}
vmb_dial(str string)                    // Dial function
{
str workstr[20];
workstr = string;
strcat(workstr,";");
cputs("ATDT");
cputs(workstr);
cputs("^M");
cputs("^M");
}
hang_up()                               // Hang Up function
{
hangup();
waitfor("",20);
cputs("ATH0");
cputs("^M");
cputs("^M");
clear_scr();
display();
}
next_code()                             // Next code function
{
int cd;
if (fflag)
   {
    if (not feof(f))                    // Check for file first
       {
        fgets(code,10,f);
        return;
       }
    if (feof(f))
       {
        file_close();
        code = "999";
        goto NEXTCODE;
       }
   }
NEXTCODE:
cd = stoi(code);
```

```
cd = cd + 1;                            // This line determines how the
code
itos(cd,code);                          // gets incremented.
}
set_code()                              // Enter new code
{
gotoxy(65,2);
gets(code,10);
}
parameters()                            // Set parameters
{
str c[1];
file_close();
GETINFO:
clear_scr();
printsc("VMB Hacker Parameters^M^J");
printsc("^M^JVMB phone number    :");
gets(vmb_number,15);
printsc("^M^JSetup sequence      :");
gets(setup,3);
printsc("^M^JValid box #         :");
gets(valid,10);
printsc("^M^JCodefile filename   :");
gets(filename,12);
if (filename != "")
   {
    open_file();
    next_code();
   }
if (not fflag)
   {
    filename = "N/A";
    printsc("^M^JStarting box/code   :");
    gets(code,10);
   }
printsc("^M^J^M^JCorrect? (Y/n):");
gets(c,1);
if (c == "n" || c == "N")
    goto GETINFO;
}
press_enter()                           // Pause routine
{
str a[1];
pstraxy("Press [ENTER] to continue...",20,23,11);
gets(a,1);
}
title_scr()                             // Title screen
{
str i[1];
TITLE:
clear_scr();
pstraxy("  - ZoSoft VMB Hacker V1.4 -",20,4,11);
pstraxy("written for Telix by: Zoso Puda",20,6,14);
press_enter();
}
display()                               // Display screen
{
box(0,0,78,3,4,0,19); box(0,0,78,5,4,0,19);
pstraxy("[ ZoSoft VMB Hacker V1.4 ]",25,0,31);
pstraxy("VMB Number:",4,2,31);          // Information display
pstraxy(vmb_number,16,2,27);
pstraxy("Valid #:",33,2,31);
pstraxy(valid,42,2,27);
pstraxy("Current:",57,2,31);
pstraxy(code,66,2,27);
pstraxy("Codefile:",6,4,31);
pstraxy(filename,16,4,27);
pstraxy("File status:",29,4,31);
pstraxy(fstatus,42,4,27);
pstraxy("Setup sequence:",50,4,31);
```

```
pstraxy(setup,66,4,27);
box(0,6,78,10,4,0,103);                 // Function key display
pstraxy("[           ]",30,6,111);
pstraxy(" 0 - 9,*,#",31,6,110);
pstraxy("[  ] Dial VMB", 2,7,111);
pstraxy("F1", 3,7,110);
pstraxy("[  ] Hang up",22,7,111);
pstraxy("F2",23,7,110);
pstraxy("[  ] Close file",42,7,111);
pstraxy("F3",43,7,110);
pstraxy("[  ] Set Current",61,7,111);
pstraxy("F4",62,7,110);
pstraxy("[  ] Setup seq.",2,8,111);
pstraxy("F5", 3,8,110);
pstraxy("[  ] Dial current",22,8,111);
pstraxy("F6",23,8,110);
pstraxy("[  ] Next box/code",42,8,111);
pstraxy("F7",43,8,110);
pstraxy("[  ] Valid box",61,8,111);
pstraxy("F8",62,8,110);
pstraxy("[  ] Parameters",22,9,111);
pstraxy("F9",23,9,110);
pstraxy("[   ] QUIT",41,9,111);
pstraxy("F10",42,9,110);
gotoxy(0,11);
}
quit_vmb()                              // End program
{
file_close();
hangup();
waitfor("",20);
clear_scr();
printsc("Thanks for using ZoSoft's VMB Hacker.^M^J^M^J");
cputs_tr(_mdm_init_str);                // Restore modem params
}
open_file()                             // Open Codefile
{
fflag = 1;
f = fopen(filename,"r");
fstatus = "OPEN";
if (ferror(f))
    file_close();
}
file_close()                            // Close Codefile
{
fflag = 0;
fclose(f);
fstatus = "CLOSED";
}
main()                                  // MAIN program module
{
int chr;
title_scr();
parameters();
clear_scr();
display();
init_modem();
TOP:
gotoxy(0,11);
chr = inkeyw();
if (chr == '0')    vmb_dial("0");       // Dial 0-9
if (chr == '1')    vmb_dial("1");
if (chr == '2')    vmb_dial("2");
if (chr == '3')    vmb_dial("3");
if (chr == '4')    vmb_dial("4");
if (chr == '5')    vmb_dial("5");
if (chr == '6')    vmb_dial("6");
if (chr == '7')    vmb_dial("7");
if (chr == '8')    vmb_dial("8");
if (chr == '9')    vmb_dial("9");
```

```
if (chr == '#')    vmb_dial("#");       // Pound sign (#)
if (chr == '/')    vmb_dial("#");       // Make (/) same as (#) for keypad
if (chr == '*')    vmb_dial("*");       // Asterisk (*)
if (chr == 15104)                       // F1
    vmb_dial(vmb_number);
if (chr == 15360)                       // F2
    hang_up();
if (chr == 15616)                       // F3
   {
    file_close();
    display();
   }
if (chr == 15872)                       // F4
   {
    set_code();
    display();
   }
if (chr == 16128)                       // F5
    vmb_dial(setup);
if (chr == 16384)                       // F6
    vmb_dial(code);
if (chr == 16640)                       // F7
   {
    next_code();
    display();
   }
if (chr == 16896)                       // F8
    vmb_dial(valid);
if (chr == 17152)                       // F9
   {
    hang_up();
    parameters();
    display();
   }
if (chr == 17408)                       // F10
   {
    quit_vmb();
    goto END;
   }
goto TOP;
END:
prints("^M^J");
}
//---------------------------<CUT HERE>---------------------
```

:: More Legal Stuff ::

>From: "Michael Lawrie, Operations" <MICHAEL@hicom.loughborough.ac.uk>
>Subject: RE: Who/What is this?
>
>In this country, the receipt of documents like this would probably be
>pretty helpful in sending a person down on a conspiracy to contravene
>a section or more of the Computer Misuse Act, I do not appreciate crap
>like this appearing on my machine but since you didn't send it me, I
>can't really moan at you - What I would appreciate though is if you
>told people that forwarding it to people who don't want it is probably
>not a good idea, unless you want all your list members locked up in
>some pokey British gaol that is!
>
>Michael Lawrie.
>---
>Michael Lawrie, Hicom Group Security <security@uk.ac.lut.hicom>

- -

Sir,
     You will have to excuse my ignorance of telecom laws in other countries.
In the United States, distribution of technical information such as Phrack Inc.

is protected by law.

Hackers are not involved in conspiracies or plots. Most hackers could care less about politics. Hackers are interested in the progression of technology and learning about how our advanced society works. The inefficient structure known as government is the last thing most hackers are interested in exploring.

Phrack Inc. has no "membership." Phrack Inc. is an electronically distributed publication. It is like any other security oriented newsletter. Have you ever heard of "Computer Security Journal", "Computers and Security", or "Computer Crime Digest?" These are some of the "security industry" publications that are read in the U.S. Phrack Inc. merely has a little different flavor to it. If you are interested in seeing any of these printed journals, I can forward their address to you.

I am sorry if you received Phrack Inc. and didn't wish to read it. You might wish to take the matter up with the person that forwarded it to you. I hope it wasn't too big of an inconvenience for you to delete the mail message containing Phrack Inc.

Cheers,

Dispater

- -

After a (as it turns out not so private) conversation with Torq, it seems this guy isn't even an admin anywhere. He just likes to pretend he is. Did my reply end this little debate? NOT! This person had the nerve to intercept my private mail to Torq and then proceeded to bitch about it some more.

- -

>From MICHAEL@hicom.loughborough.ac.uk Sat Nov 9 09:45:53 1991
Date: Fri, 8 Nov 91 13:19 GMT
From: "Michael Lawrie, Operations" <MICHAEL@hicom.loughborough.ac.uk>
To: PHRACKSUB <<@nsfnet-relay.ac.uk:PHRACKSUB@STORMKING.com>>
Subject: The EFF.

I found the following message the other day, whilst routing around, I am to assume you lied to me about taking him off the list but for now we'll forget that.

> From phrack@gnu.ai.mit.edu Wed Oct 23 01:41:51 1991
> Date: Wed, 23 Oct 91 01:41:47 -0400
> From: phracksub@stormking.com
> Message-Id: <:::::::::::::::::::::>
> To: torq@:::::::::::::::
> Subject: Phrack
>
> This guy sounds like a total idiot. If he does kill your account or something
> stupid, get a hold of the EFF. They went to bat for someone who had their
> account revoked because he/she had issues of Phrack on their directory.
>
> people should get a clue....
>
> Dispater
> phracksub@stormking.com

As you say, people should get a clue. Are you assuming that 'torq' is perhaps American and as such has his rights protected by constitution? He isn't, he is British and doesn't really as such have much going for him. If I want to kill his account I can do it at the bat of an eyelid, whilst him receiving 'Phrack' is not breaking any laws because it does not show intent, it would be breaking my machine's regulations if it came here. I would enjoy the EFF to come 'to bat' for Torq if I revoke his account for having issues of Phrack in his directory, Its a shame he hasn't. Does the EFF have any good lawyers in the UK that you know of?

Regards...
Michael.

Michael Lawrie, Operations Group, Systems Development and Security.
Mail: michael@uk.ac.lut.hicom (Span:19527::60478::lorry)
[What pretentious signature?] (Inet: lorry@mit.edu)

- -

From: Dispater
To: MICHAEL@hicom.loughborough.ac.uk

I never said I would delete him from the distribution list. I don't have to DO anything. Who the hell are you pretending to be anyway? You aren't the admin of MIT's gnu machine.

>I found the following message the other day, whilst routing around, I am to >assume you lied to me about taking him off the list but for now we'll forget >that.

Really? What the hell were you doing prowling though someone else's mail? I assume you did it without Torq's permission. I wonder if MIT would like to hear that some British hacker is rummaging around their machine? Your "finding" of our private e-mail might place you in criminal violation of the Electronic Communications Privacy Act of 1986. This is a federal law in the United States which protects the privacy of electronic communications. Your interception of our communications has violated our privacy. How would you like me to have a little chat with YOUR supervisor?

Why you care about what takes place on the MIT computer which is located here in the USA? In this country freedom of speech is a right granted to all its citizens. The previous publisher of Phrack had to go to Federal Court to prove it and he succeeded. Phrack Inc. is 100% legal here and there is not one damn thing you can do about it!

Dispater

:: Hacker Philosophy ::

From: The Dark Lord Sarik Malthus
Organization: Underground Computing Foundation

> I'm curious...now, don't think I am trying to judge you, or your
> actions, or anything...but I am wondering how you, in your mind, justify the
> actions of hackers and the kind of information provided by your magazine?

I don't. I think people spend too much time attempting to justify their "morality." I don't play that guilt trip. I only seek information. Information has no morality. It is simple and pure, just like truth.

I do feel that with knowledge comes responsibility not to use it in a destructive way. This is why I will not print "how to make bomb" files in Phrack Inc. Explosives are made for one thing and it doesn't involve too much creativity. People can get that type of stuff elsewhere.

I have never damaged any system or hurt any individual financially. Carding is unquestionable robbery. If you know the person you are carding from, that is revenge and is a different category, as far as I am concerned, but it still doesn't make it right. Besides, any poser with half a brain can pull a CBI. That doesn't demonstrate much talent to me. I admit I went through the c0deZ phase, but I moved onto better things.

I guess your basic question may boil down to, "Why hack?" I see the internet and the telecom world in as the latest frontier to be explored. If you look back at how this country started, you will see that it was explored by people who probably had a similar mentality to that of hackers. We want

to test ourselves. We want to have a broad range of different experiences in our lives. We are not content with ignorance of the unknown. And, to some extent we are sick of our current society's norms. With that in mind we leave the security of what is considered acceptable at times.

I guess I have a lot of different unpopular views....oh well.

A Review of:
~~~~~~~~~~

Full Disclosure #23 - a publication For Truth, Justice, and The American Way
~~~~~~

Full Disclosure
P.O. Box 903-FD23
Libertyville IL 60048

Subscription Rates:
U.S - 12 issues for $18.00
24 issues for $29.95
No Canadian orders, please!

by:Twisted Pair

About a month ago I mailed in a coupon I got from friend in order to get a sample issue of Full Disclosure. Within a week I received Issue #23. It's got articles on fax interception, dumpster diving, computer security tips, surveillance tips, technical stuff, mail surveillance, etc.

The Fax Interception article was most interesting to me. I've often wondered just how easy it could be to intercept faxes. Its all explained in the article. Here's some text from the article:

> False Sense of Security:
>
> With the widespread proliferation of fax machines came increased use. In general, a document transferred has been given the same sort of validity as one sent or received by the U.S. Mail.* In general, such communications were originally secure. Now that interception equipment is available, the
> sense of security has become false.

*Note: Just this month, the FCC has stopped accepting paperwork with faxed signatures on them. Their new policy states that they only accept original signatures.

How could the average Phrack reader start intercepting faxes? Use a standard fax machine hooked up to someone's line? Naaah. Wouldn't work. The handshaking routine between the two corresponding fax machines would be screwed all to hell if you threw a third machine into the mix. Full Disclosure claims to have successfully nabbed faxes with another method. They've pointed out this assertion with a photo on their front page of a "fax". It was supposedly intercepted from the FBI. It shows a computer screen with an FBI "FAX" on it. It looks more like the photo was made with some cutting and pasting at the neighborhood PIP store. Maybe they should have added the caption "Simulated Picture" to their front page.

They recommend using IBM PC fax boards to intercept faxes. You'd need "sophisticated" software that would ignore the handshaking sequences between the two fax machines you're spying on. The IBM would just save all the page information and ignore the protocol information transmitted.

Back to the article....

> Cellular phone-based fax machines provide ripe opportunity for "hacker" intercepts, since the signal is available via low cost police scanners.* No physical connection to a common carrier network is necessary. There is absolutely no risk of being detected.

*Note: That should read MODIFIED police scanners. See any of the ads in "Nuts & Volts" for a book on doing this.

Discussed in the article is something called Broadband Interception. Commercial fax interception equipment can be hooked up to monitor satellite link traffic. One unit can decode up to 150 simultaneous fax transmissions

from a 6,000 phone line satellite link.

Next, all the consequences of forged faxes are discussed. People have become so reliant on fax technology that they incorrectly assume that anything that "comes over the fax" must be legitimate. Forgers find faxing much simpler than trying to make a "real" document. The trouble of altering postmarks and signatures is bypassed. All they need now is scissors and tape to make any "legitimate-looking" document needed. In their next issue, they further discuss fax interception and all the implications of sending sensitive info by fax.

```
|                        Fax Intercept Suppliers
|          (The sale and/or use of fax interception equipment may be
|                  restricted by State and Federal law)
|
|   Burlex International, Box 6094, Silver Springs MD 20906 (301) 460-4444;
|   Communications Devices,3510 Mountain Rd,Haymarket VA 22069 (703) 754-9316;
|   El-Tec Intl, 205 Van Buren St #220, Herndon VA 22080 (703) 709-9673;
|   [Many others listed]
```

Oh, here's an ad from Full Disclosure. It's a business card run:

```
|   ____________________________________________________________
|   |                                                           |
|   | Unix Systems Specialists     Available July 10, 1992      |
|   |                                                           |
|   |               L  E  N       R  O  S  E                   |
|   |                                                           |
|   |                  Convicted "Hacker"                       |
|   |                         and                               |
|   |                Computer  Consultant                       |
|   |              799 Royal St. Geore  #105                    |
|   |          Naperville, IL 60563  (708) 527-1293             |
|   |___________________________________________________________|
```

Since you might want to check out a copy of Full Disclosure for yourself, I'll include their address and stuff. The issue I had was 16 pages long, half-newspaper size.

A Review of TAP #105
~~~~~~~~~~~~~~~~~~~

TAP Magazine
PO Box 20264
Louisville KY 40250-0264

Subscription Rates:
10 issues for $10.00

by Dispater

Around March of 1991 I mailed in my $10. for a subscription to TAP Magazine. Promoted as "the oldest hacker magazine" and "created by Abbie Hoffman." I still, to this day, have not received ONE issue for my money.

While attending CyberView '91, I met Predat0r and gave him $5.00 for a few back issues consisting of #97, #100 through issue #104. I was later given a complimentary issue of #105. After asking about #98 & #99, Predat0r said that he wasn't going to give those out because of some bullshit with Aristotle. Whatever...I still don't see why we couldn't see it.

Anyway, Issue #105 of TAP Magazine (June 1991) was nothing spectacular, but it wasn't bad either. The issue was 18 pages long. For those of you who have never seen it, TAP contains information on hacking and phreaking as well as some political commentary. The articles are always diverse and interesting.

TAP #105 contained information about the DNA Box. This is basically cellular phone phreaking. It was very good and quite detailed. There were also schematics of bugs and a flow chart explaining the incident initiation sequence of the E-911 system. This issue of TAP was sprinkled with some neat advertisements and news clippings (as usual) and wrapped up with a file about Blue Boxing. The price of $10.00 for 10 issues is worth it, but read on...
~~~~~~~~~~~~~~~~~~~

Last week I asked Predat0r what was going on with TAP magazine. He told me that he had the material for the next three issues, but his copier or some other equipment was broken. This is an excuse I have heard before. Whether it is a valid excuse or not, only he knows. Since issue #105 (June) there has been not one issue of TAP. If you have ordered a subscription prior to July and not received anything, I highly suggest you write to Predat0r.

The material contained in TAP is good and very much worth the price. (Especially compared to 2600 Magazine) However, I find that the general management of TAP to be poor, at this time, and therefore I highly recommend that you NOT send your $10 to TAP Magazine. Considering the amount of advertisements that we have all seen by TAP (in magazines such as Mondo 2000, 2600, etc.) in the past year, there is no excuse for the non-existent service that has transpired. Predat0r is a good sysop and needs to manage TAP as he does his BBS. I do urge you to call BLITZKREIG BBS (502) 499-8933 : NUP: COLUMBIAN COKE.

I really don’t like to be so critical, but I know some people I’ve talked to are feeling ripped off. This is why I wrote this. I truly hope that TAP can get out of this slump.

==Phrack Inc.==

Volume Three, Issue Thirty-five, File 3 of 13

-*[P H R A C K XXXV P R O P H I L E]*-

-=>[Presents]<=-

Sincerely Yours, Chris Goggans

by S. Leonard Spitz
Associate Publisher
INFOSecurity Product News

"A provocative interview with a former member of the "Legion of Doom" suggests that the ethics of hacking (or cracking) are often in the eye of the beholder."

Malicious hackers, even though most operate undercover, are often notorious for the colorful pseudonyms they travel under. Reformed hackers, however, prefer a low profile so as to shed their image of perceived criminality. Kevin Mitnick, infamous for the DEC caper, is one of the foremost advocates of this strategy.

Now comes Chris Goggans, trailing his former "Legion of Doom" moniker, Erik Bloodaxe, behind him, to try it his way. Goggans insists that where once he may have bent the rules, he is now ready to give something back to society. And coming across with a high degree of sincerity, he affirms his intention to try. Are he and his colleagues, wearing their newly acquired information security consultants hats, tilting at windmills, or does their embryonic, cracker-breaking start-up, Comsec Data Security Co., stand a fighting chance? We thought we would ask him.

- -

ISPNews: I am going to ask several legitimate questions. Please answer them completely, truthfully, and honestly.

Chris Goggans: OK.

JUDGEMENT BY THE MEDIA

ISPNews: Would you react to Computerworld's July 29 piece, "Group Dupes Security Experts," <also seen in Phrack World News issue 33, part 2 as part of the article called "Legion of Doom Goes Corporate> in which members of your organization were accused of masquerading as potential customers to obtain information, proposals, and prices from other security consultants?

CG: We were all amazed that something like that would ever be printed because, as we understand common business practices, we weren't doing anything unusual.

ISPNews: Computerworld reported that the Legion of Doom was "one of the nation's most notorious hacker groups, according to federal law enforcers." Can you respond to that?

CG: Notorious is a relative term. There has always been a shroud of mystery covering the Legion of Doom, because it was an organization whose membership was private. When you keep people in the dark about the activities of something, there is always going to be the perception that more is going on than there really is.

ISPNews: Would you say then that the characterization of being notorious is unfair?

CG: To some degree, yes. There certainly was activity going on within the group that could be considered illegal. But most of this was taking place when members of the group were all between the ages of 14 and 17. While I don't want to blame immaturity, that's certainly a factor to be considered.

The Legion of Doom put out four <issues of an> on-line electronic newsletter <called the Legion of Doom Technical Journals> composed of different files relating to various types of computer systems or netware. They explained different operating systems or outlined different procedures used by networks. They were always informative and explained how to use a computer. We never said "This is a computer and this is how to break into it."

Colorful names and words used to describe groups also add to notoriety. If we had been the "Legion of Flower Pickers," the "Legion of Good Guys," or the "SuperFriends," there probably wouldn't be this dark cloud hanging over the group.

ISPNews: Could you be charged with intent to provide information to others which would make it easier to gain unauthorized access?

CG: I don't see how that could be a charge. There's the first amendment. I maintain that talking about something and encouraging or forcing someone to do it are completely different.

EARNING AN "A" IN INFOSECURITY

ISPNews: What attracted you to computer security?

CG: The same thing that would attract anybody to being a hacker. For half of my life I've been in front of a computer every day. Sometimes from early in the morning until the wee hours of the night. And my particular focus has been on computer security.

ISPNews: At least the dark side of that coin.

CG: I wouldn't say the dark side. I'd say the flip side. If you do something for 11 years, you are going to pick up a lot of knowledge. And I've always wanted to find some kind of productive career that I thoroughly enjoyed. So this was just an obvious progression. No one wants to be a 40-year-old hacker living in fear of the Secret Service.

ISPNews: When you first applied to enter college, did you feel that it was the right place to learn about information security?

CG: Yes, I thought it was the right place, mainly because college is the most obvious choice to pursue an education in any field. I just assumed that I would be able to find formal training leading to certification or a degree in this field. Yet, at the University of Texas, there wasn't anything along those lines.

ISPNews: Did you graduate from the University of Texas?

CG: No, I changed majors and then moved to Houston. I had started out in computer science but it was completely unrelated to any kind of career I wanted to pursue. I eventually changed my major to journalism. There are only two things I like to do: Work on computers, and write. So, if I wasn't going to get a degree in one, it was going to be in the other. I'm a semester away, and I do plan on finishing.

ISPNews: If you were to structure a college curriculum for studies in information security, would you design it to focus on technical issues, ethics, business issues, or legal matters?

CG: I would try to focus on all of these. If you don't have a technical background, you can't understand the way the operating system works, and you really can't focus on some of the issues that need to be addressed with information security.

Ethics certainly come into play ass well for obvious reasons. I don't think hackers are going to go away. Even with the advent of

newer technology, there are always going to be people who have an interest in that technology and will learn how to manipulate it.

ETHICS, INTELLECTUAL PROPERTY RIGHTS, AND THE LAW

ISPNews: What is your definition of a hacker?

CG: A Hacker is someone who wants to find out everything that there is to know about the workings of a particular computer system, and will exhaust every means within his ability to do so.

ISPNews: Would you also comment on the ethics of hacking?

CG: There is an unwritten code of ethics that most people tend to adhere to. It holds that: no one would ever cause damage to anything; and no one would use any information found for personal gain of any kind.

For the most part, the only personal gain that I have ever seen from any sort of hacking activity is the moderate fame from letting others know about a particular deed. And even in these cases, the total audience has been limited to just a few hundred.

ISPNews: Are you unaware of hackers who have in fact accessed information, then sold it or massaged it for money?

CG: No, certainly not. I am just acknowledging and defining a code of ethics. We of the Legion of Doom tried to adhere to that code of ethics. For example, members of the original nine who acted unethically were removed from the group.

ISPNews: Do you believe that penetrating a computer system without either making changes or removing information is ethical, or a least is not unethical?

CG: At one time in the past I may have held that belief, but now I certainly must not, because the whole idea of being involved in the formation of my new company, Comsec Data Security, would show otherwise.

ISPNews: So today, you believe that unauthorized entry is unethical.

CG: Exactly. As a hacker, I didn’t particularly hold that. But as things such as invasion of privacy, even though I never caused any damage, and breach of trust became more apparent to me, I was able to step back, see the picture, and realize it was wrong.

ISPNews: Can I conclude that you are speaking for you company and its principals?

CG: Yes, I am speaking for all of the principals.

ISPNews: What are your views on the ownership of information?

CG: I feel that proprietary information, national-security-related information, information that could be considered a trade secret, all definitely have ownership, and access should be restricted.

In the past, I felt that information that affected me or had some relevance to my life should be available to me. I felt that information should be available to the people it affected, whether that be phone company information, credit bureau information, banking information, or computer system information in general. I am saying this in the past tense.

In the present tense, I feel that the public is entitled only to information in the public domain. Information not available legally through normal channels is just going to have to be left at that.

ISPNews: Do you believe that software should always be in the public

domain.?

CG: No, I do not. If I wrote something as wonderful as Lotus, or any of the Microsoft programs, or Windows, I would want people to pay for them.

ISPNews: Then you do believe in private ownership of and protection for software?

CG: Yes, definitely.

ISPNews: What are you views on current U.S. Computer crime laws?

CG: I think that the current laws are too broad. They do not make distinctions between various types of computer crimes. I consider breaking into a computer akin to trespassing. If someone simply walks across my lawn, I might be upset because they trampled my grass, but I would leave it at that. If someone drives across my lawn and leaves big trenches, and then comes over and kicks down my rosebush, well that's another thing. Then, if someone drives up my steps, goes through my house, through my kitchen, steals all my silverware, and then leaves, that's something completely different. And while these physical representations of trespassing can't be applied directly to an electronic format, distinctions are still necessary.

ISPNews: And the present computer crime laws do not make these distinctions?

CG: I am no lawyer, but from my understanding they do not. They need to be brought into focus.

ISPNews: If they were brought into the kind of focus you suggest, would they be fair and equitable?

CG: Definitely, depending on the punishment that went along with them. I don't think that people who own and operate computer systems would view someone who has logged into their system using a guest account that was deliberately left with no password to be as serious an intrusion as someone who got the system administrator password and then went through and deleted all the files. I don't think that simple intrusion would be considered as serious as unauthorized penetration along with the wholesale theft and sale to a competitor of marketing information, and advertising plans, and financial projections for the next quarter.

ISPNews: What are your views on security training for users?

CG: People need to be taught what the computer operating system is and how it works. After that, they need to establish some sort of channel by which information can be transmitted to others. Direct physical contact between communicating parties, covered by official, standard company procedures, is the best way to do this.

People need to be aware that their account, no matter the level of importance, is a link in a chain that makes up the security of the system. Information from one account can be used as a springboard to other, more powerful accounts. All users within a network must understand that their information is just as important in the security chain as is that of the next person.

ISPNews: Given where you are coming from, why should a potential client trust you?

CG: I know that is a natural question. Just the very nature of creating a company should project an image that we are trying to come out of the shadows, out of the underground. We are saying, "Look everybody, we've been doing this for a long time, now we want to help. We have 11 years of working information about how people compromise existing security, and we can help with your particular situation."

ISPNews: I am sure that you understand the natural suspicion that people have.

CG: No, that's what I don't understand. If we at Comsec were out to compromise information from an existing company's computer network, we wouldn't have incorporated. We could have done that, and someone else out there probably has already done so. Then the information would be available to from one hacker to another.

ISPNews: Are you suggesting there is no system out there that you can't break into?

CG: No, I'm not suggesting that. But I am saying the vast majority can be penetrated.

ISPNews: Which system is easiest to crack; and which is most difficult?

CG: It is hard to say which system is more inherently penetrable than another. From the initial log-in, it's not the operating system; rather it's the system's operating environment that is the problem. Users may not have addressed security measures. Certain types of security holes may not have been closed. That's where a technical background comes into play: to understand the way the applications work; how different systems are accessed; to close holes in the system which have become apparent. You have to deal with human factors and technical issues. You must understand the way the computer works and the way programs are run.

ISPNews: What is the best way to foil hackers?

CG: It depends on the hacker. There are different types. Some people hack with modems. The casual hacker may just stumble across your particular computer system, and may be foiled with something as simple as good external security. He may be turned off by physical security devices such as a call-back modem, some sort of code access, or smart card.

These measures will not stop a serious hacker who is after your company specifically. In this case, you have to beef up security, and take additional steps to ensure the safety of your computer. And you must make certain that security on the inside is as tight as on the outside.

ISPN Editor's Note: Chris Goggans will respond, in every other issue of ISPNews, to your questions on hacking computer systems. His answers promise to be problem-solving, interesting, and even entertaining. We invite you to write Chris c/o:

"Hackers' Mailbag"
ISPNews
498 Concord Street
Framingham, MA 01701-2357

==Phrack Inc.==

Volume Three, Issue Thirty-five, File 4 of 13

Amadeus Presents

////////////////////////////////////\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

<<<<<<<<<<<<< TELENET/SPRINTNET'S PC PURSUIT OUTDIAL DIRECTORY >>>>>>>>>>>

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\////////////////////////////////////

October 25, 1991

Area Code	City, State U.S.A.	300 bps	1200 bps	2400 bps
201	Newark, New Jersey	311020100001	311020100301	311020100022
	NJNEW	2011	201301	20122
202	Washington, D.C.	311020200115	311020200116	311020200117
	DCWAS	202115	202116	202117
203	Hartford, Connecticutt	311020300120	311020300121	311020300105
	CTHAR	203120	203121	203105
206	Seattle, Washington	311020600205	311020600206	311020600208
	WASEA	206205	206206	206208
212	New York, New York	311021200315	311021200316	311021200412
	NYNYO	212315	212316	212412
				311021200028
				21228
213	Glendale, California	Same as 818,see 818's NUAs & addresses		
	CAGLE	(Dial 1213+number)		
213	Los Angeles, California		311021300412	311021300413
	CALAN		213412	213413
			311021300103	311021300023
			213103	21323
213	Santa Ana, California	Same as 714,see 714's NUAs & addresses		
	CASAN	(Dial 1213+number)		
214	Dallas, Texas	311021400117	311021400118	311021400022
	TXDAL	214117	214118	21422
215	Philadelphia, Pennsylvania	311021500005	311021500112	311021500022
	PAPHI	2155	215112	21522
216	Cleveland, Ohio	311021600020	311021600021	311021600120
	OHCLE	21620	21621	216120
301	Washington, D.C.	Same as 202,see 202's NUAs & Addresses		
	DCWAS	(Dial 1301+number)		
303	Denver, Colorado	311030300114	311030300115	311030300021
	CODEN	303114	303115	30321
305	Miami, Florida	311030500120	311030500121	311030500122
	FLMIA	305120	305121	305122
312	Chicago, Illinois	311031200410	311031200411	311031200024
	ILCHI	312410	312411	31224
313	Ann Arbor, Michigan	No 300 bps		
	MIAAR	access		
313	Detroit, Michigan	311031300214	311031300216	311031300024
	MIDET	313214	313216	31324
314	St. Louis, Missouri	311031400020	311031400021	311031400005
	MOSLO	31420	31421	3145
317	Indianapolis, Indiana	No 300 bps		
	ININD	access		
404	Atlanta, Georgia	311040400113	311040400114	311040400022
	GAATL	404113	404114	40422
407	Miami, Florida	Same as 305,use 305's NUAs & addresses		
	FLMIA	(Dial 1407+number)		
407	Orlando, Florida	No 300 bps		
	FLORL	access		
408	San Jose, California	311040800110	311040800111	311040800021
	CASAN	408110	408111	40821
412	Pittsburgh, Pennsylvania	No 300 bps		
	PAPIT	access		
414	Milwaukee, Wisconsin	311041400020	311041400021	311041400120
	WIMIL	41420	41421	414120
415	Oakland, California	311041500108	311041500109	311041500224
	CAOAK	415108	415109	415224
415	Palo Alto, California	311041500108	311041500011	311041500005

	CAPAL	415108?	41511	4155?
415	San Francisco, California	311041500215	311041500217	311041500217
	CASFA	415215	415217	415217?
415	San Jose, California	Same as 408,use 408's NUAs & addresses		
	CASJO	(Dial 1415+number)		
503	Portland, Oregon	311050300020	311050300021	
	ORPOR	50320	50321	
504	New Orleans, Louisiana	No 300 bps		
	LANOR	access		
512	Austin, Texas	No 300 bps		
	TXAUS	access		
516	Hempstead, New York	No 300 bps	311051600014	
	NYHEM	access	51614	
516	New York, New York	Same as 212,use 212's NUAs & addresses		
	NYNYO	(Dial 1516+number)		
601	Memphis, Tennessee	Same as 901,use 901's NUAs & addresses		
	TNMEM	(Dial 1601+number)		
602	Phoenix, Arizona	311060200020	311060200021	
	AZPHO (Some 602 numbers require 1602+number, see exchange database below)	60220	60221	
		311060200022	311060200023	311060200026
		60222	60223	60226
612	Minneapolis, Minnesota	311061200120	311061200121	311061200022
	MNMIN	612120	612121	61222
614	Columbus, Ohio	No 300 bps		
	OHCOL	access		
617	Boston, Massachusetts	311061700311	311061700313	311061700026
	MABOS	617311	617313	61726
618	St. Louis, Missouri	Same as 314,use 314's NUAs & addresses		
	MOSLO	(Dial 1618+number)		
619	San Diego, California			
	CASDI			
703	Washington, D.C.	Same as 202,use 202's NUAs & addresses		
	DCWAS	(Dial 1703+number)		
708	Chicago, Illinois	Same as 312,use 312's NUAs & addresses		
	ILCHI	(Dial 1708+number)		
713	Houston, Texas	311071300113	311071300114	311071300024
	TXHOU	713113	713114	71324
714	Colton, California	311071400119	311071400121	311071400102
	CACOL	714119	714121	714102
714	Santa Ana, California	311071400023	311071400024	311071400021
	CASAN	71423	71424	71421
		311071400210	311071400213	311071400004
		714210	714213	7144
718	New York, New York	Same as 212,use 212's NUAs & addresses		
	NYNYO	(Dial 1718+number)		
801	Salt Lake City, Utah	311080100020	311080100021	311080100012
	UTSLC	80120	80121	80112
813	Tampa, Florida	311081300020	311081300021	311081300124
	FLTAM	81320	81321	813124
815	Chicago, Illinois	Same as 312,use 312's NUAs & addresses		
	ILCHI	(Dial 1312+number)		
816	Kansas City, Missouri	311081600104	311081600221	311081600113
	MOKCI	816104	816221	816113
817	Dallas, Texas	Same as 214,use 214's NUAs & addresses		
	TXDAL	(Dial 1817+number)		
818	Glendale, California	311081800021		
	CAGLE	81821		
818	Los Angeles, California	Same as 213,use 213's NUAs & addresses		
	CALAN	(Dial 1818+number)		
901	Memphis, Tennessee	No 300 bps		
	TNMEM	access		
908	New Brunswick, New Jersey	No 300 bps		
	NJNBR	access		
908	Newark, New Jersey	Same as 201,use 201's NUAs & addresses		
	NJNEW	(Dial 1908+number)		
913	Kansas City, Missouri	Same as 816,use 816's NUAs & addresses		
	MOKCI	(Dial 1913+number)		
914	New York, New York	Same as 212,use 212's NUAs & addresses		
	NYNYO	(Dial 1914+number)		
916	Sacramento, California	311091600011	311091600012	311091600007

	CASAC	91611	91612	9167
919	Research Triangle Park,N Carolina	311091900020	311091900021	311091900124
	NCRTP	91920	91921	919124

KEY: NUA (X.25 International Inter-Network User Address)------>311012300456
Sprintnet/Telenet's Intra-network address ---------------> 123456

PC Pursuit Outdial City/Area Code Cross Reference Directory

Ann Arbor, Michigan	313	New Brunswick, New Jersey	908
Atlanta, Georigia	404	New Orleans, Louisiana	504
Austin, Texas	512	New York, New York	212,516,718 &914
Boston, Massachusetts	617	Newark, New Jersey	201 &908
Chicago, Illinois	312, 708 & 815	Oakland, California	415
Cleveland, Ohio	216	Orlando, Florida	407
Colton, California	714	Palo Alto, California	415
Columbus, Ohio	614	Philadelphia, Pennsylvania	215
Dallas, Texas	214 & 817	Phoenix, Arizona	602
Denver, Colorado	303	Pittsburgh, Pennsylvania	412
Detroit, Michigan	313	Portland, Oregon	503
Glendale, California	213 & 818	Research Triangle Park,N Carolina	919
Hartford, Connecticutt	203	Sacramento, California	916
Hempstead, New York	516	Salt Lake City, Utah	801
Houston, Texas	713	San Diego, California	619
Indianapolis, Indiana	317	San Francisco, California	415
Kansas City, Missouri	816 & 913	San Jose, California	408 &415
Los Angeles, California	213 & 818	Santa Ana, California	213 &714
Memphis, Tennessee	601 & 901	Seattle, Washington	206
Miami, Florida	305 & 407	St. Louis, Missouri	314 &618
Milwaukee, Wisconsin	414	Tampa, Florida	813
Minneapolis, Minnesota	612	Washington, D.C.	202, 301 &703

Preface

The PC Pursuit outdials, although limited in their dialing range, are of fundamental knowledge to any X.25 hacker in the world. Collecting the addresses of the PC Pursuit outdials is among the first projects of any hacker new to the X.25 hacking arena. On and off through the years since 1986 when I first happened upon the X.25 scene, I have been attempting to compile the complete list of NUAs for all of the outdials. I still haven't realized this goal five years later, as can be evidenced by blanks in the above list.

Other outdials, such as the ones hacked out of explorations of internal corporate, government, or educational networks, come and go usually as fast as codes. Some of these outdials are prize finds that can dial any number in the world and would supplant the usefulness of this list. But such out-dials are normally gone in a matter of weeks. The ones that do stay around (such as the infamous 30209160xxxx global outdials) do not work very well. Of course there are exceptions to every rule. Some Global OutDials (GODs) go on working for years, but only because they are known only by one or a few hackers who don't go around giving it to everyone in hackerdom far and wide.

The PC Pursuit outdials have been functioning without fail for several years and will continue to be a reliable and useful hacker's tool for the foreseeable future. You can count on them to be there when you need them, especially when a GOD you've been using fails and you need something to fall back on. I have put together these two files to help further facilitate your use of the PC Pursuit outdials. I hope you find them useful references.

Some Notes for Beginners

All the modems that you access on the outdials are of the Racal-Vadic brand and accept the standard Hayes AT command set as a default. I will not go into an explanation of AT commands since you should already know them as a competent user of your computer and modem. If not, check your modem's

manual since it is almost certainly a Hayes compatible modem.

The Racal-Vadic modem offers its own command mode as an alternative to the industry standard Hayes AT command set. To access the Racal-Vadic mode, type a CTRL-E and then RETURN. You will see "READY" and an asterisk for a prompt. Type "?" for a list of commands. This mode is more attractive to many users because of its verbose interface and detailed call progress messages; because fewer keystrokes are needed to execute commands such as dial, and because of its ability to redial up to nine times until a connection is made.

None of the outdials allow you to call them collect. You will have to call them from either a PAD (Packet Assembler Deassembler) or NUI (Network User ID). PC Pursuit IDs can also be used as pseudo-NUIs by typing the NUA followed by a comma, the PCP ID, another comma, and the PCP Password. If you do not already have one, you will have to consult a fellow hacker for a valid NUI or PAD (not as freely traded nowadays). Or, to really impress your hacker friends, hack your own. (Consult other files featured in Phrack that deal with this subject matter.)

The 12 digit NUA (Network User Address) for each outdial above is for accessing the outdial from a network other than SprintNet/Telenet.

The shorter five to six digit number below it is for accessing the outdial from SprintNet/Telenet. Actually, you can use the 12 digit number as well as the shorter five to six digit number (if you precede the 12 digit NUA with a 0) on SprintNet, but the shorter one is easier to remember and use.

For the purposes of memorizing the outdials that you will use more often, it is a simple matter of remembering the shorter SprintNet address and convert- ing it to the 12 digit NUA as needed like this:

SprintNet address xxxyyy becomes 3110xxx00yyy (Add 0's in yyy where needed)
EXAMPLE: 813124 becomes 311081300124
EXAMPLE2: 4155 becomes 311041500005 (Add preceding 0's in yyy)

Note that networks usually require you to precede the NUA with a 0 or 1 (usually 0) much like when you dial a long distance phone call. For example, on Tymnet, typing an NUA does not require a 0 or 1. On Canada's DataPac, a 1 is required before the 12 digit NUA. On SprintNet and most European X.25 networks, a 0 is needed.

When you connect with an outdial modem, the first thing you might want to do is to redial the last number dialed. The last person who used the modem might have called a number that would be of interest to you in your hacking endeavors. Enter the Racal-Vadic mode and execute the "R" redial command. The last number dialed is shown on the screen and dialed. The A/ command in the Hayes AT command mode won't work for this purpose since the last number dialed is not shown and the last command executed isn't necessarily a dialing command.

Unfortunately, when a person exits the outdial, the modem resets itself in most cases and the last number dialed is lost. But occasionally you'll get lucky and find an interesting new number to call

Calling Specific Modems, and GODs (Global OutDials)

Each outdial has many modems that you can connect to. When calling the outdial NUA, you will be connected to the first available modem. If all are being used, you will get a busy message. It is possible for you to attempt to connect to one particular modem in the series rather than connect to the first available unused modem.

Append two digits to the end of a NUA to specify which modem you want. For example, to connect to the third modem on 311061200022, you would call NUA 31106120002203. So theoretically, you can call up to 99 different modems on the same outdial (31106120002200 is the same as 311061200022), but no outdials have this many modems.

On SprintNet, you can append a letter to the four to six digit address

to specify a modem. You can also add a decimal point and then the two digits for modems above 26 (and below). For example, 31106120002203 is the same as 61222C and 61222.03; 31108130012426 is the same as 813124Z and 813124.26.

So, you may ask, why would I want to call a specific modem?

The reason is that some modems permit unrestrictive dialing. Such modems will let you dial ANY number in the world, not just the local numbers that you're only suppose to call. Such modems are known as GODs, which stands for Global OutDial.

GODs don't last forever. As soon as the SprintNet priests discover the abuse occurring on a particular modem, they'll fix it. So you'll have to talk with your fellow hackers to find out which modems are known to be GODs, or better yet, scan for your own.

Local Exchange Database

For those using the outdials from international locations, it is important to note that you cannot call just any number in the same area code as the outdial. Unless you're using a GOD (see part A), you can only dial numbers local to the city the outdial is in.

At the end of this file you will find a database of all the exchanges (the three numbers in a telephone number after the area code) that are dial-able from each outdial. This database will not only be useful to verify for sure that you can dial a particular number from a PC Pursuit outdial, but will also be useful for checking which outdial to use in cases where multiple outdials can be used to dial different numbers in the same area code. For example you can dial numbers in area code 213 from THREE different outdials: 213 CALAN, 818 CAGLE, *and* 714 CASAN. Unless you are familiar with the geographic dialing plan of the Los Angeles area, you would have to consult the exchange database to figure out which outdial to use.

The raw data for the list was downloaded from the PC Pursuit Service BBS (call collectable from SprintNet at 311090900631, @C PURSUIT or @909631; logon as "Sprint Guest" with password "outdial"). I made some very time consuming modifications to the format of the list so that it could be used effectively with Unix's grep command or MS-DOG's FIND command (and similar commands on other operating systems).

For example, let's say you wanted to call a BBS at 213-395-0221. As I mentioned earlier, there are three different outdials that can dial numbers in the 213 area code. You have to find out which one to use. On Unix, you would type:

```
% grep 213 <filename>|grep 395
```

Or on MS-DOS, you would type:

```
C:\>FIND "213" <filename>|FIND "395"
```

where <filename> is the name this file is saved under. You will then see:

```
 OB
1 213 CAGLE 393 394 395 396 399 400 413 415 450 451 452 453 454 455 458
  213 CALAN 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400
```

As you can see, you can call 1-213-395-0221 from two outdials: CAGLE and CALAN. But notice that the CAGLE outdial has a 1 in front of it. This means that if you use the CAGLE outdial, you will have to dial with the toll prefix (1) and area code preceding the local number since CAGLE is in the 818 area code.

Dialing from CAGLE: ATDT12133950221
Dialing from CALAN: ATDT3950221

The Database

```
  602 AZPHO 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234
  602 AZPHO 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249
  602 AZPHO 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264
  602 AZPHO 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279
  602 AZPHO 280 285 320 331 336 340 345 350 351 352 370 371 375 376 377
  602 AZPHO 379 381 382 389 390 391 392 393 395 396 397 412 420 423 431
  602 AZPHO 433 434 435 436 437 438 439 440 441 443 450 451 460 461 464
  602 AZPHO 468 470 481 482 483 484 486 490 491 493 494 495 496 497 498
  602 AZPHO 528 530 531 534 540 542 543 545 547 548 549 551 553 554 563
  602 AZPHO 585 588 589 596 597 598 630 631 640 641 644 649 650 661 678
  602 AZPHO 681 693 730 731 732 752 756 759 784 786 788 789 820 821 827
  602 AZPHO 829 830 831 832 833 834 835 838 839 840 841 842 843 844 846
  602 AZPHO 848 849 852 853 856 860 861 862 863 864 866 867 869 870 872
  602 AZPHO 873 876 877 878 879 890 891 892 893 894 895 897 898 899 921
  602 AZPHO 924 925 926 929 930 931 932 933 934 935 936 937 938 939 940
  602 AZPHO 941 942 943 944 945 946 947 948 949 951 952 953 954 955 956
  602 AZPHO 957 961 962 963 964 965 966 967 968 969 970 971 972 973 974
  602 AZPHO 975 977 978 979 980 981 985 986 990 991 992 993 994 995 996
  602 AZPHO 997 998
1 602 AZPHO 566 583 584 546 492 561 581 582 780 569 586 471 837 373 380
1 602 AZPHO 983 982 984 986 983 671 987 988
  714 CACOL 275 276 335 350 351 352 353 354 355 356 357 358 359 360 369
  714 CACOL 370 381 382 383 384 386 387 422 431 602 681 682 683 684 685
  714 CACOL 686 687 688 689 749 780 781 782 783 784 785 787 788 789 790
  714 CACOL 791 792 793 794 795 796 797 798 799 820 822 823 824 825 829
  714 CACOL 872 873 874 875 876 877 880 881 882 883 884 885 886 887 888
  714 CACOL 889
1 213 CAGLE 201 202 203 204 205 221 222 223 224 225 226 227 228 229 230
1 213 CAGLE 236 237 238 239 245 250 251 252 253 254 255 256 257 258 259
1 213 CAGLE 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284
1 213 CAGLE 285 286 287 288 289 303 310 314 315 319 340 341 342 343 345
1 213 CAGLE 347 351 353 362 380 381 382 383 384 385 386 387 388 389 392
1 213 CAGLE 393 394 395 396 399 400 413 415 450 451 452 453 454 455 458
1 213 CAGLE 459 460 461 462 463 464 465 466 467 468 469 480 481 482 483
1 213 CAGLE 484 485 486 487 488 489 520 550 551 552 553 556 557 558 559
1 213 CAGLE 573 580 612 613 614 617 619 620 621 622 623 624 625 626 627
1 213 CAGLE 628 629 650 651 652 653 654 655 656 657 658 659 660 661 662
1 213 CAGLE 663 664 665 666 667 668 669 680 681 682 683 684 686 687 688
1 213 CAGLE 689 714 730 731 732 733 734 735 736 737 738 739 740 741 742
1 213 CAGLE 743 744 745 746 747 748 749 765 785 828 829 836 837 838 839
1 213 CAGLE 840 841 842 849 850 851 852 854 855 856 857 858 859 870 871
1 213 CAGLE 872 873 874 875 876 877 878 879 891 892 893 894 895 896 912
1 213 CAGLE 913 930 931 932 933 934 935 936 937 938 939 955 960 962 963
1 213 CAGLE 964 965 966 967 968 969 972 974 975 977
  818 CAGLE 200 240 241 242 243 244 246 247 248 249 301 303 304 350 351
  818 CAGLE 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366
  818 CAGLE 367 368 370 371 372 373 374 375 376 377 378 379 381 382 393
  818 CAGLE 397 398 399 400 401 402 403 404 405 406 409 440 441 442 443
  818 CAGLE 444 445 446 447 448 449 450 459 500 501 502 503 504 505 506
  818 CAGLE 507 508 509 528 542 545 546 547 548 560 564 565 566 567 568
  818 CAGLE 569 574 575 577 578 579 580 584 753 754 760 761 762 763 764
  818 CAGLE 765 766 767 768 769 777 780 781 782 783 784 785 786 787 788
  818 CAGLE 789 790 791 792 793 794 795 796 797 798 799 818 821 831 840
  818 CAGLE 841 842 843 845 846 847 848 890 891 892 893 894 895 896 897
  818 CAGLE 898 899 901 902 903 904 905 906 907 908 909 951 952 953 954
  818 CAGLE 955 956 957 972 980 981 982 983 984 985 986 987 988 989 990
  818 CAGLE 994 995 997
  213 CALAN 200 201 202 203 204 205 206 207 208 209 212 214 215 216 217
  213 CALAN 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233
  213 CALAN 234 235 236 237 238 239 241 245 248 249 250 251 252 253 254
  213 CALAN 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269
  213 CALAN 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284
  213 CALAN 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299
  213 CALAN 300 301 302 303 304 305 306 307 308 309 310 312 313 314 315
  213 CALAN 316 318 319 320 321 322 323 324 327 328 329 330 331
  213 CALAN 334 335 336 337 338 340 341 342 343 345 347 351 353 362 370
  213 CALAN 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385
  213 CALAN 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400
  213 CALAN 402 404 406 408 410 412 413 414 415 416 417 418 419 440 442
```

```
  213 CALAN 443 444 445 446 447 450 451 452 453 454 455 458 459 460 461
  213 CALAN 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476
  213 CALAN 477 478 479 480 481 482 483 484 485 486 487 488 489 500 512
  213 CALAN 515 516 520 527 531 532 533 535 536 537 538 540 541 542 543
  213 CALAN 544 545 546 550 551 552 553 554 556 557 558 559 560 561 562
  213 CALAN 563 564 565 566 567 568 569 573 574 578 580 581 582 583 584
  213 CALAN 585 586 587 588 589 600 601 602 603 604 605 606 607 608 609
  213 CALAN 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626
  213 CALAN 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641
  213 CALAN 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656
  213 CALAN 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671
  213 CALAN 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686
  213 CALAN 687 688 689 692 693 695 696 698 699 700 702 703 712 713 714
  213 CALAN 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729
  213 CALAN 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744
  213 CALAN 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759
  213 CALAN 760 761 762 763 764 765 769 770 771 772 773 774 775 776 777
  213 CALAN 778 779 780 781 782 783 785 791 794 801 802 803 804 806 807
  213 CALAN 809 812 813 814 819 820 821 822 823 824 825 826 827 828 829
  213 CALAN 836 837 838 839 840 841 842 846 849 850 851 852 854 855 856
  213 CALAN 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871
  213 CALAN 872 873 874 875 876 877 878 879 881 887 888 889 891 892 893
  213 CALAN 894 895 896 903 904 907 908 912 913 920 921 922 923 924 925
  213 CALAN 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940
  213 CALAN 941 942 944 945 946 948 949 955 960 962 963 964 965 966 967
  213 CALAN 968 969 970 971 972 973 974 975 977 978 979
1 818 CALAN 200 240 241 242 243 244 246 247 280 281 282 284 285 286 287
1 818 CALAN 288 289 300 301 302 303 307 308 309 350 357 358 359 401 402
1 818 CALAN 409 442 443 444 445 446 447 448 450 451 457 458 459 500 502
1 818 CALAN 507 529 545 546 547 548 570 571 572 573 574 575 576 579 580
1 818 CALAN 805 821 956
  415 CAOAK 200 222 223 227 231 232 233 234 235 236 237 241 243 251 252
  415 CAOAK 253 254 255 256 261 262 263 264 265 267 268 269 271 272 273
  415 CAOAK 274 276 278 279 282 283 284 285 287 291 292 295 296 297 298
  415 CAOAK 302 339 346 351 352 357 362 374 376 385 391 392 393 394 395
  415 CAOAK 396 397 398 399 420 421 425 428 430 431 433 434 436 437 441
  415 CAOAK 442 444 445 446 448 451 452 464 465 466 474 477 478 481 482
  415 CAOAK 483 486 495 521 522 523 524 525 526 527 528 529 530 531 532
  415 CAOAK 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547
  415 CAOAK 548 549 550 552 553 554 556 557 558 559 561 562 563 565 567
  415 CAOAK 568 569 576 577 581 582 596 597 620 621 622 624 626 627 631
  415 CAOAK 632 633 635 636 638 639 641 642 643 644 645 647 648 649 652
  415 CAOAK 653 654 655 658 660 667 668 670 673 677 678 695 724 727 729
  415 CAOAK 732 733 736 739 741 743 746 748 749 758 762 763 764 765 768
  415 CAOAK 769 771 772 773 774 775 776 777 781 782 783 784 785 786 788
  415 CAOAK 799 820 821 822 824 826 831 832 834 835 836 837 838 839 840
  415 CAOAK 841 843 845 848 849 860 861 863 864 865 869 874 881 882 884
  415 CAOAK 885 886 887 888 889 891 893 894 895 896 921 922 923 928 929
  415 CAOAK 930 931 932 933 934 935 936 937 938 939 942 943 944 945 946
  415 CAOAK 947 951 953 954 955 956 957 970 971 972 973 974 975 977 978
  415 CAOAK 979 981 982 983 984 985 986 987 989 990 995 996 998 999
  415 CAPAL 226 276 278 321 322 323 324 325 326 327 328 329 335 336 340
  415 CAPAL 341 342 343 344 345 347 348 349 354 358 361 363 364 365 366
  415 CAPAL 367 368 369 371 375 377 378 424 429 438 471 475 481 487 489
  415 CAPAL 490 493 494 496 497 498 537 538 570 571 572 573 574 578 579
  415 CAPAL 581 582 591 592 593 594 595 598 623 637 651 656 657 659 670
  415 CAPAL 683 688 691 694 696 722 723 725 727 732 733 745 770 780 782
  415 CAPAL 783 784 785 786 790 791 792 793 794 795 796 797 851 852 853
  415 CAPAL 854 855 856 857 858 859 881 884 886 887 888 889 926 940 941
  415 CAPAL 948 949 960 961 962 964 965 966 967 968 969
  916 CASAC 278 321 322 323 324 325 326 327 328 329 331 332 334 338 339
  916 CASAC 344 348 349 351 353 355 361 362 363 364 366 368 369 371 372
  916 CASAC 373 381 383 386 387 388 391 392 393 394 395 399 421 422 423
  916 CASAC 424 425 427 428 429 440 441 442 443 444 445 446 447 448 449
  916 CASAC 451 452 453 454 455 456 457 480 481 482 483 484 485 486 487
  916 CASAC 488 489 531 535 537 539 551 552 553 557 567 568 593 631 635
  916 CASAC 636 638 641 643 646 648 649 653 654 657 665 682 683 684 685
  916 CASAC 686 687 688 689 721 722 723 725 726 727 728 729 731 732 733
  916 CASAC 734 736 737 739 745 747 761 762 763 764 765 766 767 768 785
  916 CASAC 852 855 863 920 921 922 923 924 925 927 928 929 933 939 944
```

```
  916 CASAC 951 957 961 962 965 966 967 969 971 972 973 974 978 983 985
  916 CASAC 987 988 989 991 992
1 213 CASAN 430 431 433 434 438 439 493 494 498 592 594 596 597 598 797
1 213 CASAN 799 985 987
  714 CASAN 220 228 229 236 239 241 250 251 253 255 256 258 259 261 262
  714 CASAN 265 282 283 285 289 321 322 323 324 325 326 327 328 329 332
  714 CASAN 367 372 373 374 380 385 414 415 418 432 433 441 447 449 455
  714 CASAN 458 472 474 475 476 490 491 494 497 499 502 503 509 513 515
  714 CASAN 516 517 519 520 521 522 523 524 525 526 527 528 529 530 531
  714 CASAN 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546
  714 CASAN 547 548 549 550 551 552 553 554 556 557 558 559 565 566 567
  714 CASAN 568 569 572 579 581 582 583 586 587 588 589 630 631 632 633
  714 CASAN 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648
  714 CASAN 649 650 651 660 662 663 664 665 666 667 668 669 670 671 673
  714 CASAN 675 680 691 692 693 707 708 712 720 721 722 723 724 725 726
  714 CASAN 727 729 730 731 732 733 738 739 740 741 742 743 744 745 746
  714 CASAN 747 748 750 751 752 754 755 756 757 758 759 760 761 762 764
  714 CASAN 768 770 771 772 773 774 775 776 777 778 779 786 821 826 827
  714 CASAN 828 830 831 832 833 834 835 836 837 838 839 840 841 842 843
  714 CASAN 846 847 848 850 851 852 854 855 856 857 858 859 863 870 871
  714 CASAN 879 890 891 892 893 894 895 896 897 898 921 937 938 939 951
  714 CASAN 952 953 954 955 956 957 960 961 962 963 964 965 966 968 969
  714 CASAN 970 971 972 973 974 975 977 978 979 990 991 992 993 994 995
  714 CASAN 996 997 998 999
  619 CASDI 221 222 223 224 225 226 229 230 231 232 233 234 235 236 237
  619 CASDI 238 239 258 260 262 263 264 265 266 267 268 270 271 272 273
  619 CASDI 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288
  619 CASDI 289 290 291 292 293 294 295 296 297 298 299 336 338 390 401
  619 CASDI 404 406 408 412 413 416 417 419 420 421 422 423 424 425 426
  619 CASDI 427 428 429 435 437 440 441 442 443 444 447 448 449 450 451
  619 CASDI 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466
  619 CASDI 469 470 472 474 475 476 477 479 482 483 484 485 487 488 490
  619 CASDI 491 492 493 494 495 496 497 502 505 506 508 514 518 522 524
  619 CASDI 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539
  619 CASDI 540 541 542 543 544 545 546 547 548 549 551 552 553 554 556
  619 CASDI 557 558 559 560 561 562 563 565 566 569 570 571 573 574 575
  619 CASDI 576 578 579 580 581 582 583 584 585 586 587 588 589 592 594
  619 CASDI 604 660 661 662 668 669 670 672 673 690 691 692 693 694 695
  619 CASDI 696 697 698 699 701 702 717 980 981 987 990 991
  415 CASFA 200 221 227 231 232 233 234 235 236 237 239 241 243 244 251
  415 CASFA 252 255 257 258 259 261 263 264 266 267 268 269 271 272 273
  415 CASFA 274 279 282 285 287 289 291 292 296 298 302 330 331 332 333
  415 CASFA 334 337 338 339 340 341 342 343 344 345 346 347 348 349 355
  415 CASFA 358 359 362 371 374 375 377 378 381 383 385 386 387 388 389
  415 CASFA 391 392 393 394 395 396 397 398 399 420 421 428 431 433 434
  415 CASFA 435 436 437 441 442 444 445 446 448 451 452 453 454 456 457
  415 CASFA 459 461 464 465 466 467 468 469 472 474 476 477 478 479 482
  415 CASFA 485 488 491 492 495 499 502 521 522 523 530 531 532 533 534
  415 CASFA 535 536 539 541 542 543 544 545 546 547 550 552 553 554 556
  415 CASFA 557 558 561 563 564 565 566 567 570 571 572 573 574 576 578
  415 CASFA 579 583 584 585 586 587 588 589 596 597 620 621 622 624 626
  415 CASFA 627 641 645 647 648 652 653 654 655 658 660 661 664 665 666
  415 CASFA 668 673 677 681 692 695 696 697 721 722 731 737 738 739 742
  415 CASFA 748 749 750 751 752 753 755 756 759 761 762 763 764 765 768
  415 CASFA 769 771 772 773 774 775 776 777 781 788 789 821 822 824 826
  415 CASFA 832 834 835 836 839 840 860 861 863 864 865 869 871 872 873
  415 CASFA 874 875 876 877 878 882 885 891 893 894 896 921 922 923 924
  415 CASFA 925 927 928 929 931 936 951 952 953 954 955 956 957 970 971
  415 CASFA 972 973 974 978 979 981 982 983 984 985 986 987 989 990 991
  415 CASFA 992 993 994 995 996 997 998 999
  408 CASJO 221 223 224 225 226 227 234 235 236 237 238 241 243 244 245
  408 CASJO 246 247 248 249 251 252 253 255 256 257 258 259 262 263 264
  408 CASJO 265 266 267 268 269 270 272 274 275 276 277 279 280 281 282
  408 CASJO 283 284 285 286 287 288 289 291 292 293 294 295 296 297 298
  408 CASJO 299 332 345 353 354 356 358 365 370 371 374 376 377 378 379
  408 CASJO 395 398 399 432 433 434 435 436 437 441 446 447 448 452 453
  408 CASJO 463 473 491 492 496 499 522 524 534 552 553 554 559 562 575
  408 CASJO 578 629 720 721 723 725 727 729 730 732 733 734 735 736 737
  408 CASJO 738 739 741 742 743 744 745 746 747 748 749 752 756 765 773
  408 CASJO 864 865 866 867 879 920 922 923 924 925 926 927 929 942 943
```

```
  408 CASJO 945 946 947 954 957 970 971 972 973 974 977 978 980 982 983
  408 CASJO 984 985 986 987 988 989 991 992 993 994 995 996 997 998
1 415 CASJO 226 335 336 438 490 498 623 651 656 657 659 683 691 694 77
1 415 CASJO 940 941 948 949 960 961 962 964 965 966 967 968 969
  303 CODEN 200 220 230 231 232 233 234 235 236 237 238 239 252 255 261
  303 CODEN 266 270 271 273 277 278 279 280 281 286 287 288 289 290 291
  303 CODEN 292 293 294 295 296 297 298 299 320 321 322 329 331 333 337
  303 CODEN 340 341 343 344 348 355 360 361 363 364 366 367 368 369 370
  303 CODEN 371 372 373 375 377 388 393 394 397 398 399 420 421 422 423
  303 CODEN 424 425 426 427 428 429 430 431 433 440 441 442 443 444 447
  303 CODEN 449 450 451 452 455 457 458 460 461 465 466 467 469 470 477
  303 CODEN 478 480 492 494 497 499 526 530 534 538 556 571 572 573 575
  303 CODEN 581 592 595 620 623 624 628 629 631 639 640 642 643 649 650
  303 CODEN 654 657 659 660 665 666 670 671 673 674 676 680 681 688 689
  303 CODEN 690 691 692 693 694 695 696 697 698 699 720 721 722 727 730
  303 CODEN 733 739 740 741 743 744 745 750 751 752 753 755 756 757 758
  303 CODEN 759 760 761 762 763 764 766 770 771 773 777 778 779 780 781
  303 CODEN 782 786 787 788 789 790 791 792 793 794 795 796 797 798 799
  303 CODEN 820 821 825 826 829 830 831 832 836 837 839 840 841 843 844
  303 CODEN 850 851 855 860 861 863 866 868 869 871 877 880 888 889 890
  303 CODEN 891 892 893 894 896 898 899 922 924 930 932 933 934 935 936
  303 CODEN 937 938 939 940 964 965 966 969 971 972 973 977 978 979 980
  303 CODEN 985 986 987 988 989
  203 CTHAR 223 224 225 229 231 232 233 236 240 241 242 243 244 246 247
  203 CTHAR 249 252 257 258 273 275 277 278 279 280 282 285 286 289 291
  203 CTHAR 292 293 296 297 298 299 520 521 522 523 524 525 527 528 529
  203 CTHAR 547 548 549 557 559 560 561 563 565 566 568 569 623 627 633
  203 CTHAR 643 644 645 646 647 648 649 651 653 654 657 658 659 660 665
  203 CTHAR 666 667 668 673 674 675 676 677 678 679 683 688 693 721 722
  203 CTHAR 724 725 726 727 728 826 827 828 829 841 843 870 871 872 875
  203 CTHAR 930 936 951 952 953 954
  202 DCWAS 200 204 206 207 208 209 210 213 214 217 218 220 222 223 224
  202 DCWAS 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239
  202 DCWAS 240 241 242 243 244 245 246 247 248 249 250 251 252 254 255
  202 DCWAS 256 258 259 260 262 263 264 265 266 267 268 269 270 271 272
  202 DCWAS 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287
  202 DCWAS 288 289 291 292 293 294 295 296 297 298 299 306 307 309 310
  202 DCWAS 317 319 320 321 322 323 324 325 326 328 329 330 331 332 333
  202 DCWAS 334 336 337 338 339 340 341 342 343 344 345 346 347 348 350
  202 DCWAS 351 352 353 354 355 356 357 358 359 360 362 363 364 365 366
  202 DCWAS 369 370 371 372 373 374 376 377 378 379 380 382 383 384 385
  202 DCWAS 386 387 388 389 390 391 392 393 394 395 396 397 398 399 401
  202 DCWAS 402 403 404 406 407 408 409 415 416 417 418 420 421 422 423
  202 DCWAS 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438
  202 DCWAS 439 440 441 442 443 444 445 447 448 449 450 451 452 453 454
  202 DCWAS 455 456 457 458 459 460 461 462 463 464 466 467 468 469 470
  202 DCWAS 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485
  202 DCWAS 486 487 488 490 492 493 495 496 497 498 499 501 502 503 504
  202 DCWAS 505 506 507 509 513 514 516 517 519 520 521 522 523 524 525
  202 DCWAS 526 527 528 529 530 532 533 534 535 536 537 538 539 540 541
  202 DCWAS 542 543 544 545 546 547 548 549 550 551 552 553 554 556 557
  202 DCWAS 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572
  202 DCWAS 573 574 575 576 577 578 580 581 582 583 584 585 586 587 588
  202 DCWAS 589 590 591 592 593 595 597 598 599 601 602 603 604 605 606
  202 DCWAS 608 610 613 618 619 620 622 623 624 625 626 627 628 630 631
  202 DCWAS 632 633 634 635 636 637 638 639 640 641 642 643 644 646 647
  202 DCWAS 648 649 650 651 652 653 654 656 657 658 659 660 661 662 663
  202 DCWAS 664 665 666 667 668 669 670 671 673 675 676 678 679 680 681
  202 DCWAS 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696
  202 DCWAS 697 698 699 702 706 707 708 709 712 713 714 715 719 722 723
  202 DCWAS 724 725 726 727 728 731 732 733 734 735 736 737 738 739 742
  202 DCWAS 745 746 749 750 751 752 753 755 756 758 759 760 761 762 763
  202 DCWAS 764 765 767 768 769 770 772 773 774 775 776 778 779 780 781
  202 DCWAS 783 784 785 786 787 789 790 794 795 797 799 801 802 803 805
  202 DCWAS 806 807 808 812 815 816 817 818 820 821 822 823 824 825 826
  202 DCWAS 827 828 829 830 832 833 834 835 836 837 838 839 840 841 842
  202 DCWAS 843 844 845 846 847 848 849 850 851 852 853 856 857 860 861
  202 DCWAS 862 863 864 865 866 868 869 870 871 872 874 875 876 877 879
  202 DCWAS 881 882 883 885 887 888 889 890 891 892 893 894 895 896 897
  202 DCWAS 898 899 901 904 906 907 912 913 914 916 917 920 921 922 924
```

```
  202 DCWAS 925 926 927 928 929 930 931 933 934 935 936 937 938 939 940
  202 DCWAS 941 942 943 944 946 947 948 949 951 952 953 954 955 956 957
  202 DCWAS 960 961 962 963 965 966 967 968 971 972 974 975 977 978 979
  202 DCWAS 980 981 982 983 984 985 986 989 990 991 994 996 998
1 301 DCWAS 206 209 210 217 220 227 229 230 231 236 238 240 248 249 251
1 301 DCWAS 258 262 270 277 279 283 286 292 294 295 297 299 306 309 317
1 301 DCWAS 320 322 330 336 340 341 344 345 350 353 365 369 372 380 384
1 301 DCWAS 386 390 394 402 403 409 417 420 421 422 423 424 427 428 431
1 301 DCWAS 434 436 439 441 443 445 449 454 459 460 464 468 469 470 474
1 301 DCWAS 480 490 492 493 495 496 497 498 499 502 505 507 509 513 520
1 301 DCWAS 530 540 552 559 564 565 567 568 570 571 572 577 580 585 587
1 301 DCWAS 588 589 590 593 595 598 599 601 604 608 618 622 627 630 640
1 301 DCWAS 649 650 652 654 656 657 670 680 681 688 699 702 713 725 731
1 301 DCWAS 735 736 738 753 762 763 770 772 773 774 776 779 794 805 807
1 301 DCWAS 808 816 839 840 843 851 852 853 856 864 868 869 870 871 881
1 301 DCWAS 888 890 891 894 897 899 907 913 916 921 924 925 926 927 929
1 301 DCWAS 930 933 935 937 940 942 946 948 949 951 952 953 961 963 967
1 301 DCWAS 972 975 977 980 981 982 983 984 985 986 989 990
1 703 DCWAS 204 207 214 218 222 235 237 239 241 242 243 246 247 250 255
1 703 DCWAS 256 260 263 264 266 271 273 274 276 278 280 281 284 285 321
1 703 DCWAS 323 325 329 339 351 352 354 355 356 358 359 360 370 378 379
1 703 DCWAS 385 391 406 407 415 418 425 430 435 437 438 440 442 444 448
1 703 DCWAS 450 451 455 461 471 476 478 481 482 486 487 503 506 516 517
1 703 DCWAS 519 521 522 524 525 527 528 532 533 534 536 538 548 549 550
1 703 DCWAS 551 553 556 557 558 560 569 573 578 591 602 603 620 631 641
1 703 DCWAS 642 643 644 648 658 660 661 664 671 683 684 685 689 690 691
1 703 DCWAS 698 706 709 712 715 719 733 734 739 742 746 749 750 751 756
1 703 DCWAS 758 759 760 761 764 765 768 769 780 781 787 790 795 799 802
1 703 DCWAS 803 815 817 818 820 821 823 824 826 827 830 834 836 838 841
1 703 DCWAS 845 846 847 848 849 850 860 866 874 875 876 883 892 893 904
1 703 DCWAS 912 914 920 922 931 934 938 941 960 968 971 974 978 979 998
  305 FLMIA 220 221 222 223 224 226 227 230 232 233 235 238 242 245 246
  305 FLMIA 247 248 250 251 252 253 254 255 257 258 261 262 263 264 266
  305 FLMIA 267 268 270 271 274 279 284 285 324 325 326 327 329 332 342
  305 FLMIA 343 347 348 349 350 352 353 354 358 361 362 363 364 365 366
  305 FLMIA 371 372 373 374 375 376 377 378 379 380 381 382 385 386 387
  305 FLMIA 388 397 399 441 442 443 444 445 446 447 448 449 460 464 470
  305 FLMIA 471 477 478 520 526 529 530 531 532 534 535 536 538 539 541
  305 FLMIA 542 543 544 545 547 548 549 550 551 552 553 554 556 557 558
  305 FLMIA 559 560 567 571 573 575 576 577 578 579 590 591 592 593 594
  305 FLMIA 595 596 598 599 620 621 623 624 625 628 633 634 635 636 637
  305 FLMIA 638 642 643 644 649 651 652 653 654 661 662 663 665 666 667
  305 FLMIA 669 670 672 673 674 681 685 687 688 691 693 694 696 751 754
  305 FLMIA 756 757 758 759 762 769 770 773 775 780 787 789 794 795 821
  305 FLMIA 822 823 825 827 829 835 836 854 855 856 858 859 861 864 865
  305 FLMIA 866 867 868 871 873 874 876 880 881 882 883 884 885 886 887
  305 FLMIA 888 889 891 892 893 895 899 931 932 933 935 937 939 940 944
  305 FLMIA 945 947 948 949 951 952 953 956 957 993 995
  407 FLORL 222 228 236 237 238 239 240 244 246 247 249 256 257 260 262
  407 FLORL 263 273 275 277 281 282 290 291 292 293 294 295 297 298 299
  407 FLORL 327 331 332 339 341 342 345 351 352 354 356 363 365 366 380
  407 FLORL 381 382 420 422 423 424 425 438 469 539 560 568 578 579 623
  407 FLORL 628 629 644 645 646 647 648 649 651 656 657 658 660 661 671
  407 FLORL 672 675 677 678 679 682 695 696 699 740 767 774 788 823 824
  407 FLORL 825 826 827 828 830 831 834 836 839 841 843 849 850 851 855
  407 FLORL 856 857 859 862 869 872 875 876 877 880 884 886 889 894 895
  407 FLORL 896 897 898 899 934 939
  813 FLTAM 221 222 223 224 225 226 227 228 229 231 232 234 236 237 238
  813 FLTAM 239 240 241 242 247 248 251 253 254 258 259 264 265 272 273
  813 FLTAM 276 281 286 287 289 620 621 622 623 626 628 633 634 641 645
  813 FLTAM 653 654 661 662 664 671 677 681 684 685 689 690 830 831 832
  813 FLTAM 835 837 839 840 854 855 870 871 872 873 874 875 876 877 878
  813 FLTAM 879 880 881 882 883 884 885 886 887 888 889 920 931 932 933
  813 FLTAM 935 948 949 960 961 962 963 968 969 971 972 973 974 977 978
  813 FLTAM 979 980 985 986 987 988 989 990 996
  404 GAATL 200 212 215 220 221 222 223 225 230 231 233 237 238 239 240
  404 GAATL 241 242 243 244 246 247 248 249 250 252 255 256 257 260 261
  404 GAATL 262 263 264 266 270 271 279 280 281 284 286 288 289 292 294
  404 GAATL 296 297 299 310 312 313 314 315 316 319 320 321 325 329 330
  404 GAATL 331 332 333 339 341 343 344 346 347 348 349 350 351 352 355
```

```
  404 GAATL 360 361 362 363 364 365 366 368 370 371 372 373 377 378 380
  404 GAATL 381 383 388 389 390 391 392 393 394 395 396 399 413 416 417
  404 GAATL 420 421 422 423 424 425 426 427 428 429 431 432 433 434 435
  404 GAATL 436 438 439 441 442 443 445 446 447 448 449 451 452 454 455
  404 GAATL 457 458 460 461 463 466 469 471 473 474 475 476 477 478 482
  404 GAATL 483 484 487 488 489 491 493 494 496 497 498 499 505 508 512
  404 GAATL 513 515 520 521 522 523 524 525 526 527 528 529 530 533 550
  404 GAATL 551 552 558 559 564 565 566 570 572 573 577 578 580 581 584
  404 GAATL 586 587 588 589 590 591 593 594 603 607 610 618 619 621 622
  404 GAATL 623 624 626 627 631 633 634 636 639 640 641 642 651 653 656
  404 GAATL 658 659 661 662 664 668 669 671 676 679 680 681 683 686 688
  404 GAATL 690 691 696 697 698 699 712 717 723 726 727 728 729 730 732
  404 GAATL 739 740 741 744 750 751 752 753 755 756 758 760 761 762 763
  404 GAATL 765 766 767 768 772 774 785 792 794 799 804 808 810 815 822
  404 GAATL 827 833 835 837 839 840 841 842 843 847 848 850 851 852 853
  404 GAATL 859 870 871 872 873 874 875 876 877 879 880 881 885 888 890
  404 GAATL 892 894 897 898 899 907 916 920 921 922 923 924 925 926 928
  404 GAATL 929 932 933 934 936 938 939 941 942 943 944 945 946 948 949
  404 GAATL 951 952 953 954 955 956 957 960 961 962 963 964 968 969 971
  404 GAATL 972 973 974 975 977 978 979 980 981 982 984 985 986 987 988
  404 GAATL 991 992 993 994 995 996 997 998 999
  312 ILCHI 202 204 207 214 220 221 222 224 225 226 227 229 230 233 235
  312 ILCHI 236 237 238 239 241 242 243 245 247 248 252 254 261 262 263
  312 ILCHI 264 265 266 267 268 269 271 273 274 275 276 277 278 280 281
  312 ILCHI 282 283 284 285 286 287 288 292 294 302 306 308 313 321 322
  312 ILCHI 324 326 327 329 332 334 337 338 341 342 346 347 348 353 363
  312 ILCHI 368 372 373 374 375 376 378 379 380 384 404 407 408 410 413
  312 ILCHI 413 415 417 419 421 427 431 434 435 436 440 443 444 445 454
  312 ILCHI 461 463 465 467 468 471 472 476 477 478 483 486 487 488 489
  312 ILCHI 493 507 508 509 514 521 522 523 525 527 528 533 536 538 539
  312 ILCHI 542 545 548 549 558 559 561 565 567 568 569 580 581 582 583
  312 ILCHI 585 586 588 589 591 592 601 602 604 606 609 621 622 624 625
  312 ILCHI 626 630 631 633 637 638 641 642 643 644 645 646 648 649 650
  312 ILCHI 651 660 661 663 664 666 667 670 684 685 686 693 694 701 702
  312 ILCHI 703 704 707 712 715 716 718 721 722 723 725 726 727 728 731
  312 ILCHI 732 733 734 735 736 737 738 743 744 745 750 751 752 753 760
  312 ILCHI 761 762 763 764 765 767 768 769 770 772 774 775 776 777 778
  312 ILCHI 779 781 782 783 784 785 786 787 791 792 793 794 796 797 802
  312 ILCHI 804 805 807 808 812 814 819 821 822 826 828 829 836 838 842
  312 ILCHI 845 846 847 853 854 855 856 861 871 873 874 875 876 878 880
  312 ILCHI 881 883 886 889 890 899 901 902 903 906 907 908 909 915 917
  312 ILCHI 918 921 922 923 924 925 927 928 929 930 933 935 936 938 939
  312 ILCHI 942 943 944 947 951 955 962 973 975 977 978 984 987 988 989
  312 ILCHI 992 993 994 995 996 997
1 708 ILCHI 200 201 203 205 206 208 209 210 213 215 216 218 223 228 231
1 708 ILCHI 232 234 240 244 246 249 250 251 253 255 256 257 258 259 260
1 708 ILCHI 272 279 289 290 291 293 295 296 297 298 299 301 303 304 307
1 708 ILCHI 310 314 315 316 317 318 319 323 325 328 330 331 333 335 336
1 708 ILCHI 339 343 344 345 349 350 351 352 354 355 357 358 359 360 361
1 708 ILCHI 362 364 366 367 369 371 377 381 382 383 385 386 387 388 389
1 708 ILCHI 390 391 392 393 394 396 397 398 401 402 403 405 406 409 412
1 708 ILCHI 416 418 420 422 423 424 425 426 428 429 430 432 433 437 438
1 708 ILCHI 439 441 442 446 447 448 449 450 451 452 453 455 456 457 458
1 708 ILCHI 459 460 462 469 470 473 474 475 479 480 481 482 484 485 490
1 708 ILCHI 491 492 495 496 498 499 501 502 503 504 505 506 510 512 513
1 708 ILCHI 515 516 517 518 519 520 524 526 529 530 531 532 534 535 537
1 708 ILCHI 540 541 543 544 547 550 551 560 562 563 564 566 570 571 572
1 708 ILCHI 573 574 575 576 577 578 579 584 590 593 594 595 596 597 598
1 708 ILCHI 599 603 605 607 608 612 613 614 615 617 618 619 620 623 627
1 708 ILCHI 628 629 632 634 635 636 639 640 647 652 653 654 655 656 657
1 708 ILCHI 658 659 662 665 668 671 672 673 674 675 676 677 678 679 680
1 708 ILCHI 681 682 687 688 689 690 691 692 695 696 697 698 699 705 706
1 708 ILCHI 709 713 714 717 719 720 724 729 730 739 741 742 746 747 748
1 708 ILCHI 749 754 755 756 757 758 759 766 771 773 780 788 789 790 795
1 708 ILCHI 798 799 801 803 806 810 816 817 818 820 823 824 825 827 830
1 708 ILCHI 831 832 833 834 835 837 839 840 841 843 844 848 849 850 851
1 708 ILCHI 852 857 858 859 860 862 863 864 865 866 867 868 869 870 872
1 708 ILCHI 877 879 882 884 885 887 888 891 892 893 894 895 896 897 898
1 708 ILCHI 904 905 910 913 914 916 919 920 926 931 932 934 937 940 941
1 708 ILCHI 945 946 948 949 952 953 954 956 957 960 961 963 964 965 966
```

```
1 708 ILCHI 967 968 969 971 972 974 979 980 981 982 983 985 986 990 991
1 708 ILCHI 998
1 815 ILCHI 254 372 423 424 436 439 469 474 478 485 722 723 725 726 727
1 815 ILCHI 729 740 741 744 773 774 834 838 886
  317 ININD 200 222 226 228 230 231 232 233 235 236 237 238 239 240 241
  317 ININD 242 243 244 247 248 251 252 253 254 255 256 257 259 261 262
  317 ININD 263 264 265 266 267 269 271 272 273 274 276 277 278 283 290
  317 ININD 291 293 297 298 299 321 322 326 328 335 351 352 353 355 356
  317 ININD 357 359 422 424 425 431 432 439 441 442 443 445 461 462 464
  317 ININD 465 466 467 469 470 471 485 486 488 535 539 541 542 543 545
  317 ININD 546 547 549 556 571 573 574 575 576 577 578 579 580 630 631
  317 ININD 632 633 634 635 636 637 638 639 681 684 685 686 687 691 694
  317 ININD 736 738 745 769 773 776 780 781 782 783 784 786 787 788 823
  317 ININD 831 835 838 839 841 842 843 844 845 846 848 849 852 856 861
  317 ININD 862 867 870 871 872 873 875 876 877 878 879 881 882 885 887
  317 ININD 888 889 891 892 894 895 896 897 898 899 920 921 923 924 925
  317 ININD 926 927 928 929 976 994 996
  504 LANOR 241 242 243 244 245 246 253 254 255 257 260 271 277 278 279
  504 LANOR 282 283 286 288 340 341 347 348 349 361 362 363 364 366 367
  504 LANOR 368 391 392 393 394 398 431 436 441 443 450 451 454 455 456
  504 LANOR 461 462 464 465 466 467 468 469 482 483 484 486 488 521 522
  504 LANOR 523 524 525 527 528 529 552 561 565 566 568 569 581 582 583
  504 LANOR 584 585 586 587 588 589 592 593 595 596 597 656 662 671 676
  504 LANOR 682 684 689 731 733 734 736 737 738 739 762 821 822 824 826
  504 LANOR 827 830 831 832 833 834 835 836 837 838 861 862 865 866 883
  504 LANOR 884 885 887 888 889 891 895 896 897 899 941 942 943 944 945
  504 LANOR 947 948 949 976
  617 MABOS 200 223 224 225 226 227 230 231 232 233 234 235 236 237 239
  617 MABOS 241 242 243 244 245 246 247 248 252 253 254 257 258 261 262
  617 MABOS 263 264 265 266 267 268 269 271 274 275 276 277 278 279 280
  617 MABOS 282 284 285 286 287 288 289 290 292 296 298 320 321 322 323
  617 MABOS 324 325 326 327 328 329 330 331 332 333 335 337 338 340 343
  617 MABOS 345 348 349 350 353 354 357 361 362 364 367 375 377 380 381
  617 MABOS 382 387 389 391 393 394 395 396 397 421 423 424 426 427 428
  617 MABOS 429 431 432 434 436 437 438 439 442 444 445 446 449 450 451
  617 MABOS 455 456 457 461 463 464 466 469 471 472 473 479 482 483 484
  617 MABOS 486 487 488 489 491 492 493 494 495 496 497 498 499 522 523
  617 MABOS 524 527 532 534 536 538 539 541 542 546 547 552 553 556 558
  617 MABOS 560 561 562 565 566 567 568 569 570 571 572 573 574 576 577
  617 MABOS 578 579 581 586 589 592 593 594 595 596 598 599 621 622 623
  617 MABOS 625 628 629 630 633 635 637 638 641 642 643 646 647 648 654
  617 MABOS 661 662 665 666 669 674 680 684 693 694 695 696 698 720 721
  617 MABOS 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736
  617 MABOS 737 738 739 740 742 743 748 749 756 770 773 774 776 781 782
  617 MABOS 783 786 787 789 825 841 842 843 845 846 847 848 849 855 859
  617 MABOS 860 861 862 863 864 868 873 876 884 887 889 890 891 893 894
  617 MABOS 895 899 923 924 925 926 929 930 931 932 933 935 936 937 938
  617 MABOS 942 944 945 951 954 955 956 958 962 964 965 966 969 972 973
  617 MABOS 974 979 981 983 984 985
  313 MIAAR 420 426 428 429 434 437 439 449 451 453 454 455 459 475 481
  313 MIAAR 482 483 484 485 486 487 495 572 662 663 665 668 677 747 761
  313 MIAAR 763 764 769 930 936 971 973 981 994 995 996 998
  313 MIDET 222 223 224 225 226 237 240 245 252 255 256 259 267 270 271
  313 MIDET 272 273 274 275 276 277 278 291 292 295 297 298 320 321 322
  313 MIDET 323 328 330 331 336 337 341 342 343 345 361 365 366 368 369
  313 MIDET 371 372 381 382 383 386 388 389 390 393 396 430 431 436 438
  313 MIDET 440 441 444 446 448 460 491 493 494 496 499 520 521 526 527
  313 MIDET 531 532 533 534 535 536 537 538 554 556 560 561 562 563 564
  313 MIDET 565 567 568 571 577 579 581 582 584 592 593 594 596 599 630
  313 MIDET 690 745 770 780 821 822 823 824 829 831 832 833 834 835 836
  313 MIDET 837 838 839 841 842 843 845 846 849 861 862 863 864 865 866
  313 MIDET 867 868 869 871 872 873 874 875 876 881 882 883 884 885 886
  313 MIDET 891 892 893 894 895 896 897 898 899 921 922 923 924 925 926
  313 MIDET 927 928 929 931 933 934 935 937 940 943 945 956 961 962 963
  313 MIDET 964 965 966 972 974 976 980 983 993
  612 MNMIN 220 221 222 223 224 227 228 229 290 291 292 293 296 297 298
  612 MNMIN 323 330 331 332 333 334 335 336 337 338 339 340 341 342 343
  612 MNMIN 344 347 348 349 368 370 371 372 373 374 375 376 377 378 379
  612 MNMIN 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434
  612 MNMIN 435 436 437 438 439 440 441 443 444 445 446 447 448 449 450
```

```
  612 MNMIN 451 452 454 455 456 457 458 459 460 461 462 463 464 469 470
  612 MNMIN 471 472 473 474 475 476 477 478 479 481 482 483 484 487 488
  612 MNMIN 489 490 491 492 493 494 496 497 498 499 520 521 522 526 527
  612 MNMIN 529 533 534 535 536 537 538 540 541 542 544 545 546 552 553
  612 MNMIN 557 559 560 561 566 569 571 572 574 588 591 593 620 621 622
  612 MNMIN 623 624 625 626 627 631 633 635 636 638 639 640 641 642 643
  612 MNMIN 644 645 646 647 648 649 653 663 667 673 681 683 687 688 690
  612 MNMIN 696 698 699 720 721 722 723 724 725 726 727 728 729 730 731
  612 MNMIN 733 735 736 737 738 739 741 750 753 754 755 757 770 771 772
  612 MNMIN 774 776 777 778 779 780 781 782 784 785 786 788 789 822 823
  612 MNMIN 824 825 827 828 829 830 831 832 835 851 853 854 858 861 863
  612 MNMIN 865 866 867 868 869 870 871 872 874 879 881 884 885 887 888
  612 MNMIN 890 891 892 893 894 895 896 897 920 921 922 924 925 926 927
  612 MNMIN 929 931 932 933 934 935 936 937 938 939 941 942 944 949 976
  612 MNMIN 977 989
  816 MOKCI 221 223 224 225 228 229 231 234 241 242 243 245 246 247 251
  816 MOKCI 252 254 257 274 275 276 283 292 322 331 333 346 348 353 356
  816 MOKCI 358 361 363 373 374 391 395 421 426 435 436 444 452 453 454
  816 MOKCI 455 459 461 464 466 468 471 472 474 478 483 497 521 523 524
  816 MOKCI 525 531 532 537 556 561 572 576 578 587 589 591 654 698 734
  816 MOKCI 737 741 743 751 753 756 757 759 761 763 765 767 781 792 795
  816 MOKCI 796 821 822 833 836 842 844 854 861 871 881 891 921 922 923
  816 MOKCI 924 926 931 932 941 942 943 966 968 995 997
1 913 MOKCI 236 262 268 281 287 299 321 334 339 341 342 345 362 371 375
1 913 MOKCI 381 383 384 422 432 441 451 469 491 492 541 551 573 574 576
1 913 MOKCI 588 596 599 621 631 642 648 649 661 676 677 681 721 722 724
1 913 MOKCI 764 780 782 787 788 791 829 831 888 894 897 962 967
  314 MOSLO 225 227 231 232 233 234 235 241 247 253 259 261 263 268 275
  314 MOSLO 277 289 291 296 298 321 331 342 343 344 349 351 352 353 355
  314 MOSLO 361 362 367 371 381 382 383 385 388 389 391 394 421 423 424
  314 MOSLO 425 426 427 428 429 432 434 436 441 444 454 458 464 466 469
  314 MOSLO 476 481 487 489 521 522 523 524 525 529 531 532 533 534 535
  314 MOSLO 538 539 541 542 544 551 553 554 567 569 571 572 576 577 578
  314 MOSLO 595 621 622 623 631 638 644 645 647 652 653 658 664 671 677
  314 MOSLO 679 694 721 725 726 727 731 739 741 746 747 752 755 758 768
  314 MOSLO 771 772 773 776 777 781 791 795 821 822 823 826 829 831 832
  314 MOSLO 836 837 838 839 841 842 843 845 846 848 849 851 854 855 862
  314 MOSLO 863 865 867 868 869 871 872 878 879 889 891 892 894 895 899
  314 MOSLO 921 928 938 939 941 942 946 947 949 957 961 962 963 965 966
  314 MOSLO 968 969 973 982 984 991 992 993 994 997
1 618 MOSLO 271 274 337 451 452 482 583 797
  919 NCRTP 248 254 266 269 280 286 361 362 365 382 383 387 460 467 469
  919 NCRTP 470 471 477 479 481 489 490 493 528 530 541 543 544 546 549
  919 NCRTP 560 575 596 598 620 660 662 664 677 681 682 683 684 687 688
  919 NCRTP 733 737 740 755 772 779 781 782 783 787 790 821 828 829 831
  919 NCRTP 832 833 834 836 839 840 846 847 848 850 851 856 859 860 870
  919 NCRTP 872 876 878 880 881 890 899 929 932 933 941 942 956 962 966
  919 NCRTP 967 968 976 990 991 992
  908 NJNBR 202 205 214 218 220 225 231 238 246 247 248 249 251 254 257
  908 NJNBR 271 274 283 287 297 302 306 321 324 329 356 360 390 406 407
  908 NJNBR 412 417 418 422 424 442 457 463 469 494 510 519 524 525 526
  908 NJNBR 545 548 549 560 561 562 563 572 602 603 607 613 632 634 636
  908 NJNBR 658 668 679 685 699 704 707 715 721 722 723 725 727 738 745
  908 NJNBR 750 752 753 754 755 756 757 769 805 819 821 826 828 844 846
  908 NJNBR 855 873 878 880 883 885 906 932 937 954 968 980 981 985
  201 NJNEW 200 207 216 217 224 226 227 228 232 233 235 239 241 242 245
  201 NJNEW 256 259 266 268 272 273 276 277 278 279 284 288 289 298 301
  201 NJNEW 304 305 309 312 313 314 315 317 318 319 322 325 330 332 333
  201 NJNEW 338 339 340 342 343 344 345 346 348 351 352 353 354 355 365
  201 NJNEW 368 371 372 373 374 375 376 377 378 379 381 382 386 388 392
  201 NJNEW 393 394 396 399 401 403 408 413 414 416 419 420 421 423 427
  201 NJNEW 428 429 430 432 433 434 435 436 437 438 440 441 450 451 456
  201 NJNEW 460 461 464 465 467 468 470 471 472 473 474 478 480 481 482
  201 NJNEW 483 484 485 486 487 488 489 499 503 504 507 509 514 515 516
  201 NJNEW 522 523 527 533 535 541 546 547 558 564 565 567 568 569 570
  201 NJNEW 574 575 578 581 582 585 587 589 592 593 594 595 596 601 602
  201 NJNEW 608 614 617 621 622 623 624 626 628 633 634 635 636 641 642
  201 NJNEW 643 645 646 648 649 653 654 656 659 661 662 665 667 669 672
  201 NJNEW 673 674 675 676 677 678 680 684 686 687 688 690 692 694 695
  201 NJNEW 696 701 703 705 708 709 712 714 716 731 733 736 737 740 742
```

```
  201 NJNEW 743 744 746 748 750 751 759 760 761 762 763 765 771 772 773
  201 NJNEW 777 778 779 783 785 789 790 791 792 794 795 796 797 798 801
  201 NJNEW 802 803 804 807 808 812 814 815 816 817 820 822 823 824 833
  201 NJNEW 836 837 843 845 851 854 855 857 858 860 861 862 863 864 865
  201 NJNEW 866 867 868 869 871 877 881 882 884 886 887 889 890 893 894
  201 NJNEW 896 902 904 907 909 912 913 915 916 923 925 926 931 933 935
  201 NJNEW 939 941 942 943 944 945 947 952 955 956 960 961 963 964 965
  201 NJNEW 966 969 977 991 992 994 997 998
1 908 NJNEW 200 232 233 241 245 272 273 276 277 289 298 317 322 351 352
1 908 NJNEW 353 354 355 381 382 388 396 419 464 474 486 499 522 527 541
1 908 NJNEW 558 574 582 594 602 634 636 654 665 686 687 688 709 737 750
1 908 NJNEW 760 771 789 815 820 851 855 862 889 913 925 931 964 965 969
  516 NYHEM 220 221 222 223 227 228 229 235 236 237 238 239 248 249 252
  516 NYHEM 255 264 270 285 292 293 294 295 296 299 326 328 333 334 335
  516 NYHEM 336 338 346 349 352 354 355 357 358 364 365 367 371 374 378
  516 NYHEM 379 383 384 391 394 420 431 432 433 437 454 463 466 481 482
  516 NYHEM 483 484 485 486 487 488 489 496 520 521 522 526 531 535 536
  516 NYHEM 538 541 542 546 559 560 561 562 564 565 566 568 569 573 574
  516 NYHEM 575 576 577 579 593 596 598 599 621 623 624 625 626 627 628
  516 NYHEM 629 644 647 656 658 659 663 671 674 676 677 678 679 681 682
  516 NYHEM 683 684 686 691 692 694 731 733 735 739 741 742 745 746 747
  516 NYHEM 752 753 755 756 759 763 764 766 767 773 775 777 781 783 785
  516 NYHEM 789 791 794 795 796 797 798 799 822 823 824 825 826 829 832
  516 NYHEM 833 842 844 845 847 867 868 869 872 873 876 877 883 887 889
  516 NYHEM 890 897 921 922 925 926 931 932 933 934 935 937 938 939 942
  516 NYHEM 943 944 949 997
  212 NYNYO 200 205 206 207 208 210 213 214 216 218 219 220 221 222 223
  212 NYNYO 225 226 227 228 230 231 232 233 234 235 236 237 238 239 240
  212 NYNYO 241 242 243 244 245 246 247 248 249 250 251 252 254 255 260
  212 NYNYO 262 264 265 266 267 268 269 272 276 277 279 280 281 283 285
  212 NYNYO 286 288 289 290 291 292 293 294 295 296 297 298 299 301 302
  212 NYNYO 303 304 305 306 307 308 309 310 312 313 314 315 316 319 320
  212 NYNYO 321 322 323 324 325 326 328 329 330 333 334 335 337 339 340
  212 NYNYO 341 342 344 346 348 349 350 351 352 353 354 355 356 357 358
  212 NYNYO 359 360 361 362 363 364 365 367 368 369 370 371 373 374 378
  212 NYNYO 379 380 382 385 390 391 392 393 395 396 397 398 399 401 402
  212 NYNYO 404 406 407 408 409 410 412 413 414 415 416 418 419 420 421
  212 NYNYO 422 425 427 428 430 431 432 433 436 437 439 440 446 447 448
  212 NYNYO 449 451 452 453 455 456 457 458 459 460 461 463 464 465 466
  212 NYNYO 467 468 469 472 473 474 475 476 477 480 481 482 483 484 485
  212 NYNYO 486 487 488 489 490 491 492 493 495 496 502 503 504 505 506
  212 NYNYO 508 509 510 512 513 514 515 517 518 519 520 521 522 523 524
  212 NYNYO 525 527 528 529 530 531 532 533 534 535 536 537 538 541 542
  212 NYNYO 543 545 546 547 548 549 551 552 553 554 556 557 558 559 560
  212 NYNYO 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575
  212 NYNYO 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590
  212 NYNYO 593 594 595 597 598 599 601 602 603 605 606 607 608 609 610
  212 NYNYO 612 613 614 616 617 618 619 620 621 623 624 625 627 628 629
  212 NYNYO 632 633 635 637 639 640 641 642 643 644 645 648 649 650 652
  212 NYNYO 653 654 655 656 657 658 659 661 662 663 664 665 666 667 668
  212 NYNYO 669 671 673 674 675 676 677 678 679 681 682 683 684 685 686
  212 NYNYO 687 688 689 690 691 692 693 694 695 696 697 698 701 702 703
  212 NYNYO 704 705 707 708 709 711 713 714 715 716 717 719 720 721 722
  212 NYNYO 724 725 727 730 731 732 733 734 735 736 737 740 741 742 744
  212 NYNYO 745 746 747 749 750 751 752 753 754 755 757 758 759 760 761
  212 NYNYO 764 765 766 767 768 769 770 772 775 776 777 779 781 785 786
  212 NYNYO 787 790 791 792 793 794 795 796 797 798 799 804 806 807 808
  212 NYNYO 809 812 813 815 818 819 820 822 823 824 825 826 827 828 829
  212 NYNYO 830 831 832 836 837 838 839 840 841 842 844 847 848 850 852
  212 NYNYO 853 854 855 856 858 860 861 862 863 864 865 866 867 868 869
  212 NYNYO 870 871 872 873 874 876 877 878 879 880 881 882 883 884 885
  212 NYNYO 886 887 888 889 891 892 893 898 899 901 902 903 904 905 906
  212 NYNYO 907 908 909 912 916 918 920 921 922 923 924 925 926 927 928
  212 NYNYO 929 930 931 932 933 935 936 938 940 941 942 943 944 945 947
  212 NYNYO 949 951 952 953 954 955 956 957 960 962 963 964 966 967 968
  212 NYNYO 969 971 972 973 974 975 977 978 979 980 982 983 984 985 986
  212 NYNYO 988 989 991 992 993 994 995 996 997 998 999
1 516 NYNYO 221 222 223 227 228 229 235 236 237 238 239 248 249 252 255
1 516 NYNYO 264 270 285 292 293 294 295 296 299 326 328 333 334 336 338
1 516 NYNYO 346 349 352 354 357 358 364 365 367 371 374 378 379 391 420
```

```
1 516 NYNYO 431 432 433 437 454 463 466 481 482 483 484 485 486 487 488
1 516 NYNYO 489 496 520 521 526 531 535 536 538 541 542 546 559 560 561
1 516 NYNYO 562 564 565 566 568 569 574 575 576 577 579 593 596 598 599
1 516 NYNYO 621 623 624 625 626 627 628 629 644 647 656 658 663 671 674
1 516 NYNYO 676 677 678 679 681 682 683 684 686 691 692 694 731 733 735
1 516 NYNYO 739 741 742 745 746 747 752 753 755 756 759 763 764 766 767
1 516 NYNYO 773 775 781 783 785 789 791 794 795 796 797 798 799 822 823
1 516 NYNYO 824 825 826 829 832 842 844 845 847 867 868 869 872 873 876
1 516 NYNYO 877 883 887 889 890 897 921 922 926 931 932 933 934 935 937
1 516 NYNYO 938 939 942 943 944 949 997
1 718 NYNYO 200 204 209 217 221 224 225 229 230 232 233 234 235 236 237
1 718 NYNYO 238 240 241 244 247 248 251 252 253 256 257 258 259 260 261
1 718 NYNYO 262 263 265 266 267 268 270 271 272 273 274 275 276 277 278
1 718 NYNYO 279 282 284 287 291 296 297 317 318 321 322 326 327 330 331
1 718 NYNYO 332 335 336 337 338 339 341 342 343 345 346 347 349 351 352
1 718 NYNYO 353 354 356 357 358 359 360 361 363 366 370 372 373 375 376
1 718 NYNYO 377 380 381 383 384 385 386 387 388 389 390 392 395 397 398
1 718 NYNYO 403 417 421 423 424 426 428 429 434 435 436 438 439 441 442
1 718 NYNYO 443 444 445 446 447 448 449 451 452 453 454 455 456 457 458
1 718 NYNYO 459 461 462 463 464 465 467 468 469 470 471 474 476 478 479
1 718 NYNYO 480 481 482 485 486 489 492 493 494 495 497 498 499 507 520
1 718 NYNYO 522 523 525 526 527 528 529 531 533 539 541 544 545 552 557
1 718 NYNYO 565 571 574 575 591 592 596 599 604 615 622 624 625 626 627
1 718 NYNYO 628 629 630 631 632 633 634 636 638 639 641 642 643 644 645
1 718 NYNYO 646 647 648 649 651 656 657 658 659 667 670 672 680 692 693
1 718 NYNYO 694 698 699 706 712 720 721 723 726 727 728 729 735 738 739
1 718 NYNYO 740 743 745 746 748 754 755 756 760 761 762 763 764 767 768
1 718 NYNYO 769 771 773 774 776 778 779 780 782 783 784 786 788 789 793
1 718 NYNYO 797 802 803 805 816 821 826 827 830 831 832 833 834 835 836
1 718 NYNYO 837 843 845 846 847 848 849 851 852 853 854 855 856 857 858
1 718 NYNYO 859 868 871 875 876 883 886 891 894 895 896 897 898 899 917
1 718 NYNYO 919 921 922 927 932 934 935 937 938 939 941 942 945 946 948
1 718 NYNYO 949 951 953 955 956 961 962 963 965 966 967 968 969 972 977
1 718 NYNYO 978 979 981 983 984 987 990 995 996 997 998 999
1 914 NYNYO 235 237 251 253 270 282 285 286 287 288 289 321 328 332 333
1 914 NYNYO 335 337 345 347 375 376 378 381 390 391 395 397 422 423 428
1 914 NYNYO 472 476 478 523 524 576 591 592 631 632 633 636 641 642 644
1 914 NYNYO 654 662 664 665 667 668 674 681 682 683 684 686 693 694 696
1 914 NYNYO 697 698 699 721 723 725 738 761 768 771 776 779 784 789 792
1 914 NYNYO 793 833 834 835 899 921 925 933 934 935 937 939 946 948 949
1 914 NYNYO 961 963 964 965 967 968 969 993 997
  216 OHCLE 221 226 228 229 231 232 234 235 236 237 238 241 243 247 248
  216 OHCLE 249 251 252 261 265 266 267 268 271 278 281 283 289 291 292
  216 OHCLE 295 299 321 328 331 333 338 341 344 348 349 351 356 361 362
  216 OHCLE 363 368 371 381 382 383 389 391 397 398 421 423 425 429 431
  216 OHCLE 432 433 439 441 442 443 444 445 446 447 449 451 459 461 463
  216 OHCLE 464 467 468 469 471 473 475 476 479 481 486 487 491 521 522
  216 OHCLE 523 524 526 529 531 541 543 561 562 566 572 574 575 578 579
  216 OHCLE 581 582 585 586 587 589 591 621 622 623 631 634 641 642 646
  216 OHCLE 651 656 659 661 662 663 664 671 676 681 687 689 691 692 694
  216 OHCLE 696 721 728 729 731 732 734 736 737 741 749 751 752 754 761
  216 OHCLE 765 766 771 777 779 781 789 791 795 822 826 831 835 838 842
  216 OHCLE 843 844 845 851 861 871 881 883 884 885 886 888 891 892 899
  216 OHCLE 921 931 932 941 942 943 944 946 951 953 961 975 987 991 995
  614 OHCOL 221 222 223 224 225 227 228 229 231 235 236 237 238 239 243
  614 OHCOL 248 249 251 252 253 258 261 262 263 265 267 268 271 272 274
  614 OHCOL 275 276 278 279 281 288 291 292 293 294 296 297 299 325 329
  614 OHCOL 337 338 341 351 361 365 371 395 421 424 431 433 436 438 442
  614 OHCOL 443 444 445 447 451 457 459 460 461 462 463 464 466 469 471
  614 OHCOL 475 476 478 479 481 486 487 488 491 492 497 523 538 548 575
  614 OHCOL 621 644 645 752 755 756 759 761 764 766 771 777 785 786 791
  614 OHCOL 792 793 794 821 833 836 837 841 842 846 847 848 851 852 855
  614 OHCOL 860 861 863 864 866 868 870 871 875 876 877 878 879 881 882
  614 OHCOL 885 888 889 890 891 895 898 899 927 964 965
  503 ORPOR 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234
  503 ORPOR 235 236 237 238 239 240 241 242 243 244 245 246 248 249 250
  503 ORPOR 251 252 253 254 255 256 257 273 274 275 279 280 281 282 283
  503 ORPOR 284 285 286 287 288 289 291 292 293 294 295 297 299 323 324
  503 ORPOR 326 335 357 359 452 464 526 591 620 621 624 625 626 627 628
  503 ORPOR 629 630 631 632 635 636 637 638 639 640 641 642 643 644 645
```

```
  503 ORPOR 646 647 648 649 650 652 653 654 655 656 657 658 659 661 663
  503 ORPOR 665 666 667 668 669 677 681 682 684 685 690 691 692 693 694
  503 ORPOR 695 696 697 698 721 731 733 760 761 771 774 775 777 778 781
  503 ORPOR 789 790 796 936 976 985
  215 PAPHI 221 222 223 224 225 226 227 228 229 231 232 233 235 236 237
  215 PAPHI 238 241 242 243 244 245 246 247 248 254 259 260 263 265 270
  215 PAPHI 271 272 275 276 277 278 279 280 281 283 284 288 289 291 293
  215 PAPHI 299 324 328 329 330 331 332 333 334 335 336 337 338 339 341
  215 PAPHI 342 349 350 351 352 353 354 356 359 365 379 382 386 387 389
  215 PAPHI 422 423 424 425 426 427 438 440 446 447 448 449 450 452 455
  215 PAPHI 456 457 460 461 462 463 464 465 466 467 468 470 471 472 473
  215 PAPHI 474 476 477 480 482 483 485 487 490 492 494 496 497 499 520
  215 PAPHI 521 522 523 525 526 527 528 531 532 533 534 535 537 539 540
  215 PAPHI 542 543 544 545 546 548 549 551 552 553 557 560 561 563 564
  215 PAPHI 565 566 567 568 569 570 572 573 574 576 577 578 580 581 583
  215 PAPHI 585 586 587 590 591 592 595 596 597 620 621 622 623 624 625
  215 PAPHI 626 627 628 629 630 631 632 634 635 636 637 638 639 641 642
  215 PAPHI 643 645 646 649 653 657 659 660 662 663 664 665 667 668 671
  215 PAPHI 673 676 677 680 684 685 686 687 688 690 697 698 722 724 725
  215 PAPHI 726 727 728 729 732 734 735 737 739 742 743 744 745 747 748
  215 PAPHI 751 753 755 761 763 765 768 769 782 784 786 787 789 790 823
  215 PAPHI 824 825 828 829 830 831 833 834 835 836 839 840 841 842 843
  215 PAPHI 844 846 848 849 851 853 854 864 870 871 872 874 875 876 877
  215 PAPHI 878 879 880 881 884 885 886 887 891 892 893 894 895 896 897
  215 PAPHI 898 899 920 922 923 924 925 927 928 930 931 934 936 937 938
  215 PAPHI 940 941 947 951 952 955 960 961 962 963 964 969 971 972 973
  215 PAPHI 975 977 978 980 981 985 986 988 990 991 998
  412 PAPIT 200 221 227 231 232 234 236 237 241 242 243 244 247 255 256
  412 PAPIT 257 261 262 263 264 268 269 271 273 276 279 281 288 298 321
  412 PAPIT 322 323 328 331 333 338 341 343 344 351 355 359 361 362 363
  412 PAPIT 364 365 366 367 369 371 372 373 374 381 389 391 392 393 394
  412 PAPIT 421 422 427 429 431 433 434 441 442 456 461 462 464 466 469
  412 PAPIT 471 472 476 481 486 487 488 491 492 497 521 531 551 553 561
  412 PAPIT 562 563 565 566 571 572 578 594 621 622 623 624 633 636 642
  412 PAPIT 644 645 647 648 653 655 661 664 665 672 673 674 675 678 681
  412 PAPIT 682 683 687 692 699 731 734 741 747 749 751 754 761 762 765
  412 PAPIT 766 767 771 777 778 781 782 784 787 788 793 795 798 821 822
  412 PAPIT 823 824 825 826 828 829 831 833 835 840 854 855 856 858 859
  412 PAPIT 881 882 884 885 889 892 921 922 923 928 931 936 937 939 961
  412 PAPIT 963 967
1 601 TNMEM 342 349 393 781 851
  901 TNMEM 227 272 274 276 278 320 323 324 325 327 332 344 345 346 348
  901 TNMEM 353 357 358 360 362 363 365 366 367 368 369 371 372 373 375
  901 TNMEM 377 382 385 386 387 388 395 396 397 398 452 454 458 465 475
  901 TNMEM 476 483 484 485 486 521 522 523 524 525 526 527 528 529 531
  901 TNMEM 532 533 535 543 544 572 575 576 577 578 579 597 654 678 681
  901 TNMEM 682 683 684 685 721 722 725 726 728 729 743 744 745 747 748
  901 TNMEM 752 753 754 755 756 757 758 761 762 763 765 766 767 774 775
  901 TNMEM 785 789 794 795 797 829 853 854 867 872 873 876 877 922 942
  901 TNMEM 946 947 948 976
  512 TXAUS 218 219 243 244 247 250 251 255 258 259 261 263 264 266 267
  512 TXAUS 272 276 280 282 288 292 320 322 323 326 327 328 329 331 335
  512 TXAUS 338 339 343 345 346 356 369 370 371 385 386 388 389 390 397
  512 TXAUS 403 416 422 440 441 442 443 444 445 447 448 450 451 452 453
  512 TXAUS 454 458 459 461 462 463 465 467 469 471 472 473 474 475 476
  512 TXAUS 477 478 479 480 482 483 495 499 750 794 823 832 834 835 836
  512 TXAUS 837 838 860 867 870 873 891 892 926 928 929 940 941 973 984
  512 TXAUS 990
  214 TXDAL 202 203 204 205 212 216 217 218 219 220 221 222 223 224 225
  214 TXDAL 226 227 228 229 230 231 233 234 235 238 239 240 241 242 243
  214 TXDAL 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258
  214 TXDAL 259 260 262 263 264 266 269 270 271 272 275 276 278 279 281
  214 TXDAL 284 285 286 287 288 289 290 291 293 296 298 299 301 302 303
  214 TXDAL 305 306 307 308 309 313 314 315 316 317 318 319 320 321 323
  214 TXDAL 324 327 328 330 331 332 333 336 337 339 340 341 343 348 349
  214 TXDAL 350 351 352 353 357 358 360 361 363 368 369 371 372 373 374
  214 TXDAL 375 376 380 381 384 385 386 387 388 391 392 393 394 397 398
  214 TXDAL 399 401 402 403 404 406 407 412 413 414 416 417 418 420 421
  214 TXDAL 422 423 424 426 428 434 436 437 438 441 442 443 444 445 446
  214 TXDAL 450 453 456 458 462 464 466 470 471 475 480 484 487 490 492
```

```
  214 TXDAL 494 495 497 502 503 504 506 508 513 514 516 517 518 519 520
  214 TXDAL 521 522 526 528 530 533 539 541 550 553 554 556 557 558 559
  214 TXDAL 565 570 573 574 575 578 579 580 590 591 594 596 601 602 603
  214 TXDAL 604 605 606 607 608 609 612 613 615 616 618 620 621 630 631
  214 TXDAL 634 637 638 641 642 644 647 650 651 653 655 658 659 660 661
  214 TXDAL 669 670 676 680 681 686 688 689 690 691 692 696 698 699 701
  214 TXDAL 702 704 705 706 707 708 709 712 713 714 715 716 717 718 720
  214 TXDAL 721 724 727 733 739 740 741 742 744 745 746 747 748 749 750
  214 TXDAL 751 754 760 761 767 770 771 780 781 783 787 788 790 791 799
  214 TXDAL 804 808 812 815 818 819 820 821 823 824 826 827 828 830 840
  214 TXDAL 841 844 850 851 855 864 867 869 871 879 880 881 888 890 891
  214 TXDAL 902 904 905 907 909 913 917 918 919 920 922 929 931 933 934
  214 TXDAL 939 941 942 943 944 946 948 949 951 952 953 954 956 957 960
  214 TXDAL 964 969 977 978 979 980 985 986 987 988 991 992 993 995 996
  214 TXDAL 997 999
1 817 TXDAL 261 265 267 268 273 329 355 356 366 379 421 424 425 429 430
1 817 TXDAL 432 449 450 461 467 469 475 477 481 498 530 540 543 572 577
1 817 TXDAL 588 589 640 654 667 671 679 695 784 792 832 856 884 890 922
1 817 TXDAL 925 929 930 961 962 963 967
  713 TXHOU 200 220 221 222 223 224 225 226 227 228 229 230 233 235 236
  713 TXHOU 237 238 240 241 242 244 246 247 252 253 254 261 263 264 265
  713 TXHOU 266 267 268 269 270 271 272 274 277 278 280 282 283 284 285
  713 TXHOU 286 287 289 293 295 320 324 326 328 331 332 333 334 335 336
  713 TXHOU 337 338 339 341 342 343 346 347 350 351 353 354 355 356 358
  713 TXHOU 359 360 363 364 367 370 371 373 374 376 377 378 383 388 390
  713 TXHOU 391 392 393 394 395 420 421 422 424 425 426 427 428 431 432
  713 TXHOU 433 434 436 437 438 439 440 441 442 443 444 445 446 447 448
  713 TXHOU 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463
  713 TXHOU 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478
  713 TXHOU 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493
  713 TXHOU 494 495 496 497 498 499 520 521 522 523 524 525 526 527 528
  713 TXHOU 529 530 531 535 536 537 540 541 542 546 547 548 549 550 551
  713 TXHOU 552 556 558 561 563 565 568 571 575 577 578 579 580 583 584
  713 TXHOU 586 587 588 589 590 591 596 599 620 621 622 623 626 627 629
  713 TXHOU 630 631 633 635 636 639 640 641 643 644 645 649 650 651 652
  713 TXHOU 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667
  713 TXHOU 668 669 670 671 672 673 674 675 676 678 679 680 681 682 683
  713 TXHOU 684 685 686 688 690 691 692 694 695 696 697 699 720 721 723
  713 TXHOU 726 728 729 731 732 733 734 738 739 741 744 746 747 748 749
  713 TXHOU 750 751 752 753 754 757 758 759 761 762 763 764 765 768 769
  713 TXHOU 771 772 774 775 776 777 778 779 780 781 782 783 784 785 786
  713 TXHOU 787 788 789 790 791 792 793 794 795 796 797 798 799 820 821
  713 TXHOU 822 823 824 825 826 827 828 829 831 833 834 835 836 840 841
  713 TXHOU 842 844 845 846 847 850 852 853 854 855 856 857 858 859 861
  713 TXHOU 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876
  713 TXHOU 877 878 879 880 882 883 884 886 888 890 891 892 893 894 895
  713 TXHOU 896 897 898 899 920 921 922 923 924 926 928 929 930 931 932
  713 TXHOU 933 935 937 938 939 940 941 943 944 946 947 948 951 952 953
  713 TXHOU 954 955 956 957 960 961 963 964 965 966 967 968 969 971 972
  713 TXHOU 973 974 975 977 978 980 981 983 984 985 986 987 988 989 991
  713 TXHOU 992 993 995 996 997 998 999
  801 UTSLC 220 237 240 250 251 252 254 255 261 262 263 264 265 266 268
  801 UTSLC 269 272 273 277 278 287 292 295 298 299 321 322 328 350 355
  801 UTSLC 359 363 364 366 451 460 461 466 467 468 480 481 482 483 484
  801 UTSLC 485 486 487 488 521 522 524 526 530 531 532 533 534 535 536
  801 UTSLC 537 538 539 543 544 546 547 549 561 562 565 566 569 570 571
  801 UTSLC 572 573 575 576 578 579 580 581 582 583 584 585 588 594 595
  801 UTSLC 596 633 799 933 942 943 944 947 964 965 966 967 968 969 972
  801 UTSLC 973 974 975 977
  206 WASEA 223 224 226 227 228 232 233 234 235 236 237 241 242 243 244
  206 WASEA 246 248 251 255 271 277 281 282 283 284 285 286 287 292 296
  206 WASEA 298 320 322 323 324 325 326 328 329 340 343 344 345 346 358
  206 WASEA 361 362 363 364 365 367 368 382 386 389 391 392 393 394 395
  206 WASEA 421 431 432 433 439 441 442 443 447 448 451 453 454 455 461
  206 WASEA 462 464 467 477 481 483 485 486 487 488 489 522 523 524 525
  206 WASEA 526 527 528 542 543 544 545 546 547 548 554 557 562 575 583
  206 WASEA 585 587 621 622 623 624 625 626 628 630 631 632 633 634 635
  206 WASEA 637 639 641 643 644 646 649 654 655 656 657 661 662 667 670
  206 WASEA 672 682 684 685 720 721 722 723 725 726 727 728 742 743 744
  206 WASEA 745 746 747 762 763 764 767 768 771 772 773 774 775 776 778
```

```
  206 WASEA 781 782 783 784 787 788 789 820 821 822 823 824 827 828 836
  206 WASEA 838 839 842 850 852 854 859 861 865 867 868 869 870 872 874
  206 WASEA 878 880 881 882 883 885 889 930 932 933 935 936 937 938 940
  206 WASEA 941 946 947 948 949 953 954 955 965 969 972 977 979 982 986
  206 WASEA 989 991 993 994 995 996 997 998 999
  414 WIMIL 221 222 223 224 225 226 227 228 229 237 241 242 243 246 251
  414 WIMIL 252 253 254 255 256 257 258 259 263 264 265 266 271 272 273
  414 WIMIL 274 276 277 278 281 282 283 287 288 289 291 297 298 299 321
  414 WIMIL 322 323 327 332 341 342 343 344 345 347 351 352 353 354 355
  414 WIMIL 357 358 359 362 365 367 372 374 375 377 382 383 384 385 421
  414 WIMIL 422 423 425 427 438 442 444 445 447 449 453 454 461 462 463
  414 WIMIL 464 466 471 475 476 481 482 483 486 491 521 523 524 527 529
  414 WIMIL 535 536 538 541 542 543 544 545 546 547 548 549 562 575 579
  414 WIMIL 581 643 645 647 649 662 663 671 672 678 679 691 744 747 761
  414 WIMIL 762 764 765 768 769 771 774 778 781 782 783 784 785 786 789
  414 WIMIL 791 792 796 797 798 799 821 835 844 871 873 874 881 896 931
  414 WIMIL 933 935 936 937 941 955 961 962 963 964 966
```

Conclusion

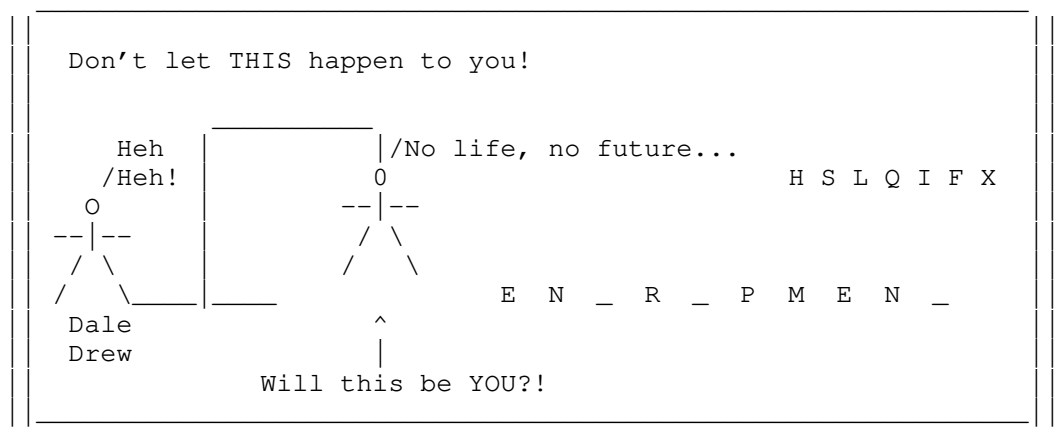
I could hardly take credit for scanning and finding the NUAs that make make up this list. I put this list together because the lists I've seen in the past were either partially incomplete or partially incorrect. A list put out by OpusWiz and Dawn Treader several years ago served as the base data for this list. I've spoken to many many hackers over the years to add to and correct the list. Erik Bloodaxe's Telenet Directory, published in the Legion of Doom Technical Journals, was of great help in clarifying and adding to the data.

The list is still neither complete or fully accurate. For example, I still don't know the outdials for San Diego, California (619). The 415 and 714 outdials might be mixed up. If you have any additions or corrections, please e/mail one of my Internet accounts.

By the way, the new 510 area code will have an impact on the PC Pursuit dialout list. SprintNet hasn't incorporated the new area code into its lists yet, so I haven't either. But they will soon, so be aware that the Oakland, California dialout will change from area code 415 to 510 someday.

== Phrack Inc. ==

Volume Three, Issue Thirty-five, File 5 of 13



The following is a reprint of the article "Sting Operations" from the book _Dedicated Computer Crime Units_ (pages 101-103) written by J. Thomas McEwen for the U.S. Department of Justice and published in June 1989.

If you would like to get your own FREE copy of this book, or its companion books:

- Organizing for Computer Crime Investigation and Prosecution
- Electronic Fund Transfer and Crime
- Electronic Fund Transfer Fraud

you can contact:

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice
Washington, D.C. 20531
(301)251-5500
(800)851-3420

- -

S T I N G O P E R A T I O N S

Will *YOU* Be The Next Victim?!

Transcribed by Sovereign Immunity

ELECTRONIC BULLETIN BOARDS

An electronic bulletin board allows for the storage of information which can be retrieved by other systems calling into the board. It is essentially a database maintained by a system that is accessible by others over telephone lines. Most bulletin boards have been created for specific purposes, usually for the exchange of messages and information among parties with common interests. For example, members of computer clubs maintain bulletin boards for communicating with each other between meetings.

Bulletin boards are especially popular among microcomputer users. Establishment of a bulletin board is facilitated by programs that can be purchased or obtained from public domain software. With one of these programs, a user can establish tailored menus for anyone dialing into the board. These menus will usually contain options on information about the board, bulletins, news summaries, personal mail, conferences, and leaving messages.

In addition, most bulletin boards have different levels of access to restrict users from certain parts of the board. The bulletin board owner, usually called the System Operator (SYSOP), personally establishes the authorized access levels for each user and enters this information into the system.

Access is determined by having a user provide their name and password when signing on to the system. A telephone line into the system is the only other requirement for establishing a board on a microcomputer.

Access to bulletin boards generally operates along the following lines:

- A user dials into the bulletin board.
- The board responds with a message asking for the person's name and password.
- The board then provides a menu showing the options available to the user.
- The user selects an option and starts interacting with the system.
- During a session, a user typically may read messages, leave messages, download files, upload files, or join a conference.
- The user eventually "quits" the session and hangs up from the board.

While most bulletin boards have been established for legitimate purposes, there are also "pirate" or "elite" boards that contain illegal information or have been established to advance an illegal activity. Security on those boards is tightly controlled by the owners. With these bulletin boards, users usually have to contact the owner directly to obtain a password for access to different levels of the system. A degree of trust must therefore be established before the owner will allow access to the board, and the owners develop "power" over who can use the system.

Pirate boards have been found with a variety of illegal information on them including the following:

- Stolen credit card account numbers
- Long distance telephone service codes
- Telephone numbers to mainframe computers, including passwords and account numbers
- Procedures for making illegal drugs
- Procedures for making car bombs
- Hacking programs
- Tips on how to break into computer systems
- Schematics for electronic boxes (e.g., black box)

These boards obviously are a threat to communities, and their existence has gained the attention of some police departments.

STING OPERATIONS WITH BULLETIN BOARDS

The experiences of the Maricopa County, Arizona, Sheriff's Department and the Fremont, California, Police Department are very instructive on how local departments can establish their own bulletin boards and become part of the network with other boards. Members of the Maricopa County Sheriff's Department were the first in the country to establish such a board. Their board resulted in over 50 arrests with the usual charge being telecommunications fraud.

In September, 1985, the Fremont Police Department established a bulletin board for the primary purpose of gathering intelligence on hackers and phreakers in the area. The operation was partially funded by VISA, Inc. with additional support from Wells Fargo Bank, Western Union, Sprint, MCI, and ITT.

After establishing their bulletin board, they advertised it on other boards as the newest "phreak board" in the area. Within the first four days, over 300 calls were received on the board. During the next three months, the board logged over 2,500 calls from 130 regular users. Through the bulletin board, they persuaded these groups that they had stolen or hacked long-distance telephone service codes and credit account numbers. They were readily accepted and were allowed access to pirate boards in the area.

The board was operated for a total of three months. During that period, over 300 stolen credit card numbers and long-distance telephone service codes were recovered. Passwords to many government, educational, and corporate computers were also discovered on other boards.

The operation resulted in the apprehension of eight teenagers in the area who were charged with trafficking in stolen credit card accounts, trafficking in stolen long-distance telephone service codes, and possession of stolen

property. Within the next week, seven more teenagers in California and other states were arrested on information from this operation.

It was established that this group had been illegally accessing between ten and fifteen businesses and institutions in California. They were regularly bypassing the security of these systems with stolen phone numbers and access codes. One victim company estimated that it intended to spend $10,000 to improve its security and data integrity procedures. Other victimized businesses were proceeding along the same lines.

CONCLUSIONS

There are several reasons for conducting Sting operations of this type. One of the most important is that it provides a proactive method of identifying hackers and phreakers in the area. These groups are particularly hard to find since they operate in closed circles with personal networks developed from friendships.

Another byproduct of these operations is the publicity surrounding the cases. Sting operations result in considerable amount of attention from the media. The publicity has the effect of closing down other pirate boards in the area. One of the greatest fears of these offenders in that their systems will be taken, and in the Fremont operation over $12,000 of computer equipment was seized. The publicity associated with these seizures seems to be the primary reason for others to stop their pirate boards.

These operations also lead to other types of offenses. In Fremont, for example, drug and alcohol cases were developed as a result of the Sting operation. This has been typical of these operations.

The Sting operations with bulletin boards have been criticized because teenagers, rather than hardened criminals, are arrested. Many hackers believe that they have a right to the data in other systems and that their activities are not illegal since the companies can afford the losses. On the other hand, as one investigator observed, the hackers of today may be the sophisticated computer criminals of tomorrow. It is therefore important to set a lesson early in their careers steering them away from these offenses.

\- -

RESPONSE FROM A MEMBER OF THE HACKER COMMUNITY:

Now lets take a look at this article and the ignorant author J. Thomas McEwen.

> "Pirate boards have been found with a variety of illegal information on them..."

The author names:

"Telephone numbers to mainframe computers" -- There is nothing illegal in having the telephone number to a mainframe computer. It is illegal to access a computer without authorization.

"Procedures for making illegal drugs" -- It is NOT illegal to know how to manufacture illegal drugs, only to actually manufacture or use them.

"Procedures for making car bombs" -- It is NOT illegal to know how to manufacture car bombs, only to actually manufacture or use them.

"Hacking programs" -- Indeed most security companies, private security consultants, or mainframe owners and operators use these to test their systems very often. It would only be illegal to use one on a machine that you are not authorized to use it on.

"Tips on how to break into computer systems" -- Again, it is NOT illegal to know how to break into a computer... although for a change, according to a section of the Computer Fraud & Abuse Act of 1986 (Federal Law), it would be illegal to traffic in passwords, codes, and theoretically any instructions that

would be the equivalent of passwords or codes for the unauthorized entry into computer systems.

"Schematics for electronic boxes (e.g., black box)" -- This is getting boring. It is NOT illegal to know how to build these devices, only the actual construction or use of them is illegal.

> "These boards obviously are a threat to communities, and their existence has gained the attention of some police departments."

How are they obviously a threat?

The author would like us to believe that if the information on how to make telephone devices, explosives, or narcotics is available on bulletin boards, this is enough to make them a threat to communities.

What he ignores is that the same information can be found in public and university libraries, text books, and technical journals;

He ignores that the mere possession of information on how a crime MIGHT be committed is NOT a crime; and finally,

He fails to recognize any First Amendment rights whatsoever of computer bulletin boards to have all such information to begin with.

> "It is therefore important to set a lesson early in the careers steering them away from these offenses."

Of course an arrest for some minor computer mischief is not going to be great resume material when these teenagers start applying for jobs, even though the establishment has inspired within them the socially acceptable goal of conforming to society's expectations.

CONCLUSIONS

The author, J. Thomas McEwen, does not know much about freedom of speech and for that matter, he does not know much about the law. He does know a lot about how to sensationalize very benign conduct into dangerous conspiracy. Perhaps he is close friends with Geraldo Rivera.

Bulletin board operators and users take note of the law and your rights. Don't let yourself get taken in by Sting boards or ignorant law enforcement officers looking for some gratification on the job since they aren't getting it at home.

S o v e r e i g n I m m u n i t y

- -

Editor's Comments by: Dispater

Sting boards have been a popular topic in Phrack and Phrack World News over the years. In this file, Sovereign Immunity, showed us an excerpt that discussed a Sting bulletin board in Fremont, California. As it turns out, Knight Lightning had some material about this way back in Phrack World News Issue 3 (which actually appeared in Phrack Issue 4). The article was titled "Phoenix Phortress Stings 7." There have also been many other articles in Phrack World News about sting operations and bulletin boards.

Additionally, Phrack Issues 21-23 each carried one part of Knight Lightning's "Vicious Circle" Trilogy. The first two parts of which ("Shadows Of A Future Past" and "The Judas Contract") contained a lot of material about sting boards and informants.

Although Phrack has not presented material concerning Sting boards in Maricopa County, Arizona, there was discussion about a bulletin board (The Dark Side) in Arizona (602) run by "The Dictator" (Dale Drew) as a sting operation revealed

in Computer Underground Digest 3.02 and recently we heard that he was back in action under the name "Blind Faith."

Dispater

_____?_

== Phrack Inc. ==

Volume Three, Issue Thirty-five, File 6 of 13

***** Social Security Numbers & Privacy *****

by Chris Hibbert

June 1, 1991

Computer Professionals for Social Responsibility

Many people are concerned about the number of organizations asking for their Social Security Numbers. They worry about invasions of privacy and the oppressive feeling of being treated as just a number.

Unfortunately, I can't offer any hope about the dehumanizing effects of identifying you with your numbers. I *can* try to help you keep your Social Security Number from being used as a tool in the invasion of your privacy.

Surprisingly, government agencies are reasonably easy to deal with; private organizations are much more troublesome. Federal law restricts the agencies at all levels of government that can demand your number and a fairly complete disclosure is required even if its use is voluntary. There are no comparable laws restricting the uses non-government organizations can make of it, or compelling them to tell you anything about their plans. With private institutions, your main recourse is refusing to do business with anyone whose terms you don't like.

*** Short History ***

Social Security numbers were introduced by the Social Security Act of 1935. They were originally intended to be used only by the social security program, and public assurances were given at the time that use would be strictly limited. In 1943 Roosevelt signed Executive Order 9397 which required federal agencies to use the number when creating new record-keeping systems. In 1961 the IRS began to use it as a taxpayer ID number. The Privacy Act of 1974 required authorization for government agencies to use SSNs in their data bases and required disclosures (detailed below) when government agencies request the number. Agencies which were already using SSN as an identifier were allowed to continue using it. The Tax Reform Act of 1976 gave authority to state or local tax, welfare, driver's license, or motor vehicle registration authorities to use the number in order to establish identities. The Privacy Protection Study Commission of 1977 recommended that the Executive Order be repealed after some agencies referred to it as their authorization to use SSNs. I don't know whether it was repealed, but that practice has stopped.

The Privacy Act of 1974 (5 USC 552a) requires that any federal, state, or local government agency that requests your Social Security Number has to tell you three things:

1. Whether disclosure of your Social Security Number is required or optional;

2. What law authorizes them to ask for your Social Security Number; and,

3. How your Social Security Number will be used if you give it to them.

In addition, the Act says that only Federal law can make use of the Social Security Number mandatory. So anytime you're dealing with a government institution and you're asked for your Social Security Number, just look for the Privacy Act Statement. If there isn't one, complain and don't give your number. If the statement is present, read it. If it says giving your Social Security Number is voluntary, you'll have to decide for yourself whether to fill in the number.

```
*****************************
***                       ***
*** Private Organizations ***
***                       ***
*****************************
```

The guidelines for dealing with non-governmental institutions are much more tenuous. Most of the time private organizations that request your Social Security Number can get by quite well without your number, and if you can find the right person to negotiate with, they'll willingly admit it. The problem is finding that right person. The person behind the counter is often told no more than "get the customers to fill out the form completely."

Most of the time, you can convince them to use some other number. Usually the simplest way to refuse to give your Social Security Number is simply to leave the appropriate space blank. One of the times when this isn't a strong enough statement of your desire to conceal your number is when dealing with institutions which have direct contact with your employer. Most employers have no policy against revealing your Social Security Number; they apparently believe the omission must have been an unintentional slip.

```
*****************************
***                       ***
*** Lenders and Borrowers ***
***                       ***
*****************************
```

Banks and credit card issuers are required by the IRS to report the SSNs of account holders to whom they pay interest or when they charge interest and report it to the IRS. If you don't tell them your number you will probably either be refused an account or be charged a penalty such as withholding of taxes on your interest.

```
***********************************
***                             ***
*** Insurers, Hospitals, Doctors ***
***                             ***
***********************************
```

No laws require medical service providers to use your Social Security Number as an ID number (except for Medicare, Medicaid, etc). They often use it because it's convenient or because your employer uses it to certify employees to its groups health plan. In the latter case, you have to get your employer to change their policies. Often, the people who work in personnel assume that the employer or insurance company requires use of the SSN when that's not really the case. When my current employer asked for my SSN for an insurance form, I asked them to try to find out if they had to use it. After a week they reported that the insurance company had gone along with my request and told me what number to use. Blood banks also ask for the number but are willing to do without if pressed on the issue. After I asked politely and persistently, the blood bank I go to agreed that they didn't have any use for the number, and is in the process of teaching their receptionists not to request the number.

```
*********************************************************
***                                                   ***
*** Why Is The Use of Social Security Numbers A Problem? ***
***                                                   ***
*********************************************************
```

The Social Security Number doesn't work well as an identifier for several reasons. The first reason is that it isn't at all secure; if someone makes up a nine-digit number, it's quite likely that they've picked a number that is assigned to someone. There are quite a few reasons why people would make up a number: to hide their identity or the fact that they're doing something; because they're not allowed to have a number of their own (illegal immigrants, e.g.), or to protect their privacy. In addition, it's easy to write the number down wrong, which can lead to the same problems as intentionally giving a false number. There are several numbers that have been used by thousands of people because they were on sample cards shipped in wallets by their manufacturers (one is included below).

When more than one person uses the same number, it clouds up the records. If someone intended to hide their activities, it's likely that it'll look bad on whichever record it shows up on. When it happens accidently, it can be unexpected, embarrassing, or worse. How do you prove that you weren't the one using your number when the record was made?

A second problem with the use of SSNs as identifiers is that it makes it hard to control access to personal information. Even assuming you want someone to be able to find out some things about you, there's no reason to believe that you want to make all records concerning yourself available. When multiple record systems are all keyed by the same identifier, and all are intended to be easily accessible to some users, it becomes difficult to allow someone access to some of the information about a person while restricting them to specific topics.

```
*********************************************
***                                       ***
*** What Can You Do To Protect Your Number? ***
***                                       ***
*********************************************
```

If despite your having written "refused" in the box for Social Security Number, it still shows up on the forms someone sends back to you (or worse, on the ID card they issue), your recourse is to write letters or make phone calls. Start politely, explaining your position and expecting them to understand and cooperate. If that doesn't work, there are several more things to try:

1. Talk to people higher up in the organization. This often works simply because the organization has a standard way of dealing with requests not to use the SSN, and the first person you deal with just hasn't been around long enough to know what it is.

2. Enlist the aid of your employer. You have to decide whether talking to someone in personnel, and possibly trying to change corporate policy is going to get back to your supervisor and affect your job.

3. Threaten to complain to a consumer affairs bureau. Most newspapers can get a quick response. Some cities, counties, and states also have programs that might be able to help.

4. Tell them you'll take your business elsewhere (and follow through if they don't cooperate).

5. If it's a case where you've gotten service already, but someone insists that you have to provide your number in order to have a continuing relationship, you can choose to ignore the request in hopes that they'll forget or find another solution before you get tired of the interruption.

If someone absolutely insists on getting your Social Security Number, you may want to give a fake number. There is no legal penalty as long as you're not doing it to get something from a government agency or to commit fraud. There are a few good choices for "anonymous" numbers. Making one up at random is a bad idea, as it may coincide with someone's real number and cause them some amount of grief. It's better to use a number like 078-05-1120, which was printed on "sample" cards inserted in thousands of new wallets sold in the 40s and 50s. It's been used so widely that both the IRS and SSA recognize it immediately as bogus, while most clerks haven't heard of it. It's also safe to invent a number that has only zeros in one of the fields. The Social Security Administration never issues numbers with this pattern. They also recommend that people showing Social Security cards in advertisements use numbers in the range 987-65-4320 through 987-65-4329.

The Social Security Administration recommends that you request a copy of your file from them every few years to make sure that your records are correct.

```
***************
***         ***
*** THE END ***
```

```
                              ***          ***
                              ***************
```

==Phrack Inc.==

Volume Three, Issue Thirty-five, File 7 of 13

```
<:=--=:><:=--=:><:=--=:><:=--=:>\|/<:=--=:><:=--=:><:=--=:><:=--=:>
<:=--=:>                                                     <:=--=:>
<:=--=:>    >>>>>=-*  Users Guide to VAX/VMS  *-=<<<<<     <:=--=:>
<:=--=:>                                                     <:=--=:>
<:=--=:>                   Part I of III                     <:=--=:>
<:=--=:>                                                     <:=--=:>
<:=--=:>            Part A:  Basic Information               <:=--=:>
<:=--=:>         Part B:  Programming the VAX/VMS            <:=--=:>
<:=--=:>                                                     <:=--=:>
<:=--=:>                   By: Black Kat                     <:=--=:>
<:=--=:>                                                     <:=--=:>
<:=--=:><:=--=:><:=--=:><:=--=:>/|\<:=--=:><:=--=:><:=--=:><:=--=:>
```

Index
~~~~

Part A contains information on the following topics:

- Background
- Terminal Control Keys
- Logging in
- Digital Command Language (DCL)
- Error Messages
- Command Line Editing
- Files and Directories
- File Operations
- Logical Names
- System Default Logical Names
- Logical Name Tables
- User Environment
- Terminal Characteristics
- File Security
- EDT Text Editor
- EDT Help manual

Part B contains information on the following topics:

- Programming VAX/VMS
- DCL Expressions
- Command Procedures
- Writing Command Procedures
- Comments
- Labels
- Debugging
- Invoking Command Procedures
- Symbols
- Lexical Functions
- Parameters
- Terminal I/O
- File I/O
- Redirecting Command Procedure I/O
- Branching and Conditionals
- Loops
- Subroutines
- Error Handling
- Termination
- Example Command Procedures

<:=- Part A : Basic Information -=:>

Introduction
~~~~~~~~~~~~

VAX is an acronym for Virtual Address eXtension, a 32-bit computer developed by Digital in the 1970's. The VAX architecture supports multiprogramming, where many users running different programs can use the VAX simultaneously and each appears to have full control of the computer's resources. The multiprocessing VAX functions vary differently from the old timesharing systems, which would allocate a slice of CPU time to each user of the system in a rotating fashion, whether the time slice was required or not. The VAX/VMS environment, however, provides each user an allocation of processor time based on the user's needs and priority. If a user does not need his quantum of time, or a portion of it, it is given to the next user. This scheduling method is very efficient when compared to the old method of timesharing.

The VAX is capable of addressing more than four billion addresses, through a method known as virtual memory addressing. Because the memory is virtual however, there is no need to have four billion bytes of physical memory. The VAX executes programs by a technique known as paging, whereby a single "page" of the program is read into memory at a time, and when a new page is needed, the old one is "swapped" back out to disk to make room for the new one. The VMS operating system ties everything together. The user interacts with VMS (Virtual Memory System) through a Command Language Interpreter (CLI), usually the Digital Command Language (DCL).

When you use VAX/VMS, you are known to the system as a process, which is created when you log in to the system and deleted when you log out. This process carries with it various attributes to identify you from other system users (process name, identification, user identification code, privileges, etc).

Terminal Control Keys

Ctrl-A	Allows you to insert, rather than overstrike, characters on a DCL command line that you're editing.
Ctrl-B	Displays DCL commands that you've previously entered.
Ctrl-C	Interrupts the coessed or the program being executed.
Ctrl-E	Positions the cursor at the end of the line.
Ctrl-H	Positions the cursor at the beginning of the line.
Ctrl-I	Tab
Ctrl-O	Alternately suppresses and continues the display of the output terminal.
Ctrl-Q	Enables (toggles on) output to the display after CTRL-S.
Ctrl-R	Retypes the current input line and repositions the cursor atthe end of the retyped line.
Ctrl-S	Disables (toggles off) output to the display until CTRL-Q is pressed.
Ctrl-T	Displays process statistics.
Ctrl-U	Discards the current input line and performs carriage return.
Ctrl-W	Refreshes the screen.
Ctrl-X	Flushes the type-ahead buffer.
Ctrl-Y	Interrupts command or program execution and returns control to the DCL command line interpreter.
Ctrl-Z	Indicates end of file for data entered from terminal.

Logging in

Most VAX systems prompt you with something like this:

```
Welcome to VAX1
Username:
```

Type your username and press <enter>. You'll then be prompted for your password. If you enter the correct username/password combination, you'll be given something like the following:

```
        Welcome to VAX/VMS V4.4
Last interactive login on Monday, 16-JUL-87  16:12
Last non-interactive login on Friday, 13-JUL-87  00:14
$
```

If you entered an incorrect username and password, you'll receive the message:

```
User authorization failure
```

Just hit <enter> and you'll be prompted for your username again. Once you're logged in, you'll be given the DCL prompt ($). This indicates that the system is ready to accept interactive commands.

To log out, use the command:

```
$ LOGOUT
```

The Digital Command Language (DCL)

DCL is comprised of more than 200 commands called verbs. Each DCL verb acts on a parameter or assumed parameter, and the action of these verbs and the scope of their parameters can be modified with qualifiers. The basic command structure is:

```
$ LABEL: COMMAND-NAME PARAMETER(S) /QUALIFIER(S) !COMMENT
    |          |          |              |           |
    |          |          |              |           +-- Optional Comment
    |          |          |              |
    |          |          |              +-------------- Command modifier(s)
    |          |          |
    |          |          +---------------------------- Object of the
Command
    |          |
    |          +------------------------------------- DCL command verb
    |
    +------------------------------------------------ Optional Label
```

A label is an optional, user-specified string with a maximum length of 255 characters. It is most commonly used in command procedures.

A DCL command verb defines the action the VAX will take when the command line is interpreted.

Parameter(s) specify the object or a list of objects the DCL command verb will act upon. Multiple parameters may be specified but must be separated from one another by a space, multiple spaces, or a tab. If you enter a DCL command that requires parameters, but you don't enter them on the command line, the DCL interpreter will prompt you for them automatically.

Qualifiers further define or modify the function the DCL command will perform. They consist of a keyword followed by a value or a list of values.

The qualifier keyword must be preceded by a slash (/). Multiple qualifiers may be specified, but each must be preceded with a slash. Qualifiers usually aren't required. There are three kinds of qualifiers: parameter, positional, and command. A command qualifier applies to the whole command. Generally, these are placed at the end of the command. For example:

```
$ DIRECTORY [BYNON],[BYNON.DECPRO]/FULL
```

This displays a full listing of two directories, using the /FULL qualifier of the DIRECTORY command. A positional qualifier takes on a different meaning based on where it is located in the command. If a positional qualifier is placed after the command verb, but before the first parameter, the qualifier will affect the entire command. If the same positional qualifier is placed after a parameter, only that parameter will be affected. For example:

```
$ PRINT/COPIES=3 MEMO1.TXT,MEMO2.TXT
$ PRINT MEMO1.TXT/COPIES=2,MEMO2.TXT
```

The first command prints three copies of each file. The second command prints two copies of the first file, but only one copy of the second. A parameter qualifier affects only the parameter it follows. In the following example, MEMO1.TXT is sent to the queue LASER and MEMO2.TXT is sent to queue FAST_PRINT:

```
$ PRINT MEMO1.TXT/QUEUE=LASER,MEMO2.TXT/QUEUE=FAST_PRINT
```

A comment is an optional, user-specified comment about the command. It is commonly used in command procedures to document the command.

Error Messages

Generally, error messages are of the format:

```
% FACILIT-L-IDENT, TEXT
|   |     |   |      |
|   |     |   |      +-- explanation of the error message
|   |     |   |
|   |     |   +--------- abbreviated message text, for reference
|   |     |
|   |     +------------- error severity
|   |
```

```
   |   +------------------- Vax/VMS facility or component (error source)
   |
   +----------------------- message number: "%" = first, "-" = subsequent
```

A percent sign (%) indicates the first error message for a given command.
All subsequent errors for that command are preceded with a hyphen (-).

The facility indicates the source of the error. The source may be the DCL command line interpreter, one of the various VMS utilities, or a program image.

The severity level indicator (L) will have one of the following values: S (successful completion), I (information), W (warning), E (error), or F (fatal or severe error).

The ident is an abbreviation of the error message text. It can be referenced in the VAX/VMS System Messages manual.

The text provides an explanation of the error message.

Command line editing

DCL stores the last 20 command lines entered. You can display a list of them with:

```
$ RECALL /ALL
```

The resulting display might look like:

```
1  DIR
2  COPY VAX1::$1$DUA5:[BYNON]LOGIN.COM LOGIN.COM;1
3  EDIT LOGIN.COM
$
```

To recall a specific command from the recall buffer, use the DCL RECALL command with a command line number as a parameter. For example:

```
$ RECALL 2
$ COPY VAX1::$1$6DUA5:[BYNON]LOGIN.COM LOGIN.COM;1
```

Files and Directories

Files are organized much like MS-DOS, with a directory-tree structure. The user's default directory (assigned by the system administrator) is the "root" directory. Up to seven subdirectories may be created, each containing as many subdirectories as you like. The complete file specification looks like:

```
VAX1 :: DUA0 : [BYNON.PROGRAMMING.FORTRAN]WINDOWS.FOR;3
  |       |          |                      |     | |
  |       |          |                      |     | |
node   device      directory            filename  | version
                                                type
```

The node name identifies a computer system in a network. If no node name is specified, VMS assumes the file is located on the local node where you're logged in.

The device name is the physical device where the file is stored. It is a four-character alphanumeric code which identifies the device type, hardware controller to which it is attached, and the unit number of the device on the controller. If you omit the device name from a file specification, VMS assumes you are referring to your default device.

The directory entry is enclosed in brackets, and is the name of the directory that contains the file. If you omit the directory name from a file specification, VMS will assume you are referring to your default directory.

The filename may consist of up to 39 alphanumeric characters.

The file type is a code consisting of up to 39 alphanumeric characters, and it generally indicates the type of information supplied in the file. Some system programs and utilities supply a three character default file type.

The version number is a 1 to 5 digit number the system assigns to every file by default. When a file is created, it is assigned a version number of 1. Each time the file is edited or another version of it is created, the version number is automatically incremented by 1. Alternatively, you may specify a version number of your choice.

No blank spaces are allowed within any portion of a file specification. In VMS Version 4.x, the maximum lengths are as follows:

node name	up to 6 characters
device name	four characters
directory name	up to 39 characters
subdirectory name	up to 39 characters
file name	up to 39 characters
file type	up to 39 characters
version number	up to 5 decimal digits with a value between 1 and 32,767

File specifications must be unique; no two files can have completely identical specifications. It's conceivable to have many copies of NOTES.TXT in a subdirectory, but only one NOTES.TXT;8 may exist in the same subdirectory.

Wildcards are similar to those in MS-DOS, with an asterisk (*) representing a filename or filetype, and a percent sign (%) indicating a single character.

File operations

Creating and modifying files:
```
$ CREATE TEMP.DAT
TEMP 1
TEMP 2
<CTRL-Z>
```

Renaming files:
```
$ RENAME TEMP.DAT NEW.DAT
$ RENAME TEMP.DAT [BYNON.PROG]TEMP.DAT
Note: you cannot rename files across devices, just
directories.
```

Copying files:
```
$ COPY TEMP.DAT NEW.DAT
$ COPY TEMP.DAT,TEST.DAT NEW.DAT
```

Appending files:
```
$ APPEND TEMP.DAT NEW.DAT
```

Deleting files:
```
$ DELETE TEMP.DAT;1
$ DELETE *.DAT;*
$ DELETE /CONFIRM .DAT;*  (confirm each file)
```

Displaying files:
```
$ TYPE /PAGE TEMP.DATE    (one page at a time)
```

Directories:
```
$ DIRECTORY
$ DIRECTORY DJA1:[BYNON.PROG]
```

Printing files:
```
$ PRINT TEMP.DAT
```

Purging files:
```
$ PURGE *.DAT   (erase all but latest version of .DAT files)
```

Create a dir:
```
$ CREATE/DIRECTORY [.BUDGET]
```

Set default dir:
```
$ SET DEFAULT [BYNON.PROG]
$ SET DEFAULT [.PROG]
```

Delete a dir:
```
$ SET DEFAULT [BYNON.PROG]
$ DELETE *.*;*
$ SET DEFAULT [BYNON]
```

```
$ SET PROTECTION=(0:D) PROG.DIR;1
$ DELETE BUDGET.DIR;1
```

Logical Names

A logical name is a substitute for a file specification, portion of a file specification, or another logical name. They provide two primary functions: file and device independence and file specification shorthand.

File and device independence means that you are not constrained by a physical element, such as a disk or printer name. If you use files nested deeply in subdirectories, with long names, or on devices or nodes other than your default, you can define a meaningful logical name to represent it. These shorthand names are faster to type and easier to remember.

To define a logical name:

```
$ DEFINE PARTS_DBF DJA2:[DATABASES]PARTS.DAT
```

This example will associate the logical name PARTS_DBF with the file specification DJA2 : [DATABASES]PARTS.DAT. Now, PARTS_DBF may be used anywhere as a substitute for the complete file specification.

Other commands also can be used to assign logical names.

Assign : Associates equivalence names with a logical name
Mount : Mounts a disk or tape volume and assigns a system logical for the volume.
Allocate: Allocates a system device for private use and optionally (command qualifier) assigns a logical name to the device.
Open : Opens a file for read or write operations and assigns a logical name to the file specification.

To display the logical name translations: $ SHOW LOGICAL PARTS_DBF will display: "PARTS_DBF" = "DJA2:[DATABASES]PARTS.DAT" (LNM$PROCESS_TABLE).

To deassign a logical name: $ DEASSIGN PARTS_DBF

System default logical names

SYS$COMMAND The initial file, or input stream, from which the DCL command line interpreter reads input data. The logical name SYS$COMMAND is equated to your terminal for interactive processes.
SYS$DISK Your default disk as assigned in the UAF.
SYS$ERROR The device on which the system displays all error and informational messages. By default, SYS$ERROR is assigned to your terminal for interactive processes, and to the batch job log file for any batch processes.
SYS$INPUT The default file or input stream from which data and commands are read by either the DCL command line interpreter or programs executing in your account. By default, SYS$INPUT is equated to your terminal for interactive processes and to the batch job stream (or command procedure) for batch processes.

Logical Name Tables

Logical names are stored in system files called logical name tables. The following are the four most commonly used:

Group table : Contains the logical names available to all users in your UIC (User Identification Code) group.
Job table : Contains the logical names available to your process and any subprocess it creates.
Process table: Contains the logical names available to your process only.
System table : Contains the logical names that may be used by all users of the system.

User Environment

The User Authorization File (UAF) is a system file controlled and modified by the system manager. A record for each system user is contained in the UAF.

A User Identification Code (UIC) is an identifier used by VAX/VMS to identify users and groups of users. It is used to identify processes, directories, files, and other objects in the system. A UIC may be specified numerically or alphanumerically, and is made up of two parts, a group and a member, specified in the format: [group,member]. For example, UIC [10,14] identifies group 10, user 14. The group number is an octal number in the range 1-37776, and the member is an octal number in the range 0-177776. An alphanumeric UIC contains a member name and optionally, a group name in the format: [member] or [group,member]. The group and member names in an alphanumeric UIC may contain 1 to 31 alphanumeric characters (A-Z, 0-9, underscore, dollar sign).

Each user of the system is limited in the consumption of system resources, and these limits control the rate at which your process or any subprocesses you create may consume a resource. There are 32 levels of priority in the VAX/VMS system, 0 through 31, the highest being 31. The priorities are divided into two ranges: timesharing (0-15) and real-time (16-31). The default user priority is 4. Depending on how heavily the system is being used, your priority may be raised above the default, but never lowered below it. VAX/VMS maintains 35 privileges, divided into the following seven categories classified by how much damage could be done to the system by possessing them:

None	No privileges.
Normal	The minimum privilege needed to use the system effectively.
Group	The ability to effect members of the same UIC group.
Devour	The potential to consume noncritical system-wide resources.
System	The ability to interfere with normal system operation.
File	The potential to bypass file protection security.
All	The ability to take over the entire system.

VAX/VMS systems keep a record of overall computer system use by account holder in a system file called ACCOUNTING.DAT. The system manager uses this file to produce reports with the Accounting Utility. This can be used to learn more about how the system is being used, how it performs, and how a particular user is using the system. It can also be used to bill users for system time.

Terminal Characteristics

Setting display width: $ SET TERMINAL/WIDTH=132

Shutting messages off: $ SET TERMINAL/NOBROADCAST
This prevents other users from phoning you, sending mail messages, and some system messages from appearing on your screen. If you just want mail and phone messages screened, use: $ SET BROADCAST=(NOMAIL,NOPHONE).

Increasing type-ahead buffer: $ SET TERMINAL/ALTYPEHD/PERMANENT

Line editing modes: $ SET TERMINAL/INSERT or $ SET TERMINAL/OVERSTRIKE

Defining keys:
```
$ DEFINE/KEY PF1 "SET DEFAULT DUA3:[INV.SUP]"
% DCL-I-DEFKEY, DEFAULT key PF1 has been defined
```

Showing keys:
```
$ SHOW KEY PF1      (or $ SHOW KEY ALL)
DEFAULT keypad definitions:
   PF1 = "SET DEFAULT DUA3:[INV.SUP]"
```

Deleting keys:
```
$ DELETE/KEY PF1    (or $ DELETE/KEY ALL)
% DCL-I-DELKEY, DEFAULT key PF1 has been deleted
```

Changing prompt: $ SET PROMPT = "What now?"

Displaying process information: $ SHOW PROCESS (add a qualifier)

Changing process information: $ SET PROCESS/NAME="Bob"
$ SET PROCESS/PRIVILEGES=OPER

File Security
~~~~~~~~~~~~

UIC-based protection permits access to be granted or denied based on protection codes that reflect four user categories:

System: system manager
Owner : account owner
Group : users in same UIC group
World : all users of system, regardless of UIC

Four type of file access can be granted or denied to members of these user categories:

Read (R): read the file
Write (W): create or modify the file
Execute (E): run a program
Delete (D): delete the file

Generally, any category of user can be granted or denied file access with this protection scheme. However, you can read a file in a subdirectory with EXECUTE access if you know its filename and filetype. Also, since SYSTEM privileges include the ability to bypass all file protection, anyone within the SYSTEM category can read a file.

CONTROL access, or the ability to change the protection and ownership of a volume, is never specified in the UIC-based protection code. This is the fifth type of protection that can be specified in an access control list (ACL). It's automatically granted to two user categories when VMS examines UIC-based protection. Users in the SYSTEM and OWNER categories receive CONTROL access by default while GROUP and WORLD categories are denied CONTROL access.

File protection defaults are as follows:

System: RWED
Owner : RWED
Group : RE
World : No access

To determine the existing or default protection of a file, use the SHOW PROTECTION command. The default in the previous example would be:

```
$ SHOW PROTECTION
    SYSTEM=RWED, OWNER=RWED, GROUP=RE, WORLD=NO ACCESS
```

If you want to see file protection in directories, use the /PROTECTION qualifier with the DIRECTORY command.

To change the protection of a file, use the command:

```
$ SET PROTECTION=(O:RWE,G,W) LOGIN.COM
```

In this example, the account owner has READ, WRITE, and EXECUTE access to his LOGIN.COM file. The GROUP and WORLD categories have no access and SYSTEM access remains unchanged.

Rules for specifying protection codes:
1. Access types must be abbreviated with one letter: R, W, E, or D.
2. User categories may be spelled out or abbreviated.
3. Each user category must be separated from its access types with a colon.
4. If you specify multiple user categories, separate each with a comma and enclose the entire code in parenthesis.
5. User categories and access types may be specified in any order.
~~~~~~~~~~~~

6. If you include a user category, but do not specify an access type for that category, access is automatically denied.
7. If you omit a user category entirely, protection for that category is unchanged.

Remember that VAX/VMS evaluates directory protection before file protection. If you grant WORLD:R access to a file, but the file is in a directory without WORLD:R access, another user couldn't read the file.

EDT Text Editor

When you enter EDT, you automatically enter line mode, indicated by the EDT prompt, an asterisk (*). All line mode commands are made at the asterisk prompt and terminated by pressing <Return>. Lines that you input are numbered sequentially by the editor. You can reference a line or group of li^S^Qnes based on the line number or range of line numbers. A list of basic EDT commands follows. Each command may be abbreviated to the characters in parenthesis. Complete information on all EDT line mode commands can be found through the use of the line mode EDT HELP command.

Commands	Function
Change (C)	Change from line to keypad mode. To switch back from keypad mode to line mode, press <Ctrl-Z>.
Copy (CO)	Copy a line or group of lines from one place to another. If you enter the command CO 5 to 10, line 5 will be copied to the line immediately preceding line 10. The command CO 5:10 to 20 would copy the contents of lines 5 through 10 into the area immediately preceding line 20.
Delete (D)	Delete a line or group of lines. The command D13 would delete line 13, while D13:20 will delete lines 13 to 20.
Exit (EX)	Terminates the EDT session, saving all changes. This also creates a new version of the file being edited.
Help (H)	Display on-line help on all EDT line mode commands. The help messages will not be included in the file being edited.
Include (INC)	Copy text from an external file into the file being edited. When the EDT command INCLUDE FILENAME.TYPE is executed, the contents of FILENAME.TYPE are copied into the file being edited.
Insert (I)	Inserts specified text directly before the current position in the file. While inserting text, you will not receive the EDT "*" prompt. Press <Ctrl-Z> to return to the "*" prompt when you're finished inserting.
Move (M)	You can't cut and paste with a line-oriented editor. Text will be moved to the area immediately preceding a specified line. The command M 10:15 to 50 would move lines 10 through 15 to the area immediately preceding line 50.
Quit (QUI)	Exit the EDT editor without saving changes.
Replace (R)	Deletes a specified line or group of lines and enters the INSERT mode so you can add text in that place. The command R5:10 would delete lines 5 through 10 and switch to the INSERT mode to permit you to enter new text. To exit the INSERT mode, press <Ctrl-Z>.
Resequence (RES)	Numbers all of the lines in the file that you're editing in increments of 1. This is useful because text insertion, movement, or deletion causes the file to lose numeric sequence.
Substitute (S)	Substitute a new text element for an old one in the format s/oldtext/newtext/range. The old and new text elements must be enclosed in angle bracket (< >) delimiters and the range must be specified.
Write (WR)	Write a given range of text to a new file. WRHISTORY.TXT 50:100 would write lines 50 through 100 to a new file called HISTORY.TXT.

EDT Help Manual
~~~~~~~~~~~~~~

To dump the entire EDT Help file to disk, enter the following DCL command during a terminal session: $ ASSIGN EDTHELP.FIL SYS$OUTPUT. Now, enter line mode EDT and type: * HELP *. Now exit EDT and enter the DCL command: $ ASSIGN TTnn: SYS$OUTPUTT (TTnn: is your terminal number).

<:=- Part B : Programming VAX/VMS -=:>

Introduction
~~~~~~~~~~~~

A symbol is a name chosen to represent a string of characters, a numeric value, or a logical (true/false) value. A symbol may be used wherever the value it represents would normally be found, and can be up to 255 characters long. Symbols must begin with a character, dollar sign, or underscore, and are not case-sensitive. Symbols are created like this:

```
symbol_name = value    (local symbol)
symbol_name == value   (global symbol)
```

A global symbol may be used at any command level, but local symbols are lost when command procedures are finished. For example:

```
$ WIDE = "SET TERMINAL/WIDTH=132"
```

Now, anytime you type WIDE at the DCL command line, the terminal width will be changed to 132 characters. To show the contents of a symbol:

```
$ SHOW SYMBOL ANSWER
   ANSWER = 1584    HEX = 00000630    OCTAL = 000000003060
```

The SHOW SYMBOL command uses the local symbol table by default. To show the value of a global symbol, use the /GLOBAL qualifier. To show all symbols, use the /ALL qualifier (or /GLOBAL/ALL). To delete symbols, use: $ DELETE/SYMBOL symbol_name command (with /GLOBAL if it's global).

When a DCL command is executed, symbols in the following positions are automatically translated:

- the beginning of the command
- in a lexical function
- in a WRITE or IF statement
- on the right side of an = or == assignment statement
- inside brackets on the left side of an assignment statement when you're preforming string substitution

If none of these cases fits, apostrophes will force the translation:

```
$ DIRECTORY 'PARTS'  (after $ PARTS = "DJA2:[DBA]PARTS.DAT")
```

Symbols are commonly used for shorthand. For example, to clear the screen:

```
$ ESC[0,8] == 27
$ CLEAR == "[J"
$ HOME  == "[H"
$ CLR == WRITE SYS$OUTPUT ESC,HOME,ESC,CLEAR
```

Now, anytime you enter CLR, the screen will be cleared. Symbols can also be used to execute command procedures:

```
$ NETBACK == "@SYS$LOGIN:NETBACKUP"
```

Finally, foreign commands unknown to DCL can be executed by using symbols:

```
$ KERMIT == RUN SYS$$SYSTEM:KERMIT
```

DCL Expressions
~~~~~~~~~~~~~~~

Expressions are built by combining data elements with operators. A logical
~~~~~~~~~~~~~~~

comparison evaluates the relationship between two components as true or false (True = 1, False = 0).

Lexical functions are VAX/VMS routines that return process or system information, or manipulate user-supplied data. Lexical functions are unique because the result is returned in the function name, allowing it to be used as a symbol (much like Pascal). Lexical functions are called with the following format:

```
F$function_name(parameter, parameter...)
```

For example, the following lexical function manipulates user-supplied data:

```
$ STRING = "Go     home    right      now!"
$ STRING = F$EDIT(STRING, "COMPRESS, UPCASE")
$ SHOW SYMBOL STRING
   STRING = "GO HOME RIGHT NOW!"
```

Command Procedures

A command procedure is a file consisting of a sequence of DCL commands which can be executed interactively or as a batch job (like a .BAT file in MS-DOS or a REXX EXEC in VM/SP). Command procedures are used in VAX/VMS to perform repetitive or complex tasks and to save time. With a command procedure, you can execute many DCL commands with a single statement.

Command procedures aren't bound by simple lists of DCL commands executed in sequence. They can take advantage of labels, lexical functions, symbols and relational operators to build sophisticated procedures which act like VAX/VMS programs. Command procedures are flexible. They can be written to take specific actions based on responses to questions, or even to perform a given function depending on the time or date.

Writing Command Procedures

A text editor such as EDT or EVE is used to create and edit command procedures, which should be named "PROCEDURE_NAME.COM". The file type ".COM" is the default procedure file type, and if a different file type is included, it must be included when the procedure is invoked.

Each new command line must begin with a dollar sign ($). Multiple spaces or tabs may be included after the "$" for readability, and command lines may be extended past a single line by ending the previous line with a hyphen (-) and not starting the next line with a dollar sign.

Data input to programs, such as responses, must be entered without the dollar sign. Data lines are used by the program running and are not processed by the DCL command line interpreter. For example:

```
$ MAIL          <--- invokes the Mail Utility
SEND            <--- Mail SEND command
JONES, BOB      <--- response to Mail prompt "To:"
Memo            <--- response to Mail prompt "Subj:"
Bob,            <--- Mail message

How's it going?'?

Joe
$               <--- terminates Mail program
$ EXIT          <--- terminates command procedure
```

Comments

Comments may be included by preceding them with an exclamation point (!), which causes everything to the right of it to be ignored by the DCL command interpreter. Comments make command procedures easier to debug and modify later. Spelling DCL commands out rather than using the abbreviations also

makes the command procedure more readable.

Labels

Labels are used by the DCL command line interpreter for conditional processing and repetitive looping. Labels should be placed on separate lines, making them easier to find. Labels can be 255 characters long, may not contain blanks, and must be terminated with a colon (:).

Debugging

The SET VERIFY command tells DCL to display each command as it processes it. This allows you to see where errors are generated, and how strings are translated. SET NOVERIFY turns the verify mode off.

The SHOW SYMBOL command displays the contents of defined symbols, and is used to show the contents of a symbol in a command procedure as it is being executed.

Invoking Command Procedures

Command procedures may be invoked interactively by typing the "at" sign (@) followed by the procedure name. The file type must also be included if it is not ".COM" (the default). Command procedures may be invoked at the command line or from within another command procedure, called nesting. The DCL SUBMIT command will place your command (job) in a batch queue with other jobs waiting to be run. Command procedures are generally submitted as batch jobs when you want them to execute at a specific time, they will take a long time to run, or when a job must run at a reduced priority. The following command submits the command procedure ACCOUNT.COM to the VAX/VMS batch processor:

```
$ SUBMIT ACCOUNT
Job ACCOUNT (queue SYS$BATCH, entry 103) started on SYS$BATCH
```

The SYS$BATCH queue is the default and is used unless otherwise specified with the /QUEUE qualifier. When VAX/VMS runs this job, a process with your rights and privileges will be created and the procedure executed within that process.

Symbols

Symbols may be local (single equal sign) or global (double equal sign). Local symbols are recognized by DCL only at the command level at which it was defined and more deeply nested levels (subsequently called command procedures). Global symbols are recognized at any command level. Local symbols should be used when the symbols is only needed for the duration of the command procedure employing it. You should only define global symbols if you’re going to use them in other command procedures or for the duration of your login session.

An asterisk can be used to tell the command line interpreter (CLI) to accept abbreviations. For example:

```
$ NO*TES == "@SYS$LOGIN:NOTES"
```

This tells the CLI to accept NO, NOT, NOTE, or NOTES as a valid abbreviation for the NOTES command. This notation is usevul for long symbol names.

Lexical Functions

Lexical functions allow you to obtain basically the same information as DCL SHOW commands. However, it’s easier to manipulate information which comes from a lexical function. As an example, the following two command give the same information:

```
$ SHOW TIME                  ! DCL SHOW TIME command
```

```
       12-JUN-1989 14:29:23
   $ WRITE SYS$OUTPUT F$TIME()  ! lexical function
       12-JUN-1989 14:29:25.17
```

The second command is more usable, however:

```
   $!  Show_Date.COM
   $!
   $ TIME&DATE = F$TIME()
   $ DATE = F$EXTRACT(0,11,TIME&DATE)
   $ WRITE SYS$OUTPUT DATE
```

This procedure displays only the date portion of the string returned by the lexical function F$TIME(). (Use @SHOW_DATE to invoke it) VAX/VMS supports lexical functions to manipulate text strings, convert data types, and return information about the system, your process, symbols, files and devices.

Parameters

Eight reserved symbols (P1 through P8) are available to command procedures to supply data to process. By using these parameters in a command procedure, different data can be specified each time it's run. Parameter specification is done on the command line where the procedure is called. Unless designed to, the command procedure will not prompt for parameters. Parameters are separated with spaces and may be character strings, integers, or symbols. If you want to skip a parameter, us a null string (" ").

```
   $! Add.Com
   $! command procedure to demonstrate passing parameters
   $! (add the first and third parameter)
   $!
   $  WRITE SYS$OUTPUT P1+P3

   $ @ADD 12 " " 14
   26
```

If a command procedure requires multiple letters or words as a single parameter, enclose it in quotes and it will be treated as one parameter and not converted to uppercase.

Terminal Output

The WRITE and TYPE commands send data to the terminal. TYPE is used to display the contents of a file, but may also be used to print lines of text from within a command procedure. TYPE may only be used to output text strings. Since the WRITE command is processed be DCL, expressions, symbols and lexical functions are evaluated before the data is sent to the terminal.

The output expression must translate to a string and be sent to the logical device SYS$OUTPUT, but may be a string, lexical function, symbol, or any combination of the three. Here's an example of a command procedure that uses terminal output:

```
   $! Writing a simple text string
   $!
   $  WRITE SYS$OUTPUT "This is a test..."
   $!
   $! Displaying multiple lines at the terminal
   $!
   $  TYPE SYS$OUTPUT Warning!
          It's been 30 days since you changed
          your password.  Change it now!
   $!
   $! Writing a string with a lexical function
   $!
   $  WRITE SYS$OUTPUT " "HI' You are in directory "F$DIRECTORY()' "
```

Terminal Input

The INQUIRE command's default device is the terminal keyboard, while the READ command must be told where to accept data from. The INQUIRE command prompts for input, reads data and assigns it to a symbol. All data is accepted as a character string and is converted to uppercase and compressed (extra blanks removed). The READ command prompts for input if the /PROMPT qualifier is used, accepts data from a specified source and assigns it to a symbol. The data is accepted with no string conversion or compression occurring. Here's an example of a command procedure that uses terminal input:

```
$! Puts whatever you type in the symbol NAME
$! the /NOPUNCTUATION qualifier will suppress the colon
$! and space INQUIRE puts at the end of the prompt
$!
$  INQUIRE /NOPUNCTUATION NAME "What is your name? "
$!
$! Example of READ using SYS$INPUT (terminal) for data
$!
$  READ /PROMPT = "First value: " SYS$INPUT VALUE_1
$  READ /PROMPT = "Second value: " SYS$INPUT VALUE_2
$  WRITE SYS$OUTPUT VALUE_1," + ",VALUE_2," = ",VALUE_1+VALUE_2
```

File I/O

The basic steps to read and write files from within command procedures are similar to most other languages. Use the OPEN command to open the file. If it does not exist, OPEN will create it. Use the READ or WRITE commands to read or write text records from the file. Use the CLOSE command to close the file when you're done.

To open a file for writing, you must use the /APPEND or /WRITE qualifier. The /WRITE qualifier creates a new file and places the record pointer at the beginning of the file. If the file already exists, a new version will be created by OPEN/WRITE. The /APPEND qualifier is used to add records to the end of an existing file. The file must already exist before using the OPEN/APPEND command, and when the file is opened, the record pointer is placed at the end of the file.

To open a file for reading, use the /READ qualifier (the default for the OPEN command). A file opened for reading may not be written to, and the record pointer will initially be placed at the first record in the file. Each time a record is read, the pointer is moved down to the next record. The WRITE/UPDATE must be used to write over an existing record. Here's an example of a command procedure using file input and output:

```
$ OPEN/APPEND OUTPUT_FILE NEW.DAT
$ OPEN/READ INPUT_FILE OLD.DAT
$ READ INPUT_FILE RECORD
$ WRITE SYS$OUTPUT "First record from OLD.DAT - ",RECORD
$ WRITE OUTPUT_FILE "First record from OLD.DAT - ",RECORD
```

To open a file for both reading and writing, use both the /READ and /WRITE qualifiers. The record pointer will be placed at the first record in the file. Using this method, however, you can only overwrite the record you most recently read, and records you replace must be the same length.

Redirecting Command Procedure I/O

Command procedures often invoke VAX/VMS utilities, and these programs will normally get input from the logical device SYS$INPUT. While executing a command procedure, SYS$INPUT is directed to the command procedure itself, and this is why you can put command and data lines for a utility or program directly in the procedure. SYS$COMMAND defaults to the terminal from where a command procedure is being executed, and by redirecting SYS$INPUT to SYS$COMMAND you can use utilities and other programs interactively from command

procedures:

```
$ DEFINE/USER_MODE SYS$INPUT SYS$COMMAND:
$ EDIT JUNK.DAT
```

The /USER_MODE qualifier causes the re-assignment to be in effect only for the next command.

Normally command procedure output is displayed at your terminal. You may redirect output to a file by using the /OUTPUT qualifier:

```
$ @SHOW_TIME/OUTPUT = TIME.DAT
```

By default, DCL error and severe error messages are directed to the file represented by the logical name SYS$ERROR, which usually points to your terminal. If you want to log error messages, simply redirect SYS$ERROR to a file. If you redirect SYS$ERROR without also redirecting SYS$OUTPUT, DCL will send error messages to both, and you'll receive the error messages twice -- at your terminal and in the file.

To completely suppress error messages you can redirect both SYS$ERROR and SYS$OUTPUT to the null device (NL:) or you can use the SET MESSAGE command to turn off all message output. To suppress all messages, use: SET MESSAGE/NOTEXT/NOIDENTIFICATION/NOFACILITY/NOSEVERITY.

Branching and Conditionals

You can use the DCL IF/THEN statements and conditional operators withing command procedures to cause the execution of a command based on the evaluation of a condition. The basic use is: $ IF condition THEN command. The condition is a Boolean expression (True or False) and the command is any legal DCL command. The following is a list of conditional operators:

Operator	Function
.EQ. / .EQS.	Determines if two numbers/character strings are equal
.GE. / .GES.	Tests to see whether the first number/character string is greater than or equal to the second
.GT. / .GTS.	Determines if the first number/character string is greater than the second
.LE. / .LES.	Tests to see if the first number/character string is less than or equal to the second
.LT. / .LTS.	Determines if the first number/character string is less than the second
.NE. / .NES.	Tests to see whether the two numbers/character strings are not equal
.AND.	Combines two numbers with a logical AND (boolean algebra)
.OR.	Combines two numbers with a logical OR (boolean algebra)
.NOT.	Logically negates a value

The following is a command procedure using conditional branching:

```
$! Time.Com
$!
$    TIME = F$TIME()
$    HOUR = F$EXTRACT(12,2,TIME)
$    IF HOUR .LT. 12 THEN GOTO MORNING
$    IF HOUR .LT. 17 THEN GOTO AFTERNOON
$    IF HOUR .LT. 18 THEN GOTO EVENING
$    GOTO END
$  MORNING:
$    WRITE SYS$OUTPUT "Good morning!"
$  AFTERNOON:
$    WRITE SYS$OUTPUT "Good afternoon!"
$  EVENING:
$    WRITE SYS$OUTPUT "Good evening!"
$  END:
$    EXIT
```

Loops

Loops are used to repeat a statement or group of statements until a given condition is met. DCL supports both DO WHILE and DO UNTIL loops. The DO WHILE loop tests the condition before evaluation:

```
$ LOOP:
$    IF .NOT. condition THEN GOTO END
  .
  .
  .
$    GOTO LOOP
$ END:
$    EXIT
```

The DO UNTIL loop executes the statement(s) and then tests the condition:

```
$ LOOP:
  .
  .
  .
$    IF condition THEN GOTO LOOP
$    EXIT
```

Subroutines

The DCL command GOSUB transfers execution control to a label and the RETURN command terminates subroutine execution, returning control to the statement after the GOSUB command. Subroutines are useful where you need to do the same series of commands repeatedly in different parts of a command procedure. They also make procedures easier to read and more compact. The DCL commands GOSUB and RETURN are not supported in VAX/VMS versions before VAX/VMS Version 4.4. The following is an example procedure using a subroutine:

```
$! Personal.Com
$!
$!     opens the personal info file
$!
$  OPEN/WRITE OUTPUT_FILE PERINFO.DAT
$!
$!     collect info
$!
$  INQUIRE RECORD "Enter full name"
$  GOSUB WRITE_FILE
$  INQUIRE RECORD "Enter address"
$  GOSUB WRITE_FILE
$  INQUIRE RECORD "Enter phone number"
$  GOSUB WRITE_FILE
$  CLOSE OUTPUT_FILE
$  EXIT
$!
$!     subroutine WRITE_FILE
$!
$  WRITE_FILE:
$      WRITE OUTPUT_FILE RECORD
$      RETURN
```

Error Handling

The command interpreter will execute an EXIT command if a severe error occurs, terminating the procedure and returning control to the previous command level, unless the DCL ON command is used to specify an action for the command interpreter to take. The ON command supports the three keywords WARNING, ERROR, and SEVERE_ERROR. To override error handling for procedure warnings, for example, use something like this:

```
$ ON WARNING THEN EXIT
  or
$ ON WARNING THEN GOTO label
```

WARNING causes the command procedure to take action if a warning, error, or severe error occurs. ERROR causes the action if an error or severe error occurs, and SEVERE_ERROR causes the action only if a fatal error occurs.

$STATUS and $SEVERITY are reserved DCL global symbols, and each time a command is executed, values are assigned to these symbols. $STATUS holds the full condition code of the last statement and $SEVERITY holds an error severity level. The condition code in $STATUS is valid to the VAX/VMS MESSAGE facility and can be used in conjunction with F$MESSAGE to obtain the actual text message associated with the code:

```
$ SET DEFAULT DUB1:[BYNON]
$ WRITE SYS$OUTPUT $STATUS $X00000001
$ WRITE SYS$OUTPUT F$MESSAGE(%X00000001)
% SYSTEM-S-NORMAL, normal successful completion
```

All DCL commands will return a condition code, but not all condition codes have text messages. Condition codes without text messages will return the message "%NONAME-E-NOMSG Message number (8-digit code)".

The message text isn't very useful for making conditional decisions though, so $SEVERITY is used. It contains one of five possible values extracted from the first three bits of $STATUS. Here are the codes:

Code	Definition
0	Warning
1	Success
2	Error
3	Information
4	Severe Error

Odd values (1,3) indicate success while even values (0,2,4) indicate failure. There are basically two ways to use the status and severity codes to handle errors. The first is to treat $STATUS as a Boolean value:

```
$ SET NOON
$ command                          ! a DCL command
$ IF $STATUS THEN GOTO NO_ERR      ! test $STATUS for T or F
  .
  .                                ! handle the error
  .
$ NO_ERR                           ! continue processing
  .
  .
  .
$ EXIT
```

The second method is to trap the error with the ON WARNING command, then use the severity level to determine an appropriate course of action:

```
$ SET NOON
$ ON WARNING GOTO ERR_TRAP
$ command                          ! a DCL command
$ command                          ! a DCL command
  .
  .
  .
$ EXIT
$!
$! error trap code
$!
$ ERR_TRAP:
$    SEVERITY = $SEVERITY              ! save the error code
$    IF SEVERITY = 0 THEN command      ! if warning...
$    GOTO DONE
```

```
$    IF SEVERITY = 2 THEN command     ! if error...
$    GOTO DONE
$    IF SEVERITY = 4 THEN command     ! if severe error...
$ DONE:
  .
  .
  .
$ EXIT
```

Error checking can be completely disabled with the SET NOON command. When this is in effect, the command interpreter continues updating the condition code, but does not perform any error checking. The DCL command SET ON restors error checking to normal. For example:

```
$ SET NOON      ! turn off error checking
$ command       ! a DCL command
$ SET ON        ! restor error checking
```

Termination

The EXIT command will terminate the current command procedure and return control to the command level that called it while the STOP command terminates all command procedures (if nested) and returns control to DCL.

Example Command Procedures

The following are two example command procedures to demonstrate some of the previously discussed techniques.

Login.Com

```
$! Login.Com - executed each time you log in
$!
$! Check for a network or batch login
$!
$      IF F$MODE() .EQS. "NETWORK" THEN GOTO NETWORK
$      IF F$MODE() .EQS. "BATCH" THEN GOTO BATCH
$!
$! Define process permanent symbols for convenience
$!
$      SD == "SET DEFAULT"
$      SH == "SET HOST"
$      WI*DE == "SET TERMINAL/WIDTH=132"
$      NA*RROW == "SET TERMINAL/WIDTH=80"
$      DIR*ECTORY == "DIRECTORY/SIZE"
$      PU*RGE == "PURGE/LOG/KEEP=2"            ! keep latest 2 version
$      HO*ME == "SET DEFAULT SYS$LOGIN:"
$      WHO == "SHOW USERS"
$      EVE == "EDIT/TPU"
$      EDT == "EDIT/EDT/COMMAND=SYS$LOGIN:EDTINI.EDT"
$      BR*OWSE == "TYPE/PAGE"
$!
$! Define special keys
$!
$      DEFINE/KEY/NOLOG/TERM PF1 "DIR"         ! term ends with <enter>
$      DEFINE/KEY/NOLOG PF2 "EDIT"
$      DEFINE/KEY/NOLOG/TERM/NOECHO PF3 "LOGOUT"
$      DEFINE/KEY/NOLOG/TERM/NOECHO HELP "SHOW KEY/ALL"
$!
$! Modify terminal characteristics
$!
$      SET TERMINAL/INSERT     ! insert mode
$      SET PROMPT = "[BYNON]> "
$!
$! Show time and quit
$!
$      SHOW TIME
$      EXIT
```

```
   $!
   $! If it's a network login, we can now
   $! perform some other commands if desired.
   $! Just quit for now though.
   $!
   $  NETWORK:
   $      EXIT
   $!
   $! If it's a batch job login, set verification on and quit.
   $!
   $  BATCH:
   $      SET VERIFY
   $      EXIT
```

Subdir.Com
~~~~~~~~~~

```
   $! Subdir.Com - how to search and parse character strings
   $!
   $      WRITE SYS$OUTPUT F$DIRECTORY()+ " Subdirectories:"
   $      WRITE SYS$OUTPUT " "
   $!
   $! Search for subdirectory names and display them on the terminal
   $!
   $  DIR$LOOP:
   $      FILE = F$SEARCH("*.DIR")
   $!
   $! If DCL returns a null string (" ") we're done
   $!
   $      IF FILE .EQS. " "THEN GOTO END$DIR$LOOP
   $!
   $! Find the position of the period
   $!
   $      DOT = F$LOCATE(".",FILE)
   $!
   $! Find the position of the right bracket
   $!
   $      BRACKET = F$LOCATE("]",FILE)
   $!
   $! Extract the string between the dot and bracket
   $!
   $      FILE = F$EXTRACT(BRACKET+1,DOT-BRACKET-1,FILE)
   $!
   $! Display the subdirectory name and start over
   $!
   $      WRITE SYS$OUTPUT "      ' 'FILE' "
   $      GOTO DIR$LOOP
   $  END$DIR$LOOP:
   $      EXIT
```

<END PART I>

~~~~~~~~~~

==Phrack Inc.==

Volume Three, Issue Thirty-five, File 8 of 13

+===+

A Beginners Guide to Novell Netware 386

Brought to you by:

The Butler

+===+

As most of you know NOVELL is the most popular PC network software around,with that being the case I decided to put together a little file on just what you can do with a NOVELL network.

* The information in this file is primarily for NOVELL NETWARE 386 networks!!! If you have NOVELL NETWARE 286 some of this information may not be correct.

When the word "Network" is mentioned in this file I am referring to a PC-based network or LAN (Local Area Network).

If you are not familiar with the concept of a "Network" I would suggest you first get acquainted with it by either picking up a good book or if you have access to one, go exploring.

This file is for those who have some experience with networks and or the concept of a network.

(---)

Variations in Setups:

Every network is setup differently is some way. Even within the same company two different networks may be setup different. The differences may be slight or major and can consist of everything from menus to naming conventions.

Companies that install networks as a business are inconsistent with their setups also because every network technician does things differently and every customer wants things to be a certain way.

Keep this idea in mind when exploring different networks because most likely the setup will be different from network to network.

(---)

Terminology:

Bindery-- A database that contains definitions of entities such as users groups, and workgroups. The bindery is comprised of three components: objects, properties, and property data sets.

Console-- The monitor and keyboard at which you actually control fileserver activity.

File Server-- The Computer that the Network software, applications, and some data reside on. (Usually a very powerful one, i.e. Compaq 486 with 1 gigabyte of storage).

Groups-- A means of dealing with users collectively rather than individually. i.e. Word Processing, Accounting.

LAN-- Local Area Network

Login Script-- Similar to autoexec.bat, contains commands that initialize environmental variables, map network drives, and control the user's program execution.

Netware-- Novell's Network Operating System.

Netwire-- Novell's on-line information service, accessible via Compuserve.

Network-- A group of computers that can communicate with each other.

NIC-- Network Interface Card

Novell-- Software Manufacturer

Objects-- any physical or logical entities, including users, user groups, workgroups, file servers, print servers, or any other entity that has been given a name.

Print Server-- A computer dedicated to controlling all jobs for a specified printer.

Properties-- the characteristics of each bindery object. Passwords, account restrictions, account balances, internetwork addresses, list of authorized clients, and group members are all properties.

Property Data Sets-- the values assigned to an entity's bindery properties.

Rights-- Rights control which directories and files a user or group can access and what the user or group is allowed to do with those directories and files.

User-- Any person allowed to work on the network.

WAN-- Wide Area Network

Workstation-- Any usable computer connected to a network.

(---)

Netware Environment:

The SYS:SYSTEM directory is used for system administration and contains operating system files, NetWare utilities, and programs reserved for SUPERVISOR.

The SYS:PUBLIC directory is used for general access and contains NetWare utilities and programs for regular network users.

The SYS:LOGIN directory contains the programs necessary for logging in.

The SYS:MAIL directory is used by NetWare-compatible mail programs. This directory also has and ID number subdirectory for each user that contains the user login script and print job configurations.

(---)

Breaches in Security:

Set Allow Unencrypted Passwords=on/off.

Enter this command from the "CONSOLE".

By changing this command you will disable the encryption scheme which will then allow you to sniff passwords from the cables between workstations and servers.

By default Netware comes with usernames GUEST and SUPERVISOR that have no

passwords.

Also try names like TAPE, BACKUP, SERVER, REMOTE, CONNECT, NOVELL, etc... If you have access to an existing account use SYSCON to get a list of all the user names, most likely there will be one or two accounts that don't have passwords.

Also on some of these accounts that do not have passwords, part of their logon process is the execution of a batch file that executes the individual software i.e. backup. A batch file is a batch file so if its not disabled do the old CTRL-C to break out of the batch file and roam around. Some accounts like the backup account must have supervisor rights so that everything can be backed up. So if you can break out of one of these you can roam the whole Network.

There are also a few neat little programs out there in cyberspace that will make your task of getting access a little easier:

1. THIEFNOV.ZIP ===> THIEFNOV is a TSR that will capture usernames and passwords from a workstation on Novell Networks. The Thief works by hiding in a user's autoexec.bat file, and executing every time someone tries to login to the network. The Thief captures their username and password and saves them in a hidden file in the root directory of their C: drive.

2. TEMPSUP.ZIP ====> TEMPSUP is a utility that will create a user for you to play with. TEMPSUP comes with two programs, an executable and a NLM module. The executable can be run by any user with access to DOS but only gives you the rights of that user. But, the NLM module can be loaded at the Console and will give you Supervisor Rights to the whole Network. The syntax is "Tempsup_username to be created" i.e. f:> tempsup hacker <return>.

3. NETCRACK.ZIP ===> NETCRACK is a brute force hacking program designed for Novell. NETCRACK can be run with out login in to the network but by just loading ipx and netx. NETCRACK starts with AAA and goes from there trying to guess the password for any user. The syntax is "netcrack_username <return>.

These are the only programs I know of made especially for Novell and I have personally tried them all out with excellent results.

If you do get access to a Novell Network and you are not sure what to do, then go to the F:\PUBLIC directory and type HELP. Novell comes with an online help system that uses FOLIO Infobases. The HELP system is very easy to navigate through and is better that the actual Novell Manuals. You can even download the programs NFOLIO.COM & NFOLIO.EXE and the infobases *.NFO to your local PC to examine further.

If you are using the brute force hacking method Novell will stop you dead in your tracks if the Intruder Detection/Lockout option has been enabled because after 3 unsuccessful login attempts the account is locked until a supervisor resets it.

Intruder Detection/Lockout options are as follows:

```
Detect Intruders:                       Yes/No
Intruder Detection Threshold
Incorrect Login Attempts:               #
Bad Login Count Retention Time:         # Days    # Hours   # Minutes

Lock Account After Detection:           Yes/No
        Length of Account Lockout:      # Days    # Hours   # Minutes
```

The following restrictions are optional for every user account:

```
        Account Disabled:                       Yes/No
        Account Has Expiration Date:            Yes/No
                Date Account Expires:
        Limit Concurrent Connections:           Yes/No
                Maximum Connections:
        Allow User To Change Password           Yes/No
        Require Password:                       Yes/No
                Minimum Password Length:
        Force Periodic Password Changes:        Yes/No
                Days Between Forced Changes:
                Date Password Expires:
                Limit Grace Logins:             Yes/No
                        Grace Logins Allowed:
                        Remaining Grace Logins:
        Require Unique Passwords:               Yes/No
```

Novell can also be setup so that users can only logon during certain hours, i.e. 8 a.m. - 5 p.m. Monday thru Friday.

Trustee Assignments grant rights to specific users (or groups) that allow them to use a file or directory in particular ways (i.e., only for reading) The network supervisor can select the appropriate rights to assign to users or groups in each directory or file.

A trustee assignment automatically grants users the right to see to the root of a directory. However, the users can't see any of the subdirectories unless they also have been granted rights in the subdirectories.

Inherited Rights Masks are given to each file and directory when they are created. The default Inherited Rights Mask includes all rights. But this does not mean that users have all rights; users can only use rights that they been granted in trustee assignments.

If the Inherited Rights Mask is modified for a file or subdirectory below the original trustee assignment, the only rights the user can "inherit" for the file or subdirectory are rights that are allowed by the Inherited Rights Mask. For example, if a user is granted Read right with a directory trustee assignment, the right to read files in a subdirectory could be revoked by having the Read right removed from the subdirectory's Inherited Rights Mask.

Both trustee assignments and Inherited Rights Masks use the same eight trustee rights to control access to directories and file.

S -- Supervisory

> Supervisory right grants all rights to the directory or file. At the directory level, this right grants all rights to the directory and to any files, subdirectories, or subdirectory files in that directory. The Supervisory right overrides any restrictions placed on subdirs or files with Inherited Rights Masks. Users who have the Supervisory right in a directory can grant other users Supervisory rights to the directory, its files, and subdirectories.
>
> Once the Supervisory right has been granted, it can be revoked only from the directory is was granted to. It cannot be revoked in a file or subdirectory.

R -- Read

> Read right allows users to open and read files. At the directory level this right allows users to open files in a directory and read the contents or run the program. At the file level, this right allows users to open and read the file (even when the right has been revoked at the directory level).

W -- Write

> Write right allows users to write to files. At the directory level,

this right allows users to open and write to (modify the contents of) file in the directory. At the file level, this right allows users to open and write to the file (even if the right has been revoked at the directory level).

C -- Create

Create right allows users to create directories and files. At the directory level, this right allows users to create files and subdirectories in the directory. At the file level, this right allows users to salvage a file after it has been deleted.

E -- Erase

Erase right allows users to delete directories and files. At the directory level, this right allows users to delete a directory as well as any files, subdirectories, and subdirectory files in that directory. At the file level, this right allows users to delete the file (even when the right has been revoked at the directory level).

M -- Modify

Modify right allows users to change directory and file attribute sand to rename subdirectories and files. At the directory level, this right allows users to change the attributes of and rename any file, subdir, or subdirectory file in that directory. At the file level, this right allows users to change the file's attributes or to rename the file (even when the right has been revoked at the directory level).

F -- File Scan

File Scan right allows users to see files. At the directory level, this right allows users to see files and subdirectories in a directory. At the file level, this right allows users to see the file (even when the right has been revoked at the directory level).

A -- Access Control

Access Control right allows users to modify trustee assignments and Inherited Rights Masks.

(--)

As a network user, you should be familiar with the operation of the personal computer you are using. If you have an IBM PC-type workstation, you should also be familiar with basic Disk Operating System (DOS) commands.

User Basics is divided into the following ten sections. The first section explains basic networking concepts and gives an overview of how a NetWare network operates.

The second section introduces the NetWare menu and command line utilities and explains how to use them.

The next seven sections explain some basic network tasks:

- Booting up
- Logging in and out
- Creating your login script
- Mapping your drives
- Sending messages
- Managing files and directories
- Printing

Some basic troubleshooting hints are covered under "What If ..." at the end of each of these modules and are also listed in the index.

The last section lists some common error messages and how to respond to them.

This booklet does not explain how to perform every network task or how to use

every available network command. For complete explanations of all network tasks and commands, see NetWare v3.11 Utilities Reference.

INTRODUCTION TO NETWARE

If your personal computer is part of a NetWare network, it is connected to other computers and peripherals. You can share files and resources and communicate with others in your workgroup, thus increasing productivity.

This introduction answers the following questions about using a NetWare network:

- What is a NetWare network?
- How does a network operate?
- How are files stored on a network?
- Who can use the network?
- How is information protected on a network?

WHAT IS A NETWARE NETWORK?

A NetWare network is a group of computers (such as IBM PCs or Macintoshes) that are linked together so they can communicate and share resources.

Network users, each working on a different personal computer, can communicate with each other via the network. They can also share network resources (hard disks on the file server, data, applications, and printers) and use any service the network provides (for example, access to a mainframe system).

HOW DOES A NETWORK OPERATE?

To understand how a network operates, you must know about the principal components of a network: the file server, the workstations, and the software that runs on each----NetWare and operating systems like DOS, OS/2, VMS, UNIX, and the Macintosh operating system.

Beyond these basic components, a NetWare network can incorporate mainframe computers, backup devices, modem pools, and different types of servers (such as file servers, print servers, or archive servers).

The Network Workstations and DOS

Workstations are the personal computers on which network users do their work. Workstations are used much like non-networked personal computers. The only difference is that they can access files from more than just the local drives. Each workstation processes its own files and uses its own copy of DOS.

The Network File Server and NetWare

The file server is a personal computer that uses the NetWare operating system to control the network. The file server coordinates all of the workstations and regulates the way they share network resources. It regulates who can access which files, who can make changes to data, and who can use the printer first.

All network files are stored on a hard disk in or attached to the file server, instead of on diskettes or hard disks in individual workstations.

The NetWare Workstation

Workstations use two pieces of software to communicate with the file server, the shell and a protocol. The shell must be loaded into each workstation before that workstation can function on the network.

The NetWare shell, either NET3 or NET4 (depending on whether you are using DOS 3.x or 4.x), directs workstation requests to DOS or NetWare. When a workstation makes a request (asks to do a task), the shell decides if it is a workstation task (to be directed to DOS) or a network task (to be directed to NetWare). If the request is a workstation task (such as using the DOS DIR command to list the files in a local directory), DOS should handle the request. If the request is a network task (such as printing a job on a network printer),

NetWare should handle the request. The shell sends the request to the appropriate operating system, somewhat like a railroad track switcher sends trains to the proper destination.

The workstation shell uses another file, IPX.COM, to send network messages to the file server and, in some cases, directly to other network stations. This IPX protocol is the language the workstation uses to communicate with the file server.

HOW ARE FILES STORED ON A NETWORK?

All network information is stored on the file server's hard disk. The system for storing that information is called the "directory structure."

The NetWare directory structure, or storage system, is organized into

- File servers, which contain one or more
- Volumes, which can span several hard disks and are divided into
- Directories, which can contain other directories (subdirectories) and
- Files.

A directory structure can be compared to a filing cabinet system.

- The file server corresponds to the filing cabinet.

- The volumes correspond to the filing cabinet drawers. Each file server has at least one volume, the SYS volume, which is created when the server is installed. In NetWare v3.11, however, one volume can span several hard disks.

- The directories correspond to the hanging folders within the filing cabinet drawers. You can create and delete directories to suit your organizational needs, much as you insert hanging folders into, and remove them from, a filing cabinet.

- Directories can contain other directories, which are sometimes referred to as "subdirectories. These directories within a directory then correspond to the manila folders inside the hanging folders. They divide directories into smaller units, just as manila folders divide hanging folders into smaller units.

- And finally, directories contain actual files, just as manila folders contain individual documents. A file might be a letter or a list of addresses. When you save information in a file, you give the file a unique name so you can retrieve it later.

WHO CAN USE THE NETWORK?

Before being able to work on the network, a person must be designated as a network user. Network users can be assigned four levels of responsibility on the network.

- Regular network users

- Operators (file server console operators, print queue operators, print server operators)

- Managers (workgroup managers, user account managers)

- Network supervisors

Regular network users are the people who work on the network. They can run applications and work with files according to the rights assigned to them.

Operators are regular network users who have been assigned additional privileges. For example, a file server console operator is a network user who is given specific rights to use the FCONSOLE utility.

Managers are users who have been given responsibility for creating and/or managing other users. Workgroup managers can create and manage users; user

account managers can manage, but not create, users. Managers function as supervisors over a particular group, but they do not have supervisor equivalence.

Network supervisors are responsible for the smooth operation of the whole network. Network supervisors maintain the system, restructuring and updating it as needed. Supervisors may also teach regular network users how to use the network.

HOW IS INFORMATION PROTECTED ON A NETWORK?

All information on a NetWare network is stored in a central location---the file server's hard disk. However, all users should not be able to access all information (such as payroll files). In addition, users should not always be able to access the same data file at the same time; otherwise, they may overwrite each other's work.

To prevent problems like these, NetWare provides an extensive security system to protect the data on the network.

NetWare security consists of a combination of the following:

- Login security

  Login security includes creating usernames and passwords and imposing station, time, and account restrictions on users.

- Trustee rights (privileges) assigned to users

  Trustee rights control which directories and files a user can access and what the user is allowed to do with those directories and files, such as creating, reading, erasing, or writing to them.

- Attributes assigned to directories and files

  Directory and file attributes determine whether that directory or file can be deleted, copied, viewed, or written to. Among other things, they also mark a file as shareable or non-shareable.

These three levels of security work together to protect the network from unauthorized access.

REVIEW

This introduction explained the following:

- A NetWare network links personal computers so users can communicate and share resources.

- A NetWare network consists of two or more workstations and at least one file server.

  Workstations are personal computers on which network users do their work. Workstations run their own native operating system (for example, DOS) and process their own files. They can access files, applications, and resources through the file server.

  File servers are personal computers that use the NetWare operating system to coordinate all network activities.

- Workstations and the file server communicate via the NetWare shell, which must be loaded into each workstation (just as DOS must be loaded into each workstation). NET3 or NET4 (the NetWare shells corresponding to DOS 3.x or 4.x) sends workstation requests to the proper operating system (file server or workstation) for processing.

- The shell uses a protocol, such as IPX, to send messages to the appropriate network station.

- Information is stored on the file server in a directory structure that is

made up of volumes, directories, and files.

- There are four types of network users: regular network users, network operators, network managers, and network supervisors. The type of user you are is determined by your responsibilities.

- NetWare's extensive security system prevents users from corrupting data in network files and prevents unauthorized users from accessing restricted files.

WHAT ARE MENU AND COMMAND LINE UTILITIES?

You use NetWare utilities to perform network tasks. There are two types of utilities: menu utilities and command line utilities. Menu utilities let you perform network tasks by choosing options from menus. Command line utilities let you perform tasks by typing commands at the DOS command line. This section explains how to execute both types of NetWare utilities.

WORK WITH MENU UTILITIES

Access a Menu Utility

To access a menu utility, such as FILER, type the utility's name at the DOS prompt and press <Enter>. The utility's main menu is displayed along with a screen header showing the following:

- The utility's full name
- The current date and time
- The directory path leading up to your current directory (some utilities)
- Your username on your file server (some utilities)
- Your connection number (some utilities)

Exit a Menu Utility

There are two ways to exit a menu utility:

- Press <Escape> until an exit confirmation box appears. Then highlight "Yes" and press <Enter>.

- Press the Exit key (usually <Alt><F10>). Do not press the Exit key to exit a menu utility if you have made changes within the utility; if you do, the changes are not saved. Exiting via the Escape key saves your changes.

Additional Information

Once you have accessed a menu utility and the main menu is displayed, you are ready to work. Menu utilities use certain keys to perform special functions. The utilities also have certain standard components. The keys, wildcards, and components are described below.

F1 (Help) Key. Displays help screens.
If you press the help screen once, a help screen that applies to the task you are currently working on appears. The help screen describes all the options on the screen. To get help on a specific option, highlight the option and press <Enter>.

If you press the Help key twice, your computer's function key assignments are listed. There are three screens containing function key assignments. Press the <PageDown> key to see subsequent screens.

F5 (Mark) Key. Allows you to mark multiple items in a list so you can add or delete several items at once.

Esc (Escape) Key. Has three functions:

1) If you are on a menu screen, pressing <Escape> allows you to return to a previous menu.

2) If you are at the main menu, pressing <Escape> causes an exit confirmation box to appear. By highlighting "Yes" and pressing

<Enter>, you exit the menu utility and return to the menu or command line prompt.

3) If you are performing a process, pressing <Escape> allows you to continue.

Wildcard characters (* and ?). DOS and NetWare recognize these as universal replacements for any other character or set of characters. Wildcards can be used to search for groups of volumes, directories, or files, or they can be used to search for a particular file when you are unsure of its complete name.

An asterisk (*) in a filename indicates that any character can occupy that position and all remaining positions in the filename. For example, in the FILER utility, to copy all subdirectory's files with the extension .EXE to another directory, type "*.EXE" in the menu's entry box and press <Enter>.

In contrast, a question mark (?) in a filename indicates that any character can occupy that position, and that position only. So, if you were to type "ACCOUNT?.NEW", you would copy files like ACCOUNT1.NEW, ACCOUNT2.NEW, and so on.

NetWare's use of wildcard characters differs from DOS's in one respect. For example, to represent all files in a directory, DOS expects you to type "*.*", whereas NetWare only needs one asterisk (*).

For more information about wildcard characters (global filename characters), see your DOS manual.

Components. When you first access a menu utility, the main menu is displayed. Menus contain options you can choose from. Options can be selected one of two ways:

- You can use the arrow keys to highlight the option you want. Then press <Enter>.
- You can type the first letter of an option to highlight that option. If more than one option in the menu starts with the same letter(s), type enough additional letters to distinguish one option from the others. (For example, if both "Search" and "Select" were options, you would have to type "Sel" to highlight "Select.") Once the option you want is highlighted, press <Enter>.

When you select an option from the main menu, additional menus and displays appear on the screen. These displays include lists, entry boxes, insets, forms, and confirmation boxes. Each type of screen display is explained below.

Lists	Lists are similar to menus, and items in the lists can be selected the same way menu options are. However, you can also add to and delete items from some lists. Lists may have more than one column, and they may extend below the screen display. Press the Down-arrow key to see additional items. Pressing <Ctrl><PageDown> takes you to the bottom of the list. Pressing <Ctrl><PageUp> takes you to the top of the list.
Entry boxes	Entry boxes are boxes in which you can get information, such as a username or pathname. The Delete, Backspace, and arrow keys work in these boxes.
Insets	Insets display information that cannot be edited (except by the network supervisor). Regular users cannot add to or delete from the information in this window.
Forms	Forms are windows that contain fields. You can move around in a form using the arrow keys or the Enter key. (When you press <Enter>, the cursor moves to the next field in the form.) You can change the information in the field by highlighting the field and pressing <Enter>.

What you do next depends on the type of field. Some fields allow you to type in information; others display menu items to select.

Confirmation boxes Confirmation boxes are displayed whenever you exit a menu utility or whenever you create or delete items (such as directories or files). You can either confirm or cancel the action by selecting "Yes" or "No" and pressing <Enter>.

WORK WITH COMMAND LINE UTILITIES

Command Format

The command format displays the appropriate syntax for command line utilities. Command line utilities are typed in at the DOS prompt.

The following are examples of the command formats for the NPRINT and the TLIST utilities:

NPRINT path [option...] <Enter>

TLIST [path [USERS | GROUPS]] <Enter>

Conventions

The conventions for these example command formats are explained below:

NPRINT Words that appear in all capital letters must be spelled exactly as shown. Although they appear in capital letters, they can be typed in either upper or lower case.

path Words that appear in lower case are variables. They should be replaced with the information pertinent to your task. In this case, "path" would be replaced with the path leading to and including the file you want to indicate, and you would replace "option" with any NPRINT options you want to specify.

[ ] Square brackets indicate that the enclosed item is optional: you can enter a command with or without the enclosed item. In this case, "option" is optional.

.... Ellipses indicate that more than one option can be used with the command. In this case, more than one NPRINT option can be entered in the command.

<Enter> The angle brackets indicate that you should press the key whose name appears between them.

Always press <Enter> after typing the command format for command line utilities.

[[ ]] Nested square brackets indicate that all enclosed items are optional. However, if you use the item(s) within the innermost brackets, you must also use the item(s) within the outer brackets.

| A vertical bar or "pipe" means "either, or." You can use either the item to the left of the vertical bar or the item to the right, but not both.

Wildcard Characters

DOS and NetWare recognize wildcard characters (* and ?) as universal replacements for any other character or set of characters. Wildcards can be used to search for groups of volumes, directories, or files, or to search for a particular file when you are unsure of its complete name.

An asterisk (*) in a filename indicates that any character can occupy that position and all remaining positions in the filename. For example, to search

for all filenames with the extension .EXE in your default directory, type "NDIR *.EXE" and press <Enter> to display the list.

In contrast, a question mark (?) in a filename indicates that any character can occupy that position, and that position only. So, if you were to type "NDIR *.?", you would see a list of all files in your default directory with a single-character extension or no extension at all.

NetWare's use of wildcard characters differs from DOS's in one respect. For example, to represent all files in a directory, DOS expects you to type "*.*", whereas NetWare only needs one asterisk (*).

For more information about wildcard characters (global filename characters), see your DOS manual.

GET HELP IN NETWARE

Use the NetWare HELP utility to view on-line information about NetWare utilities, NetWare system messages, and NetWare concepts. NetWare HELP allows you to search for and retrieve information from infobases (information databases). To access HELP, type

    HELP <Enter>

Press <Enter> again to bring up the main menu. For more information on how to use NetWare HELP, press the Tab key until you get to "How to use this reference." Then press <Enter>.

BOOT UP

To "boot up" your workstation means to turn on your computer, load DOS, and then load the workstation shell. You accomplish all of this with a boot diskette, or you can put the necessary boot files on your workstation's hard disk. These boot files start up the workstation operating system, load the NetWare shell, and gain access to the network.

Create Boot Diskettes

1. Format a blank diskette as a boot diskette, using the DOS FORMAT command. Insert a diskette into drive A and type

       Format a: /s <Enter>

   Follow the screen prompts.

2. Copy IPX.COM and the shell file (NETx.COM) onto the boot diskette or to the root directory of your workstation's hard disk.

   If your workstation uses DOS 3.x, use NET3.COM.

   If your workstation uses DOS 4.x, use NET4.COM.

3. Copy these following additional boot files to the boot diskette or your hard disk, if needed. Your network supervisor can provide you with these files:

   AUTOEXEC.BAT
   CONFIG.SYS
   SHELL.CFG

   See also "Boot files" in NetWare v3.11 Concepts and Appendix A in NetWare v3.11 Installation.

4. Label the boot diskette.

Create an AUTOEXEC.BAT File

You can create an AUTOEXEC.BAT file that automatically loads the shell file each time you boot the workstation. This AUTOEXEC.BAT file can also set your workstation to the first network drive (F), connect you (user MARIA) to a file

server (WONDER), and set your DOS prompt to show your current directory (PROMPT PG).

Follow these steps to create your AUTOEXEC.BAT file:

1. Insert your boot diskette into drive A and change to drive A. If you plan to boot from your hard disk, change to your hard disk drive (C or D).

2. If you are using DOS 4.x, type

```
COPY CON AUTOEXEC.BAT  <Enter>
IPX  <Enter>
NET4  <Enter>
F:  <Enter>
LOGIN WONDER/MARIA  <Enter>
PROMPT $P$G  <Enter>
<Ctrl>Z  <Enter>
```

   If you are using DOS 3.x, replace NET4 with NET3.

LOGIN/LOGOUT

When you log in to a network, you establish a connection between your workstation and the file server. When you log out, you terminate that connection.

To log in to the network, you must type in a unique password. If there were no password, other unauthorized users could easily get to your files and use them for their purposes.

Log In to Your Network

To log in to your default server, type

    LOGIN servername/username <Enter>

Replace servername with the name of the file server you want to log in to. Replace username with your login name and (if applicable) type your password when you are prompted for it.

Log Out of Your Network

To log out of your default server, type

    LOGOUT <Enter>

To log out of a file server you are attached to, type

    LOGOUT servername <Enter>

Attach to Another File Server

Attach to another file server if you want to do the following:

- Send messages to users on that file server
- Map a drive to that file server
- Copy a directory to that file server

To access another file server while remaining logged in to your default file server, type

    ATTACH servername/username <Enter>

Replace servername with the name of the server you want to attach to. Replace username with the username you have been assigned to use on that file server.

Create or Change a Password

1. To create or change a password on your default server, type

       SETPASS <Enter>

   The following prompt appears on the screen:

   Enter your old password:

2. If you are changing a password, enter the old password. If you are creating a new password, press <Enter>. The following prompt appears on your screen:

   Enter your new password:

3. Enter the password you want. The following prompt appears:

   Retype your new password:

4. Enter the new password again. The following message appears on your screen:

   Your password has been changed.

View Who You Are on Your Network

Type

    WHOAMI <Enter>

Information similar to the following is displayed:

```
    You are user FRANK attached to server MKTG, connection 1
    Server MKTG is running NetWare v3.11.
    Login time:  Wednesday October 2, 1991  8:05 am

    You are user GUEST attached to server ACCT, connection 7
    Server ACCT is running NetWare v3.11.
    Login time: Wednesday, October 2, 1991  8:05 am
```

This screen display indicates that you are attached to both file servers MKTG and ACCT. Your username on MKTG is FRANK, and your username on ACCT is GUEST.

View File Servers on Your Network

Type

    SLIST <Enter>

Information similar to the following appears:

Known NetWare File Servers	Network	Node Address
RECORDS	[CED88]	[2608C234732]
SALES	[CED87]	[2608C217651]
MFG	[CED86]	[2608C293185]

View Current Users on Your File Server

You must be attached to a file server before you can view the list of users for that file server.

Type

    USERLIST <Enter>

Information similar to the following appears:

```
    User Information for Server BLOOM
    Connection  User Name     Login Time
```

1	JOE	4-17-1991 8:05 am
2	*CORRINE	4-17-1991 11:20 am
3	PAULO	4-17-1991 7:58 am
4	GUS	4-17-1991 6:01 pm

An asterisk (*) appears next to your username.

What If ...

.... I can't log in?

o Your password may have expired or you may have run out of grace logins.

  Your supervisor or manager has to unlock your account.

o You haven't changed to the network login drive (F).

o The LOGIN.EXE file is missing.

o Your shell may be outdated. Type

    NVER <Enter>

  Report the version number to your supervisor.

o Your network board may not be seated correctly.

o Your file server may be down. Type

    SLIST <Enter>

  If your file server is listed, log in by typing

    LOGIN servername/username <Enter>

o You may be restricted from logging in during certain times. Ask the network supervisor.

.... My screen is frozen?

o Your supervisor should run the MONITOR utility and clear your connection. This saves the work you were doing. Then complete one of the two following tasks:

  o To warm boot, press <CTRL><ALT><DEL> simultaneously.

  o To cold boot, turn the computer OFF, wait 15 seconds, and then turn it ON again.

o Your network cable may not be connected or terminated properly. Notify your supervisor.

o Your node (or station) address may be in conflict with another workstation. See if new workstations have been added to your network.

o You may have the wrong IPX configuration. Ask your supervisor.

o You may have received a message while in graphics mode. Disable messages before entering graphics mode by typing

    CASTOFF <Enter>

CREATE YOUR LOGIN SCRIPT

Your login script is a program that automatically sets up your workstation's environment each time you log in. It performs tasks such as mapping network drives for you, automatically executing programs and starting applications, and attaching you to different file servers.

This section introduces some basic login script commands.

To access your login script, follow these steps:

1. Type

       SYSCON <Enter>

2. Select "User Information" from the main menu.

3. Select your user name from the list of users that appears.

4. Select "Login Script."

5. Enter the commands you need in your login script. Some common commands are listed under "Common Login Script Commands" below.

6. Exit and save the login script by pressing <Escape> and answering "Yes" in the confirmation box.

7. To execute your new login script, you must first log out of the network, and then log in again.

Common Login Script Commands

The commands below can be used in your login script. Each command is followed by its purpose and an example of how to use it.

MAP INS16:= Inserts the drive as the next available search drive.

```
MAP INS16:=pd3\sys:jan
```

MAP drive:= Maps the specified drive to the given directory.

```
MAP G:=pd3\sys:home\jan
```

MAP *n:= Maps the next available drive to the given directory.

```
MAP *1:=pd3\sys:home\jan
```

Runs an executable file (a file with an .EXE or .COM extension).

```
#SYSCON
```

REMARK
* These three commands allow you to insert explanatory text in the login script. They will not appear on your screen.
;

```
REMARK Be sure to update the PROJECTS file.

* Check for new mail.

; Assign OS-dependent Search mappings.
```

ATTACH Allows you to attach to other file servers while remaining logged in to your current file server.

```
ATTACH pd3\jan
```

SET Allows you to set DOS variables.

```
SET wp="/u-jlw/"

SET usr="jwilson"
```

IF...THEN Executes certain commands, if a specified condition exists.

```
IF DAY_OF_WEEK="Monday" THEN WRITE "AARGH..."
```

.... My login script doesn’t execute all the way?

- You may have inserted an EXIT command to a batch file in the middle of your login script. Anything after the EXIT command is ignored. Move the EXIT command to the end of your login script.

- An IF...THEN clause in your login script may be incomplete or incorrect. Check the proper command format in Appendix A of NetWare v3.11 Installation.

.... I am unable to map a drive to another file server?

The file server you want to map a drive to may be down. To check whether the file server is up, type

```
SLIST  <Enter>
```

.... I add some mapped drives to my login script and some I wanted are gone?

The system login script executes before the user login script. You can overwrite the mapped drives in the system login script with those in your user login script. Instead of using the command "map drive:=", use the command "map ins 16:=" or "map *1:=". (Remember: You can have only 26 drive mappings.)

VIEW OR CREATE YOUR MAPPED DRIVES

Mapped drives point to particular locations in the directory structure. In NetWare, there are three type of drives: local drives, network drives, and search drives. Local drives are physically attached to a workstation. Network drives allow users to access particular locations in the directory structure. Search drives allow users to execute program files (such as applications or utilities) that are in a directory other than the user’s current directory. For more information, see "Drive mappings" in NetWare v3.11 Concepts.

This section tells you how to do the following:

- View all mappings
- Map network drives
- Map search drives

View All Mapped Drives

Type

```
MAP  <Enter>
```

You see information similar to the following:

```
DRIVE A:  maps to a local drive
DRIVE B:  maps to a local drive

DRIVE F:= COUNT/SYS:  /HOME/KAREN
DRIVE G:= COUNT/SYS:  /
DRIVE H:= COUNT/ACCT: /ACCDATA

-------

SEARCH1:=Z:  [COUNT/SYS:  /PUBLIC]
SEARCH2:=Y:  [COUNT/SYS:  /PUBLIC/WP]
SEARCH3:=X:  [COUNT/ACCT:  /ACCREC]
```

Map Network Drives

Suppose you want to map a network drive to a directory in which you have files. To see what network drive letters are available, type

```
MAP  <Enter>
```

Choose a drive letter that is not being used, such as J. Type

```
    MAP J:= path  <Enter>
```

Replace path with the directory path (including the file server name and the volume name) leading to the directory to which you want to map network drive J.

For example, suppose your username is MARIA and you want to map drive J to your home directory, which is on file server COUNT in volume SYS. Type

```
    MAP J:= COUNT/SYS:HOME/MARIA  <Enter>
```

MAP SEARCH DRIVES

Suppose your search drives appear as follows:

```
    SEARCH1:=Z:  [COUNT/SYS:  /PUBLIC]
    SEARCH2:=Y:  [COUNT/SYS:  /PUBLIC/WP]
```

The next available search drive is SEARCH3 (S3). To map a search drive to directory ACCREC on volume ACCT, type

```
    MAP S3:=COUNT/ACCT:ACCREC  <Enter>
```

When you type MAP again, the new search drive appears:

```
    SEARCH1:=Z:  [COUNT/SYS:  /PUBLIC]
    SEARCH2:=Y:  [COUNT/SYS:  /PUBLIC/WP]
    SEARCH3:=X:  [COUNT/ACCT:  /ACCREC]
```

What if ...

.... I just mapped a drive and then rebooted, and now the mapped drive is gone?

Did you map the drive in your login script? Drives mapped at the command line are temporary----they are deleted when you log out of your file server or turn off your workstation. If you want the mapping to be permanent, you must enter it in your login script.

.... The system won't accept my mapped drives?

o You may not have rights to the directory you want to map to. Change to that directory and type

```
        RIGHTS  <Enter>
```

    If your rights aren't sufficient, see your supervisor.

o You may have used the wrong command format.

.... I just viewed my mapped drives and some of them seem to be incorrect?

Did you use the DOS CD command to change your default directory? Changing directories changes your mapping.

.... My search drives are in reverse order?

Search drives are numbered, but their associated drive letters begin in reverse alphabetical order. For example, the first search drive (Search 1 or S1) appears as network drive Z, the second one appears as network drive Y, and so on. However, in your login script, they should appear in normal alphabetical order.

SEND MESSAGES TO OTHER USERS

You can communicate with other users on your network by sending messages from your workstation command line.

This section explains how to do the following:

- Send a message to one or more users
- Send a message to all workstations
- Block/allow messages from other workstations

Send a Message to One or More Users

Suppose you want to send the following message to users CINDY and ERIC: "Meeting at 1:30 today." Also suppose that CINDY and ERIC are logged in to your default server. Type

```
SEND "MEETING AT 1:30 TODAY" CINDY, ERIC  <Enter>
```

A confirmation message appears, telling you that the message was sent.

If CINDY is logged in to another file server called SALES, attach to that file server and type

```
SEND "MEETING AT 1:30 TODAY" SALES/CINDY  <Enter>
```

Send a Message to All Workstations

Suppose you want to send the following message to all workstations: "Paychecks are here." Type

```
SEND "PAYCHECKS ARE HERE." EVERYONE  <Enter>
```

A confirmation message appears listing all the users to whom the message was sent.

If you want to send a message to everyone on another file server, you must be attached to that file server and specify the name of the file server in the command.

Block/Allow Messages from Other Workstations

If you do not want to receive messages sent to you from any network stations, type

```
CASTOFF   <Enter>
```

The following message appears on your screen:

```
Broadcasts from other stations will now be rejected.
```

To allow your workstation to again receive messages from other network users, type

```
CASTON  <Enter>
```

The following message appears on your screen:

```
Broadcast messages from the console and other stations will now be
accepted.
```

What If ...

.... I am unable to send a message to a user?

- Is the user logged in? Type

  ```
  USERLIST  <Enter>
  ```

- Is your message buffer full? You can only receive up to two messages. You must clear these messages from your screen (by pressing <Ctrl><Enter>) before you can receive others.

- Did you type the SEND command properly?

.... I am unable to send messages to users on another file server?

o Did you attach to that file server?
o Is the user logged in? Type

```
USERLIST <Enter>
```

o Did you type the SEND command properly?

MANAGE FILES AND DIRECTORIES

You can manage your files and directories in a variety of ways. You can copy, delete, rename, view, write to, share, and print them. NetWare uses a system of file and directory rights and attributes to make sure that only authorized network users can access and handle network data.

Attributes are assigned to files and directories. They override rights, which are assigned to users. For example, suppose you have the right to rename files (the Modify right). However, the file you want to copy is flagged with the Rename Inhibit attribute. This prevents you from renaming it, even though you have the right to do so.

For more information, see "Attributes" and "Rights" in NetWare v3.11 Concepts.

Know Your Rights

To view your rights in your default directory, type

```
RIGHTS <Enter>
```

If your effective rights include all rights, the following information appears:

```
SERVER1\SYS:PUBLIC\UTIL
Your effective rights for this directory are [SRWCEMFA]
    You have Supervisor Rights to Directory. (S)
   *May Read from File.                      (R)
   *May Write to File.                       (W)
    May Create Subdirectories and Files.     (C)
    May Erase Directory.                     (E)
    May Modify Directory.                    (M)
    May Scan for Files.                      (F)
    May Change Access Control.               (A)

*Has no effect in directory.

Entries in Directory May Inherit [SRWCEMFA] rights.  You have ALL RIGHTS to
Directory Entry.
```

Copy a File to Another Network Directory

Suppose you want to copy a file called ACC.DAT from your default directory (for example, F) to the SALEPROG directory in volume SYS on the file server SALES. First, make sure you have a drive (for example, G) mapped to SALEPROG as follows:

```
G:=SALES/SYS:SALEPROG
```

To copy ACC.DAT from your default directory to the SALEPROG directory, type

```
NCOPY F:ACC.DAT TO G:  <Enter>
```

Suppose you want to copy a file called ACC.DAT from the SALEPROG directory in volume SYS on the file server SALES to your default directory. Also suppose drive G is mapped to SALEPROG as G:=SALES/SYS:SALEPROG. Type

```
NCOPY G:ACC.DAT F:  <Enter>
```

Copy All of a Directory’s Files to Another Directory

1. Type

FILER <Enter>

and select "Directory Contents" from the "Available Topics" menu.

2. Select the directory you want to copy from the "Directory Contents" window. The "Subdirectory Options" window appears.

3. Select "Copy Subdirectory's Files." The "Copy Subdirectory To:" window appears.

4. To copy subdirectory files, complete one of the following:

   - Copy to a subdirectory in your current directory. Type the name of the directory; then press <Enter>.

     You can also use <Insert> to bring up the "File Servers/Local Drives" window, from which you can select your directory path by selecting file server, volume, and directory options.

     After you select your directory path, press <Escape> to bring your cursor back to the "Copy subdirectory To:" window. Then press <Enter> to copy your subdirectory's files.

   - Copy to a directory on another volume on your file server. Type in the name of the volume and directory; then press <Enter>.

     You can also use <Insert> to bring up the "File Servers/Local Drives" window, from which you can select your directory path by selecting file server, volume, and directory options.

   - Copy to a directory to another file server. You must be attached to the file server you want to copy files to. Type in the name of the file server, volume, and directory; then press <Enter>.

Delete a File

1. Type

   FILER <Enter>

2. Select "Directory Contents" from the "Available Topics" menu.

3. Highlight the file you want to delete from the "Directory Contents" window and^S press <Delete>. Answer "Yes" in the confirmation box.

   To delete more than one file, use the Mark key (<F5>) to highlight multiple files; then press <Delete>. Answer "Yes" in the confirmation box.

Salvage a File You Just Deleted

1. Type

   SALVAGE <Enter>

2. Select "View/Recover Deleted Files" from the "Main Menu Options"window. To change to another volume, you must select the directory path from the "Select Current Directory" option in the main menu.

Note: If you have too many salvageable files to fit on the screen, you will see the heading "Inc^Qomplete." Scroll through the list to see the entire list, or use the Mark Pattern key <F6> to mark the file pattern. Then exit the list and reenter it.

3. To salvage files using wildcards or to salvage a specific file, type the information in the "Erased File Name Pattern To Match" window.

   To view all salvageable files, press <Enter>.

4. To salvage a file, complete one of the following:

- Salvage a single file. Select the file you want to salvage. Select "Yes" from the "Recover This File" box.

- Salvage multiple files. Use the Mark key (<F5>) to select multiple files. Select "Yes" from the confirmation box.

- Salvage multiple files using wildcards. To match a filename pattern or extension, press the Mark Pattern key (<F6>) and type the pattern you want to match.

  Once you match the pattern of the files you want to salvage, press <Enter> and select "Yes" from the "Recover ALL marked files?" confirmation box.

5. Press <Escape> to exit SALVAGE.

Find a Lost File

Suppose you don't remember the location of a file. The file is called FUTURE.DAT. You think it may be in the PROGRAMS directory, and drive G is mapped to that directory.

To find the location of the lost file, type

    NDIR G: FUTURE.DAT <Enter>

If you don't know which directory the file is in, change directories back to the volume level. Then type

    NDIR filename sub <Enter>

The NDIR utility searches all those directories you have rights to on the volume for the file.

Rename a Directory

Suppose you want to change the name of the ACCT directory to PROGRAMS. Also suppose drive G is mapped to ACCT in volume SYS on file server RECORDS as follows:

    Drive G: = RECORDS/SYS:ACCT

To rename the directory, type

    RENDIR G: PROGRAMS <Enter>

Note: You must be attached to a file server before you can change the name of a directory on that file server.

  You must also have the Modify right in the directory to rename subdirectories in that directory.

  Drive mappings in login scripts (if they exist) must be changed to reflect the new name of the directory.

What If ...

.... I can't copy?

- You may not have sufficient rights. Type

  RIGHTS <Enter>

  You must have the Create right to copy files into a directory.

- The file may be flagged "non-shareable" and may be in use. Type

  FLAG filename <Enter>

If it is flagged "non-shareable," try again at a later time, when the file is not in use.

.... I can't see a directory?

o You may not have enough rights to that directory. Type

RIGHTS <Enter>

o The directory attribute may be set to "Hidden" or "System." Type

FLAG filename <Enter>

o The directory may have set disk space limitations. To view the directory restrictions, type

DSPACE <Enter>

o The directory may have been deleted. Ask your supervisor.

PRINTING

Printing from a network workstation is similar to printing from a stand alone workstation. When you send a print job to a network printer, however, the job is routed first through the file server and then delivered to the printer by the print server.

When a print job leaves the workstation, it is stored temporarily in a print queue on the file server. This queue, which is a subdirectory on the file server, stores the print job until the print server can deliver it to the printer. When the printer is ready to service the job, the print server moves it from the queue to the printer.

Permanently Set Up Workstation Printing

If you want to print from a non-NetWare-compatible application or from the screen, you need to route print files from your local printer port (LPT1) to a file server queue.

1. Enter the SYSCON utility.

2. Select "User Information" from SYSCON's main menu.

3. Select your username.

4. Select "Login Script."

5. Insert the following command into the login script:

#CAPTURE Q=queuename TI=5

6. Exit SYSCON, saving changes when prompted.

7. Log back in to or reboot your workstation to allow the CAPTURE command to take effect.

Print Screens Using CAPTURE

Before you start printing screens using CAPTURE, you need to set the CAPTURE parameters in your login script. See "Permanently Set Up Workstation Printing" on the previous page. Also, your supervisor needs to set up a default queue.

1. At the command line, type

CAPTURE <Enter>

You can include any of the CAPTURE options except Show. Some of the most common CAPTURE options are the following:

L=n
Indicates which of your workstation's LPT ports (local parallel printing ports) to capture. Replace "n" with 1, 2, or 3. Default:

^S^Q L=LPT1

Q=queuename
Indicates the queue the print job should be sent to. If multiple queues are mapped to a printer, you must include this option. Replace "queuename" with the name of the queue.

TI=n
Indicates the number of seconds between the last time the application writes to the file and the time it releases the file to the queue. Include this option if you want to print from an application without exiting the application. Replace "n" with a number of seconds (1-1000). Default: TI=O (Timeout disabled)

2. Access the application containing the screen you want to print.

3. Press <Shift><Print Screen>.

4. If you want to print more screens, repeat steps 2 and 3.

5. When you have selected the screens you want printed, return to the DOS prompt and type

ENDCAP <Enter>

ENDCAP sends your print job to the default print queue of your default file server, and then the job is printed. ENDCAP also ends the capture of your LPT port.

Note: Your workstation might hang if you press the <Shift><Print Screen> keys when none of your LPT ports are captured and no local printers are attached to your workstation. To prevent this, ask your supervisor to include the following line in the SHELL.DFG file on your workstation boot disk.

LOCAL PRINTERS = 0

List the Jobs in a Queue

A queue is a special directory where print files are stored while waiting for printer services. To see which jobs are waiting in a queue to be printed, complete the following steps:

1. Type

PCONSOLE <Enter>

2. Select your file server (if other than your current file server).

3. Select "Print Queue Information" from the "Available Options" menu.

4. Select the print queue whose print job you want to view. If you don't know the name of the print queue, ask your supervisor.

5. Select "Current Print Job Entries" from the "Print Queue Information" list. The print job entries are displayed.

Delete Your Print Job from a Queue

You can cancel your print job by deleting it from the print queue (even after the job has started printing). You can delete a print job only if you are the owner of the job or if you are the print queue operator.

To delete your print job, complete the following steps:

1. Type

PCONSOLE <Enter>

2. Select "Print Queue Information" from the "Available Options" menu.

3. Select the print queue whose entries you want to view. The "Print Queue Information" list is displayed.

4. Select "Current Print Job Entries."

5. Highlight the print job entry and press <Delete>.

6. Select "Yes" at the confirmation box.

What If...

.... I send commands to print a screen, but it doesn't print?

Did you include the CAPTURE command in your login script? See a previous section called "Permanently Set Up Workstation Printing."

.... The application I'm using says that the print job was sent, but it doesn't print out?

- Did you use CAPTURE to redirect output to a print queue first?

- Are the LPT ports captured? Type

  CAPTURE SH <Enter>

- Check PCONSOLE and find the appropriate queue. If the queue has a long list of jobs and none are marked "active," see your print server operator. If your job isn't in the queue, the application is not set up properly; check with the applications expert.

COMMON ERROR MESSAGES

Error messages point to a software or hardware error that doesn't allow further processing. An explanation of the nature of the message and a recommended course of action follow each message listed below.

"Access denied"

Explanation 1

This message indicates one of the following:

- You entered your username, your password, or both incorrectly.
- You tried to log in to a file server on which you are not defined as a user.

Action 1

Try to log in again and make sure you type the username and password correctly. Make sure you are logging in to a file server on which you are defined as a user or as a member of a group. You can log in to most file servers as GUEST because user GUEST seldom requires a password.

Explanation 2

You tried to copy, delete, rename, or modify the file attributes of a file for which you lack rights.

Action 2

Find out about your rights to this file by typing

RIGHTS filename <Enter>

or by asking your supervisor.

"A File Server could not be found"

Explanation

The shell tried to build a connection with the network, but no file server responded to the request in the given time limit.

Action

Check the cable connection and make sure at least one active file server exists on the network. Also ask your supervisor to make sure the IPX file and the network board have the same configuration.

"Message NOT sent to <servername>/<username> (station number)"

Explanation

If a number of messages have been sent to the user or group and have not been cleared, either of the following may be true:

- The workstation's buffer for incoming messages may be full.
- The message was not sent to the user or group because the user or group used the CASTOFF utility.

Action

Send the message later, or try another method of communication.

"Network Error <cause> during <operation>. File = <drive>:<filename> Abort, Retry or Fail?" (or "Abort, Retry?")

Explanation 1

The shell called a function call or a DOS interrupt, but the specified operation could not be performed. The <drive>:<filename> specify the drive and filename on which the error condition occurred.

Action 1

Press the R key to retry the operation and, if necessary, repeat this several times. If the problem persists, ask your supervisor or look up the specific message in NetWare v3.11 System Messages.

Explanation 2

Your file server may be down.

Action 2

Press the A key to abort the operation, and then try to connect to the file server again. If this attempt fails, contact your supervisor.

"Password has expired"

Explanation

This message indicates your password has expired.

The network supervisor can require users to periodically change their passwords on the file server to protect the file server from access by unauthorized persons. The network supervisor can also assign a number of grace logins during which users can still use their old passwords (after they have expired) before having to create new passwords.

Action

Use the SETPASS command to change your password. If you use the old password during your remaining grace logins, be sure to change it before you run out of grace logins, or else your network supervisor has to change it for you.

"Password has expired and grace period has also expired."

Explanation

This message indicates that your user account is locked because your password has expired and you have used all your grace logins.

After your password expires, you may have a number of grace logins during which you can still use your old password. If you do not change your password before your grace logins are used, you are denied access.

Action

Since you have run out of grace logins, you cannot access your account until your network supervisor or manager assigns you a new password.

"Server <servername> not found"

Explanation

This message indicates that you tried to attach to the file server <servername>, but the file server did not respond for one of the following reasons:

- You mistyped the name of the file server.
- You specified a file server not cabled to your network.
- You specified a file server that is down for system maintenance.

Action

- Type the file server name correctly.

- Use the SLIST command to list all the available file servers.

- If the file server is down for maintenance, try the command later when the file server has been brought back up.

If you still have problems, ask your network supervisor for help.

"Unable to attach to server <servername>"

Explanation

This message indicates one of the following:

- You mistyped the name of the file server.
- You specified a file server not cabled to your network.
- You specified a file server that is down for system maintenance.

Action

- Type the file server name correctly.

- Use the SLIST command to list all available file servers.

- If the file server is down for maintenance, try the command later when the file server has been brought back up.

If you still have problems, ask your network supervisor for help.

"User <fileserver>/<username> not found"

Explanation

This message indicates that you either specified a user who does not exist on <fileserver> or mistyped the user's name.

Action

- Make sure you have typed the user's name correctly.
- If you are not certain which users are established on the file server, use the SYSCON utility to view the list of network users.
- You can also use the USERLIST command to view a list of currently attached users.

(----------)

One of the most useful tools that any Novell Network user can have is access to Netwire on Compuserve. Netwire is a forum that contains messages, files, and access to Novell product information firsthand. You can submit questions to Novell technicians and hundreds of other Novell users. A must for any Netware user.

Another handy tool for those that do have access is the SALVAGE program. SALVAGE will let you undelete files throughout the system unless the directory is marked to be purged. PURGE is nice too because it will allow you to completely erase any files you created or copied. To use purge and or salvage make sure you are mapped to the public directory and execute them from any DOS prompt.

(----------)

As far as dialing up a Novell Network the means are unlimited. Some have very tight security systems that only let users with certain hardware dial-in and others limit the usernames that are allowed dial-in access.

==Phrack Inc.==

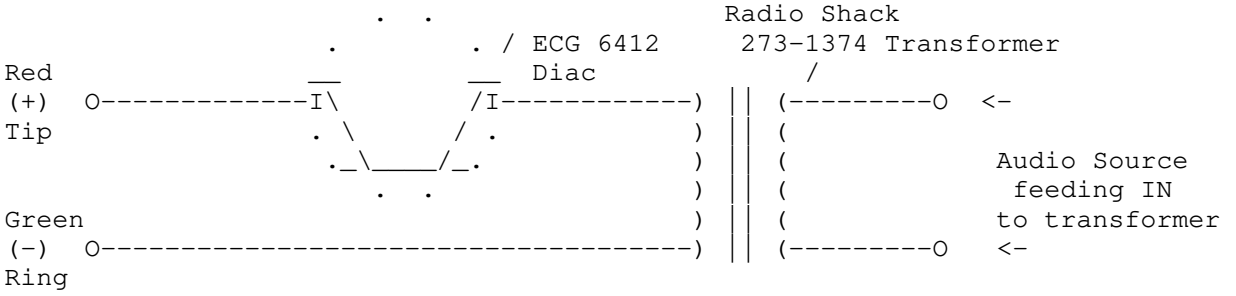
Volume Three, Issue Thirty-five, File 9 of 13

```
          //////////    ////////////////////////////////////
         //  C   //    //                                  //
        //  r   //    //  A U T O - A N S W E R   I T !   //
       //  e   //    //                                  //
      //  a   //    ////////////////////////////////////
     //  t   //
    //  e   ////////////////////////////////////////////
   //  d     B y :     T w i s t e d   P a i r        //
  ////////////////////////////////////////////////////
```

Many times I've wanted to be able to start and/or listen to devices at my home when I'm somewhere else. I've developed the following circuits to do this for me. The circuits have all kinds of uses. I'll let your mind ponder the endless fun activities you can have. Some of the things I have used them for are monitoring my own house, tape record my friends for fun without their knowledge, or listen to a radio station when you're out of town, etc.

///// Automatically Answer a Phone /////

This has got to be the best way to automatically answer the phone. With just 2 parts, we can couple an audio source into a phone line. The cost will be less than $5 no matter where you get the parts!

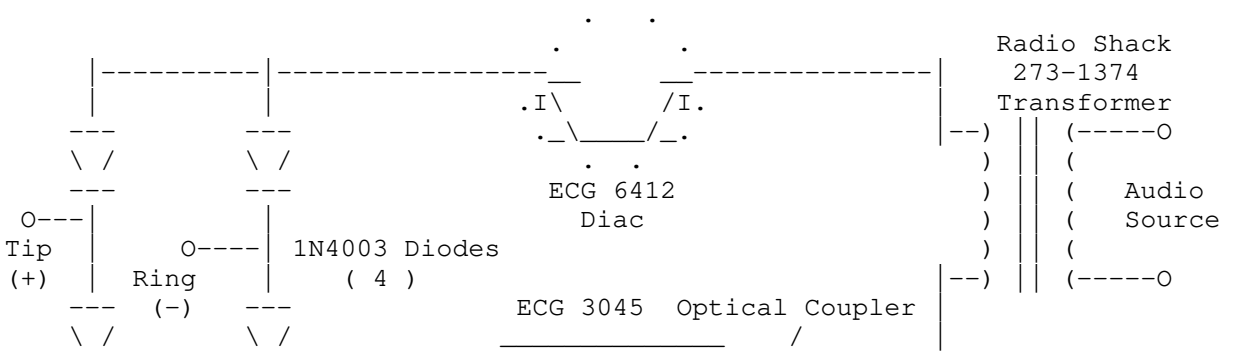


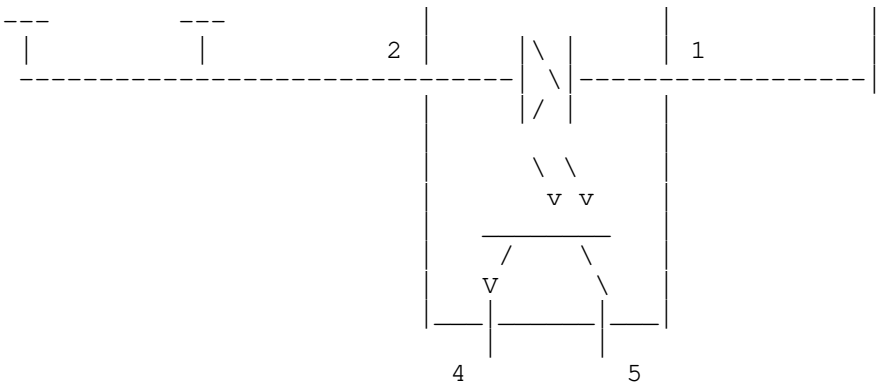
The "Diac" or "Bilateral Trigger Diode" looks like an open circuit until a voltage of either polarity is applied that is above its threshold of 63 Volts. (plus or minus 7 Volts) When this voltage is exceeded, like when the line rings, the device acts as a switch and goes into conduction. This "answers" the phone and holds the line through the transformer, which couples the audio to the line.

When the caller hangs up, most telephone companies provide a momentary reversal of Tip and Ring which causes the Diac to stop conducting and release the line.

///// Another Way to Automatically Answer /////

For those who want to really play with this circuit, I suggest the following additions. I have added a bridge rectifier and an optical coupler to the circuit. The bridge just makes sure that the LED inside the optical coupler gets the proper polarity. If you are careful to observe polarity when connecting to Ma Bell, you can leave out the diodes and save a little money.





Pins 4 and 5 on the optical coupler can be wired to remotely start a device upon answering the line. An example would be a tape machine or battery-powered bugging amplifier. Be careful not to connect anything over 25 volts to pins 4 and 5 to avoid frying the opto-coupler. Either circuit will accommodate an extra LED that could be used as a status indicator. Just be sure to keep the polarity proper and put it in series with the other components.

The Audio Source can be almost ANYTHING. If you want to hook up a microphone as the Audio Source, connect the microphone to some kind of amplifier first, then to the transformer.

///// An Interesting Catalog to Read Through /////

If you really want to get fancy, you could consider ordering a free catalog from Monroe Electronics. They sell the following products you might wish to play with. Use these as building blocks to make whatever you need...

DTMF Decoders (a) Which provide a momentary or latching relay output for the duration of time the DTMF digit is being pressed. (If you're really obnoxious, you'd use one of these with one of the above circuits. Then you could call and randomly turn things on and off like maybe a TV scrambler/ jammer.)

(b) Which can accept multiple digits and be programmed for a momentary or latching relay output. (Use one of these to make a DTMF combination lock for your BBS. Or use as a call screener, i.e. only the correct DTMF sequence could make your phone actually ring)

(c) Which can control access by a 4 digit code to latch a relay, then a single digit to unlatch it. (A little bit more sophisticated than (b) above.

DTMF Encoders Which can convert BCD to DTMF tones. Crystal-controlled, of course. 600-ohm audio output. (Use one of these to convert your computer's output into ANY DTMF tones of your choosing. You'd be able to choose the duration as well! Then this circuit would couple your evil DTMF into the phone line)

Audio Detectors Detect BUSY and DIAL TONE and operate a relay. (Useful when making scanning hardware/software applications)

Audio Generators Generate Ring Tone, Dial Tone, Busy Tone, Tone Burst, etc. (Start your own phone company. Fool your friends, trip out the operator)

Dial-up DTMF remote control systems which can be used to control and monitor remote relays and status inputs at unattended sites. They can also provide automatic dialing of stored phone numbers to

report status of inputs, and can make use of an internal timer to execute control commands. (Water strange plants by call-in remote control, check moisture levels, see if a certain mailbox is empty or full, have the mailbox CALL you when something is delivered, etc. Do I have to tell you everything? Just get the catalog!)

Their address is:

MONROE ELECTRONICS, INC.
100 HOUSEL AVENUE
LYNDONVILLE NY 14098
(716) 765-2254

==Phrack Inc.==

Volume Three, Issue Thirty-five, File 10 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN            Issue XXXV / Part One            PWN
PWN                                             PWN
PWN            Compiled by Dispater             PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Welcome to another edition of Phrack World News. Read this issue very carefully because it is full of very important stories about a multitude of different issues. Special thanks goes to Dark OverLord, Stainless Steel Provider, and Private Citizen for their help in preparing this issue.

XMASCON 1991
~~~~~~~~~~~~

NIA Magazine & Phrack Inc. present:

The Second Annual

X M A S C O N

Who: All Hackers, Journalists, Security Personnel, Federal Agents, Lawyers, Authors and Other Interested Parties.

Where: Houston Airport Hilton Inn
500 North Belt East
Houston, Texas 77060
U.S.A.
Tel: (713) 931-0101
Fax: (713) 931-3523

When: Friday December 27 through Sunday December 29, 1991

Yes, ladies and gentlemen, you read it right... Xmascon has returned! This will undoubtedly be the telecom event of the year. Unlike certain conferences in the past, Xmascon 91 has a devoted and dedicated staff who are putting in an unmentionable amount of time to ensure a large, vast and organized collection of some of the most diversified people in the telecommunications world. The event will be open to the public so that anyone may attend and learn more about the different aspects of computer security.

Hotel Information

The Houston Airport Hilton Inn is located about 6 miles from Intercontinental Airport. The Xmascon group room rates are $49.00 plus tax (15%) per night, your choice of either single or double. There are also 7 suites available, the prices of which vary from $140 to $250. You can call the hotel to find out the differences and availability of the suites, and you will also NEED to tell them you are with the Xmascon Conference to receive the reduced room rate, otherwise, you will be paying $69.00. There is no charge for children, regardless of age, when they occupy the same room as their parents. Specially designed rooms for the handicapped are available. The hotel provides free transportation to and from the airport, as well as neighboring Greenspoint Mall, every 30 minutes on the hour, and on call, if needed. There are 2 restaurants in the hotel. The Wicker Works is open until 11:00 pm, and The Forty Love is open 24 Hours. There will also be breakfast, lunch and dinner buffets each day. There is a piano bar, The Cycle Club, as well as a sports bar, Chaps, which features numerous table games, large screen TV, and a disco with a DJ. Within the hotel compound, there are 3 pools, 2 of which are
~~~~~~~~~~~~

indoors, a jacuzzi, a miniature golf course, and a fully equipped health club which features universal weights, a whirlpool and sauna. A car rental agency is located in the hotel lobby, and you can arrange to pick your car up at either the airport or the hotel. Xmascon attendees are entitled to a discounted rate. Contact the hotel for more information.

Xmascon will last 3 days, with the main conference being held on Saturday, December 28, in the Osage meeting room, starting at 12:00 p.m. and continuing on throughout the evening. This year, we have our own complete wing of the hotel, which is housed around a 3,000 square foot atrium ballroom. The wing is completely separated from the rest of the hotel, so we are strongly encouraging people to make their reservations as far in advance as possible to ensure themselves a room within our area.

We are hoping to have a number of people speak on a varied assortment of topics. If you would like to speak, please contact us as soon as possible and let us know who you are, who you represent (if anyone), the topic you wish to speak on, a rough estimate of how long you will need, and whether or not you will be needing any audio-visual aids.

There will be a display case inside the meeting room which will hold items of telecom interest. Specific items that will be available, or that we hope to have, include the first issues of 2600, Tap, Mondo 2000, and other magazines, non-computer related magazines that feature articles of interest, a wide array of boxes, the Quaker Oats 2600 mhz whistle, The Metal AE, etc. We will also have a VCR and monitor set up, so if you have any interesting videos (such as the Unsolved Mysteries show featuring Kevin Poulsen), or if you have anything you think people would enjoy having the chance to see, please let us know ahead of time, and tell us if you will need any help getting it to the conference. If all else fails, just bring it to the con and give it to us when you arrive.

If anyone requires any additional information, needs to ask any questions, wants to RSVP, or would like to be added to the mailing list to receive the Xmascon updates, you may write to either myself (Drunkfux), Judge Dredd, or Lord Macduff via Internet at:

nia@nuchat.sccsi.com

Or via US Mail at:

Hard Data Corporation
ATTN: HoHo
P.O. Box 60695
Airport Mail Facility
Houston, Texas 77205-9998
U.S.A.

We will hopefully have an 800 mailbox before the next update is sent out. If someone cares to donate a decent one, that will stay up throughout the end of the year, please let us know. We should also be listing a few systems as an alternative form of reaching us.

Xmascon 91 will be a priceless learning experience for professionals, and gives journalists a chance to gather information and ideas direct from the source. It is also one of the very few times when all the members of the computer underground can come together for a realistic purpose. We urge people not to miss out on an event of this caliber, which doesn't happen very often. If you've ever wanted to meet some of the most famous people from the hacking community, this may be your one and only chance. Don't wait to read about it in all the magazines, and then wish you had attended, make your plans to be there now! Be a part of our largest and greatest conference ever.

Remember, to make your reservations, call (713) 931-0101 and tell them you're with Xmascon.

In closing... if you miss this one, you're only cheating yourself.

>From Arizona State University State Press
Further Reading: Phrack Issue 34, File 11, "MindRape or MediaRape?"

An Arizona State University (ASU) student is one of seven suspects in a computer fraud scheme that one US West Communications official said could cost the carrier and the phone company as much as $5 billion in one year.

Police in Phoenix, Arizona have seized computer equipment, software, and a list of long distance calling card codes from the home of the unidentified 19-year-old student.

The student is one of seven people -- three in Oregon and one each in Washington, Utah, and Iowa -- singled out as suspects in a month-long investigation of electronic phone fraud conducted by Phoenix police, said Jim Waltman, a fraud manager for US West Communications. The Phoenix man has not been arrested.

The computer "hackers" allegedly used their computers to gain access to secret long distance phone access codes such as the ones found on calling cards, and sold codes to other students for profit.

US West officials told the Associated Press that it is unknown how many local customers have been wrongfully billed for long distance calls on their accounts.

Kevin Robinson, public information sergeant for the Phoenix Police Department, would not comment on the investigation.

Art Carter, dean of Student Life at Arizona State University (ASU), said that if the student is charged, the case will be reviewed under the ASU Code of Conduct and the action taken by the University will be determined at that time.

Mark Knighton, security director for LDL Long Distance, said his company and US West were able to trace calls to several location, including the home of the Phoenix man.

The Phoenix man has not been arrested, authorities said.

Waltman said he was with Phoenix police a week ago when they searched the north Phoenix home and uncovered what turned out to be an inexpensive and relatively simple system for getting free codes.

- -
Editor's Comment by: Dispater

What MindRape has been charged with cannot be determined now. A request must be submitted to Arizona Public Records and be considered for release to the requestor.

Here are some possibly useful numbers:

Arizona Special Investigations Division	(602)542-4853	
County Attorney's Office	(602)262-3411	(Gail Thackeray)
Arizona Republic Newspaper	(602)271-8000	
Phoenix Police Department		
- General Investigations	(602)262-6141	
- Police Information	(602)262-7626	
- Police Records	(602)262-6134	

East Coast LOD Hackers Create Virtual Reality MAELSTROM
~~~~~~

"It's reached the point where hacking is counter-productive."

If the 1980's were the decade that hackers emerged from their relative obscurity as computer oddities, to be transformed in the public's perception as front-page news -- then the 90's are shaping up to be the decade of hacker turned entrepreneur. Lately the notorious hacker group Legion of Doom seems to be a particularly fertile spawning ground for ex-hackers turned young-businessman.
~~~~~~

Two former East-Coast Legion of Doom members, Bruce Fanscher <Dead Lord> and Patrick Krupa <Lord Digital>, have pooled their talents to form a new company in the burgeoning field of Virtual Reality.

The arena of Virtual Reality has often been called technology in search of a purpose and at times resembles nothing more than an interactive movie meets videogame. This chaotic state of affairs has led to a never-never land of incompatible technologies and far-out ideas, that have tremendous potential, but little commercial application at present. Fanscher and Krupa plan to change all that. "VR isn't anything new, it's something we've been living for over half our lives. The only difference is the state of current technology, makes possible an incredible variety of application." said Krupa in an interview. "Right now we're in the ideal position to move forward on ideas we've been working on for years," added Fanscher.

Krupa, who had attained the status of cult figure in the hacker underground prior to his arrest, as chronicled by John Markoff (New York Times) technology columnist, has spent the last several years working in the very lo-tech world of theater, "Basically I was totally burnt out on computers. I mean I don't give a damn if my word processor boots in one second instead of eight, and that's the only place anything was heading for a long time. The NeXT has changed all that and brought to market something truly innovative, although I still don't care too much about technology as anything but a medium through which you can reach people and affect their experiences and perceptions."

No stranger to creative innovation himself, Fanscher, Krupa's longtime compatriot, has spent his share of time in the somewhat murky spotlight of the hacker underground. Musing about his days as a hacker delving into computer systems to see how they worked, Fanscher remarked that:

> "It's reached the point where hacking is counter-productive. You can only take apart things other people have designed and see what makes them work, for so long, before it becomes an exercise in boredom and the time comes to use what you've learned to create something new that nobody has ever seen before. My current interest in other people's systems is zero. It was a useful learning experience for me, but there's no future in it."

This oddly charismatic, dynamic duo is rounded out by Delia Kopold a former actress and theater major who is the architect of the worlds that make MAELSTROM come alive. This initial offering by the collection of talents will be an online system run on the NeXTcube supermicro -- a machine that looks more like a piece of modern art than a computer -- that offers enhanced versions of all the usual amenities like electronic messaging, file transfers, and networking, all revolving around MAELSTROM, a program Fanscher calls, "a real-time virtual interaction simulation engine." MAELSTROM will initially take the form of an extremely detailed fantasy world complete with custom graphic programs that run on MS-DOS, Macintosh and Amiga computers, allowing users to tap into the NeXTcube's system architecture through their home computers connected to telephone lines. "Maelstrom isn't really a fantasy game, it's actually a universal engine comprised of objects that can be accessed by a variety of graphic, sound and data files to create just about any multi-user reality you can dream up," explains Krupa.

The MAELSTROM system is about to go through a short beta-test run in New York City prior to a national ad campaign that will herald its universal accessibility on packet switch. "Our beta system already offers everything that competing services offer, but at a much lower cost -- and we're still adding features. And nothing like Maelstrom has ever existed before, the technology just wasn't there," concludes Fanscher.

2600 Magazine Exposes Security Holes October 18,1991
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by John F. McMullen & Barbara E. McMullen (Newbytes)

Armonk, New York -- Supported by videotape examples, Emmanuel Goldstein, editor and publisher of 2600 Magazine: The Hacker Quarterly, told those in attendance at an October 17th New York City press conference that "the American public is
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

often lulled into a false sense of security; a security that is often not supported by the facts of specific cases."

The videotapes, produced by 2600 and provided to the press show both the intrusion of a Dutch "hacker" in to United States Military computers and what Goldstein alleges is the fallibility of a brand of mechanical, pushbutton locks used by, among others, New York State University sites, Federal Express, United Parcel Service, JFK International Airport, IBM and NASA.

Goldstein told Newsbytes "We invested considerable time and money to wake people up to the fact that we have a false sense of security when it comes not only to computer networks but to physical safety as well."

The tape of the Dutch "hacker" was made by Goldstein while in Europe. and shows the intrusion into a Unites States Army computer system. The intruder was able to set up a fictitious account called "danquayle" and, once into the system, was able to obtain "root" privileges thus giving him total control of the workings of the system.

A portion of this tape had previously been shown with Goldstein's approval on an episode of the Geraldo Rivera television show "Now It Can Be Told". Goldstein told Newsbytes that one^S^Q reason for his release of the entire tape to the press was his feeling that the Rivera episode entitled "The Mad Hacker's Key Party" had distorted the message of the tape -- "This was not a case of a terrorist break-in but was rather simply a demonstration of the lack of security of our systems. To find root accounts with password like "Kuwait" and lack of sophisticated security in our military computers should be of real concern and should not be lost in an exploitation of the 'hacker' issue."

A background paper provided at the conference by 2600 explains the entire intrusion effort in detail and states "The purpose of this demonstration is to show just how easy it really was. Great care was taken to ensure that no damage or alteration of data occurred on this particular system. No military secrets were taken and no files were saved to a disk by the hackers. What is frightening is that nobody knows who else has access to this information or what their motivations might be. This is a warning that cannot be taken lightly."

The second videotape show Goldstein and other 2600 staff opening seemingly at will locks manufactured by Simplex Security Systems. The locks of the mechanical pushbutton combination variety were shown to be installed at the State of New York University at Stony Brook, JFK International Airport and on Federal Express and United Parcel pick-up boxes throughout the New York Metropolitan area.

In the film, Goldstein is shown filling out a Federal Express envelope for delivery to 2600 Magazine and inserting in the Fedex dropbox. He then lifts the weather protection cover on the box's lock and keys a combination that allows him to open the lock and remove his envelope. Scott Skinner, a SUNY student and 2600 staff member told Newsbytes that it had actually taken the staff 10 minutes to determine the proper code combinations to open the lock.

Skinner explained, "While Simplex prefers people to think that there is an endless number of permutations to the lock, there are actually only 1,085. In most cases, even this number is greatly reduced -- if one knows that only three buttons are being used, it reduces the possibilities to 135. Additionally, we found that, once we had the combination to one Federal Express dropbox, it worked in every other one that we tried in the New York area."

Goldstein told Newsbytes "When we contacted Simplex, they first denied that the locks were unsafe and then said that the permutations were much greater. After some discussion, they admitted that the 1,085 figure was correct but said that it would take a person with a complete listing of the combinations over four hours to try them all. Our experience obviously shows that they may be opened in a much shorter time than that."

Goldstein also pointed out that, "although a $5 Master combination lock may be broken by a crowbar, it is a much more secure combination device. It has 64,000 combinations compared to the 1,085 with the Simplex."

Goldstein continued, "One of the real problems is that, should a person have the misfortune to be robbed, entry due to a failure of the Simplex lock gives no evidence of a forcible break-in and police and insurance companies often put the blame on the homeowner or office manager for 'giving away the combination.' It really can create a problem."

Skinner told Newsbytes "I'm really concerned about t^Shis. I'm a student at SUNY, Stony Brook and all our dormitories use these locks as the only means of security. I've shown the problem to Scott Law who is responsible for residence security but he has discounted the problem and said that the locks were installed at the recommendation of the campus locksmith. The locksmith, Garry Lenox contradicts Law and says that he recommended against these locks years ago and said that they were not secure for dormitory use." Skinner said that he will write an article for the college newspaper in an attempt to raise consciousness about this problem.

Goldstein also said that he intends to publish the list of valid combinations in an up-coming iss^Que of 2600 to demonstrate to the public the problems with the lock. He further said that he will raise the issue on his weekly radio show, "Off The Hook", heard on New York's WBAI-FM.

In response to a Newsbytes question concerning how the 2600 staff happened to become involved in a problem with locks, Goldstein said, "We're hackers and when we see something with buttons on it, whether it's a computer or not, we tend to try it. While the average person tends to accept that things are secure just because he is told that they are, hackers will usually try them out. It's because of this 'trying out' that we can point out the problems with both the US military computer security and this lock -- and we feel that, in both cases, we have performed a service. People should be aware when they are at risk so that they may take action to correct it."

Questions Exist On Israeli Break-In Of US Systems September 10,1991
~~~~~~

by Barbara E. McMullen & John F. McMullen (Newsbytes)

NEW YORK -- Amidst reports of the intrusion by an Israeli national into United States military computer systems, there have been conflicting accounts of the extent and nature of the invasion.

According to wire services, Deri Schriebman, an 18 year-old graduate of Israel's Technion Institute and a native of the northern Israeli city of Carmiel, was arrested by Israeli police for allegedly breaking into US military computers and commercial credit card systems. Israeli spokes person Eitan Raz, commenting on the equipment found at Schriebman's home for allegedly making free overseas phone calls, was quoted as saying "This was a very complex system. It was the first time such technology was discovered in Israel."

Newsbytes has ben able to confirm with sources that a trail of credit card fraud in the United States and Canada led investigators to Schriebman but has not been able to confirm that Schriebman, as reported in Israeli press, was able to access classified Pentagon information concerning Patriot missiles during the recent Gulf War. A US government investigative official told Newsbytes that, while his agency has formally requested documentation of the events from the Israeli police, that there seems to have been no contact to date between any US service and the Israeli investigators.

Other investigative sources have told Newsbytes that the investigation into Schriebman's activities began in May 1991 when two Quebec teenagers were arrested for purchasing goods through the use of stolen credit card identification. The teenagers told Canadian authorities that they had received the information from a source in Carmiel, Israel and the authorities notified Israeli police. According to the Israeli reports, Schriebman admitted the intrusion into credit card files and the subsequent dissemination of codes but denied making any use of the information. He was quoted as saying that his cracking into the systems was done only out of curiosity.

A "hacker" source told Newsbytes that underground bulletin boards utilized for the exchange of such credit information are often frequented by foreign nationals. He said that the most frequent visitors come from Australia, Israel
~~~~~~

and Germany and that many of the Israelis identify themselves as have a connection with the Technion Institute.

==Phrack Inc.==

Volume Three, Issue Thirty-five, File 11 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN            Issue XXXV / Part Two            PWN
PWN                                             PWN
PWN            Compiled by Dispater             PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Justice Revs Up Battle On Computer Crime — October 7, 1991

by Michael Alexander (ComputerWorld)(Page 4)

Washington D.C. -- The nation's top federal computer crime law enforcers announced plans to escalate the war on computer crime.

At the federal government's 14th National Computer Security Conference held in Washington D.C., officials at the U.S. Department of Justice said the department is launching a computer crime unit that will be charged with prosecuting crimes and pushing for stiffer penalties for convicted computer outlaws.

"Computer crime is on the rise, and the Justice Department is taking this area very seriously -- as well as the FBI, U.S. Secret Service, and the military," said Mary Spearing, chief of general litigation and legal advice in the criminal division at the Justice Department.

The new crime unit will also advocate closing loopholes in the government's computer crime statute. The Computer Fraud & Abuse Act of 1986 "is outmoded and outdated," said Scott Charney, a computer crime prosecutor and chief of the new computer crime unit.

The Justice Department wants to amend the law with a provision that would make inserting a virus or worm into a computer system a crime, Charney said.

Those convicted of computer crimes will more often be sentenced according to federal guidelines rather than on recommendation of prosecutors, who may ask for lighter penalties, said Mark Rasch, the government's attorney who prosecuted Robert Morris in the infamous Internet worm case.

A new Justice Department policy now mandates that all defendants will be treated equally, without regard for personal history or other factors that might mitigate stiffer sentences, Rasch said.

"The penalties for computer crime will become increasingly more severe," predicted Kent Alexander, assistant U.S. attorney in Atlanta <prosecutor of the Atlanta members of the Legion of Doom>. "In five years, they are going to look back and think a year in jail was a light sentence."

The FBI is "staffing up to address concerns about computer crimes" and increasing its training efforts, said Mike Gibbons, FBI supervisory special agent <who worked on both the Morris and the Clifford Stoll KGB hackers cases>.

- -

Supreme Court Refuses Morris Appeal — October 14, 1991

by Michael Alexander (ComputerWorld)(Page 14)

Washington, D.C. -- The U.S. Supreme Court refused without comment to hear Robert T. Morris' appeal last week, ending a legal journey that began nearly three years ago when he injected a worm into the Internet network.

While the trek is over for Morris, there remain serious questions about the

Computer Fraud and Abuse Act of 1986, the statute under which he was prosecuted.

The refusal to review the Morris case leave intact a "bone breaker" law that could transform otherwise law-abiding computer users in felons and inhibit the creative uses of computer technology according to Thomas Viles, an attorney at the Silverglate & Good law firm in Boston. Viles authored a friend of the court brief in the Morris appeal on behalf of the Electronic Frontier Foundation.

Some legal experts worry that computer users who enter a computer system without authorization, either unwittingly or with the intention of merely looking around, could be given penalties that are overly severe.

"A single computer entry is of an entirely different order than the destruction of data or the intentional alteration of data, just as simple trespass is pretty minor stuff compared to vandalism or burglary," Viles said. "Now if people whose livelihoods depend on computers get into somebody else's computer without authorization, they could be in Leavenworth for five years."

The Morris appeal boiled down to the critical question of whether he intended to cause the harm that ensued after he set loose his ill-conceived computer program on November 2, 1988.

In 1990, a federal judge in Syracuse, New York ruled that it was not necessary for the government to prove that Morris intended to cause harm, only that Morris intended to access computers with authorization or to exceed authorization that he may have had. Earlier this year a federal appeals court upheld Morris' May 1990 conviction under which he received three years probation, a $10,000 fine, and 400 hours of community service.

That affirmation goes against the widely accepted tenet that an injury can amount to a crime only when deliberately intended, Viles said. "The law distinguishes, say, between murder and manslaughter. You can't be guilty of murder if the killing was utterly accidental and unintended."

A General Accounting Office (GAO) report released in 1989 noted other flaws in the federal computer statute. While the law makes it a felony to access a computer without authorization, the law does not define what is meant by "access" or "authorization," the GAO reported.

UPDATING THE LAW

U.S. Department of Justice Officials recently acknowledged that the Computer Fraud and Abuse Act is outdated and noted that it should be refined <see Justice Revs Up Battle On Computer Crime (the previous article)>. Scott Charney, chief of the Justice Department's newly created computer crime unit, said the department will lobby to fortify the law with provisions that would outlaw releasing viruses and worms and make it a felony to access a computer without authorization and cause damage through reckless behavior.

Trespassing into a computer is more serious than it may appear at first glance, Charney said. "It is not easy to determine what happened, whether there was damage, how safe the system now is or what the intruder's motives were."

Some legal experts said they believe the law is already overly broad and do not advocate expanding it with new provisions. "It is a far-reaching law, whose boundaries are still not known," said Marc Rotenberg, an attorney and director of the Washington, D.C. office of Computer Professionals for Social Responsibility. "The way I read the law is, the Justice Department has everything it needs and more," he said. "After the Morris decisions, if you sneeze, you could be indicted."

The Morris case pointed out deficiencies in the law that have resulted from technology's rapid advance, said Thomas Guidoboni, the Washington, D.C.-based attorney who defended Morris.

Neither Guidoboni nor Morris were surprised by the Supreme Court's refusal to hear his appeal, according to Guidoboni. "Robert's case had a particular

problem in that it was the first one involving the 1986 act. They like to take cases after the circuit courts had had some chance to play with them and see if there is a disagreement."

Morris is working as a computer programmer in Cambridge, Massachusetts for a company that "knows who he is and what he's done," Guidoboni said. He declined to identify the company.

<Editor's Note: Morris was actually the SECOND person to be tried under the 1986 Computer Fraud and Abuse Act. The first person was Herbert Zinn, Jr. a/k/a Shadow Hawk of Chicago, Illinois, who was convicted in 1989 in a prosecution led by William Cook, a now former assistant U.S. attorney whose name most of you should recognize from the Craig Neidorf (Knight Lightning) and Lynn Doucette (Kyrie) cases.

Zinn was tried as a minor and therefore in a bench trial before a sole judge. Morris is the first person to be tried under the Act in front of a jury. Zinn's conviction earned him 10 months in a juveniles prison facility in South Dakota, a fine of $10,000, and an additional 2 1/2 years of probation that began after his prison term ended.

For additional information about the Shadow Hawk case, please read "Shadow Hawk Gets Prison Term," which appeared in Phrack World News, Issue 24, Part 2.

- -

Justice Unit Spurred On By Cross-Border Hackers October 21, 1991
~~~~~~

by Michael Alexander (ComputerWorld)(Page 6)

Washington D.C. -- The U.S. Department of Justice's formal launch of a computer crime unit was prompted largely by an alarming rise in computer invasions that traverse geographic and jurisdictional boundaries, according to a top Justice Department official.

Robert Mueller III, assistant U.S. attorney general, said the Justice Department needs to be better prepared to prosecute computer criminals. he is one of the architects of a five-person unit recently established by the justice department expressly to combat computer crime.

"One of the principal functions of the unit is to anticipate areas where federal, state, and local law enforcement will have to expend resources in the future," Mueller said. "One that comes immediately to our attention is crime related to computers used as a target as in The Cuckoo's Egg." He was referring to author Clifford Stoll's account of how he tracked West German hackers who penetrated U.S. computers for the KGB in exchange for cash and cocaine.

Increasingly, computer crimes cut across state and international boundaries, making them difficult to investigate because of jurisdictional limits and differing laws, Mueller said. The computer crime unit will be charged with coordinating the efforts of U.S. attorneys general nationwide during investigations of crimes that may have been committed by individuals in several states.

One of the unit's first assignments will be to take a pivotal role in OPERATION SUN-DEVIL, last year's much-publicized roundup of computer hackers in several states. That investigation is still under way, although no arrests have resulted, Justice Department officials said.

The unit will coordinate efforts with foreign law enforcers to prosecute hackers who enter U.S. computer systems from abroad while also working to promote greater cooperation in prosecuting computer criminals according to Mueller.

The unit will also assist in investigations when computers are used as a tool of a crime -- for example, when a computer is used to divert electronically transferred funds -- and when computers are incidental to a crime, such as when a money launderer uses a computer to store records of illegal activities,
~~~~~~

Mueller said.

"There have been many publicized cases involving people illegally accessing computers, from phone phreaks to hackers trying to take military information," said Scott Charney, chief of the new computer unit. "Those cases have high importance to us because any time that computers are the target of an offense, the social cost is very high. If you bring down the Internet and cripple 6,000 machines and inconvenience thousands of users, there is a high social cost to that type of activity."

The computer crime unit will also work to promote closer cooperation between the Justice Department and businesses that have been the victims of computer crime, Charney said.

Law enforcers are better trained and more knowledgeable in investigating and prosecuting computer crimes, Charney said. "Businesses need not be concerned that we are going to come in, remove all of their computers, and shut their businesses down. FBI and Secret Service agents can go in and talk to the victim in a language they understand and get the information they need with a minimum amount of intrusion."

<Editor's Note: "Businesses need not be concerned that we are going to come in, remove all of their computers, and shut their businesses down." Excuse me, but I think STEVE JACKSON GAMES in Austin, Texas might disagree with that statement. Mr. Charney -- Perhaps you should issue an apology!>

- -

V I E W P O I N T

Let's Look Before We Legislate October 21, 1991
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Marc Rotenberg (ComputerWorld)(Page 25)

"Laws Are Adequate To Handle Computer Crime -- 'Net Police' Not Needed"

The U.S. Department of Justice is now circulating a proposal to expand the reach of federal computer crime law. On first pass, this might seem a sensible response to concerns about computer crime. The reality, however, it that the current federal law is more than adequate and the Justice Department proposal is poorly conceived.

The Justice Department proposal will give federal agencies broad authority to investigate computer crime, allowing them to intercede in any situations involving a computer hooked to a network.

Creating a worm or virus could become a felony act, no questions asked. Espionage laws would be broadened and intent requirements would be lowered. Certain procedural safeguards would be removed from existing law.

CURRENT LAW ADEQUATE

Taken as a whole, the proposal will make it possible for the federal government to prosecute many more computer crimes, but the question is whether this additional authority will improve computer security. Between the current federal statute, the Morris decision, and the sentencing guidelines, federal prosecutors already have more than enough tools to prosecute computer crime.

Under the Computer Fraud & Abuse Act, passed in 1984 and amended in 1986, the unauthorized use of a computer system is a felony. Though the act does not define what "authorization" is or how it is obtained, a person found guilty faces up to five years in jail and fines of $250,000. It is a far-reaching law whose boundaries are still not known.

THE MORRIS FACTOR

The Morris case strengthened the hand of federal prosecutors still further. The judge ruled that it was not necessary for the government to prove that Morris intended the harm that resulted when the worm was released, only that he intended unauthorized use when he did what he did.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

>From a common law viewpoint, that's a surprising result. Traditional criminal law distinguishes between trespass, burglary, and arson. In trespass, which is a misdemeanor, the offense is entering onto someone else's property. Burglary is simple theft and arson is destruction. To punish a trespasser as an arsonist is to presume an intent that may not exist.

A federal appeals court affirmed the Morris decision, and the Supreme Court has refused to hear his appeal, so now the computer crime statute is essentially a trip-wire law. The government only has to show that the entry was unauthorized -- not that any resulting harm was intentional.

There is another aspect of the Morris case that should be clearly understood. Some people were surprised that Morris served no time and jumped to the conclusion that sentencing provisions for this type of offense were insufficient. In fact, under the existing federal sentencing guidelines, Morris could easily have received two years in jail. The judge in Syracuse, New York, considered that Morris was a first-time offender, had no criminal record, was unlikely to commit a crime in the future, and, not unreasonably, decided that community service and a stiff fine were appropriate.

To "depart" as the judge did from the recommended sentence was unusual. Most judges follow the guidelines and many depart upwards.

That said, if the Department of Justice persists in its efforts, there are at least three other issues that should be explored.

UNANSWERED QUESTIONS

First there is the question of whether it is sensible to expand the authority of federal agents at the expense of local police and state government. If theft from a cash register is routinely prosecuted by local police, why should the FBI be called in if the cash register is a computer?

What will happen to the ability of state government to tailor their laws to their particular needs? Do we really want "Net Police"?

There is also the need to explore the government's performance in recent computer crime investigations before granting new powers. For example, the botch Operation Sun-Devil raid, which involved almost one quarter of all Secret Service agents, resulted in hardly a conviction. (A good cop could have done better in a night's work.)

In a related investigation, Steve Jackson, the operator of a game business in Texas was nearly forced out of business by a poorly conceived raid.

In fact, documents just released to Computer Professionals for Social Responsibility by the Secret Service under the Freedom of Information Act raise substantial questions about the conduct, scope, and purpose of Operation Sun-Devil investigations. They reveal, for example, that the Secret Service monitored and downloaded information from a variety of on-line newsletters and conferences.

A congressional hearing to assess Operation Sun-Devil would certainly be in order before granting federal officials new powers.

PROTECTION OF RIGHTS

Finally we should not rush to create new criminal sanctions without fully recognizing the important civil liberties interests in information technologies, such as the rights of privacy and free expression. There are, for example, laws that recognize a special First Amendment interest in newsroom searches.

But no case has yet made clear the important principle that similar protections should be extended to computer bulletin boards. New criminal sanctions without necessary procedural safeguards throws off an important balance in the criminal justice system.

Expanding the reach of federal law might sound good to many people who are concerned about computer crime, but broadening criminal law is always

double-edged. Could you prove to a court that you have never used a computer in an "unauthorized" manner?

<Editor's Note: Marc Rotenberg is the Director of the Washington office of Computer Professionals for Social Responsibility and he has testified in both the House of Representatives and the Senate on computer crime legislation.>

PWN Quicknotes
~~~~~~~~~~~~~~

1. Operation Sun-Devil Scope Emerges (ComputerWorld, 10/14/91, page 119)
--

The Computer Professionals for Social Responsibility (CPSR), an advocacy group, received more than 2,400 documents from the U.S. Secret Service under the Freedom of Information Act. The documents relate to Operation Sun-Devil, last year's nationwide dragnet through the hacker underground. An early look at the documents reveals that the scope of the operation was considerably broader than the U.S. Secret Service has admitted, said Marc Rotenberg, director of CPSR's Washington, D.C. office. CPSR will soon hold a press conference to discuss the findings, he added.

- -

2. 6 Police Employees Probed for Wiretaps (Washington Post/AP, 10/24/91, page A4) -- Jefferson City, Missouri -- Missouri's Highway Patrol is investigating six employees implicated in three illegal wiretaps, officials said.

The wiretaps were "stupid" and were intended to "gain personal information in an effort to supervise subordinates," said Colonel C.E. 'Mel' Fisher, the patrol's chief.

Fisher said that six employees are on administrative leave without pay after a two-month internal investigation confirmed conversations were recorded at patrol headquarters and at a troop office in Kirkwood, Missouri.

Fisher did not identify the employees, who face hearings that could lead to possible penalties ranging from a written reprimand to dismissal. It is a federal felony to conduct an illegal wiretap. He said the FBI investigated the wiretaps.

Major Bobby G. Gibson, chief of the patrol's Criminal Investigation Bureau, in which two of the wiretaps occurred, committed suicide on October 9, 1991. He was among five defendants in a $7 million federal lawsuit filed recently by a black patrolman, Corporal Oliver Dixon, who alleged he had been wiretapped and denied promotions because of his race. All of the defendants, including Fisher, are white.

- -

3. Patrick Townson, the moderator of the Internet's Telecom Digest (comp.dcom.telecom) was less than pleased when an unknown person placed Phrack 34 into alt.dcom.telecom. Townson consistently preaches about the evils of hacking, but we know that he did not learn everything he knows about telecommunications in the classroom. See you after World War Three Pat! We know who you are, we know who you WERE and we know what crimes you have committed in the realm of telecommunications. We're anxious to talk some more with you about this in the near future.

See below:

"I assume you saw the stuff which was left in alt.dcom.telecom today: A whole series of messages telling how to break into several voicemail systems; how to break into the MILNET; a program designed to discover passwords; and other obnoxious files. All of them were left by the same anonymous user at the same non-existent site. Siemens Medical Systems (one of the victims in the theft-of-voicemail-services tutorial in alt.dcom.telecom today) has been notified that their 800 number link to voicemail is now under attack, and given the box number involved. Like cockroaches, you can stomp on those people all you like; they seem to survive. One person has said in the event of WW-3, the only species to
~~~~~~~~~~~~~~

survive will be the cockroaches and the hackerphreaks. Good socially responsible computing, that's what it is! PAT"

---

4. The existence of back issues of Phrack Inc. found in a user's home directory was enough for a system administrator at Tufts University in Massachusetts to revoke a users account. Michael Godwin, an attorney for the Electronic Frontier Foundation went to bat for this individual and succeeded in restoring the user's account. The incident prompted the following response by a reader of Telecom Digest (comp.dcom.telecom):

   On Oct 19 at 11:51, TELECOM Moderator writes:

   > Is it easier and more pragmatic for a
   > system administrator to answer to his/her superiors regarding files at
   > the site which harassed or defrauded some third party (ie. telco) or
   > to simply remove the files and/or discontinue the feed" PAT]

   But this requires a judgment call on the part of the system administrator, does it not? Most of the system administrators that I know are too busy administering the system to worry about this file or that feed, except perhaps as it relates to traffic volume or disk space consumed.

   Will we ever get to the point where those in charge will stop dreaming of practicing mind control? I am so sick of those who are paranoid that someone somewhere may actually express an uncontrolled thought or idea to someone else.

   Ah, the advantages of owning one's own UUCP site ...

---

5. The National Public Network Begins Now. You Can Help Build it.

   Telecommunications in the United States is at a crossroads. With the Regional Bell Operating Companies now free to provide content, the shape of the information networking is about to be irrevocably altered. But will that network be the open, accessible, affordable network that the American public needs? You can help decide this question.

   The Electronic Frontier Foundation recently presented a plan to Congress calling for the immediate deployment of a national network based on existing ISDN technology, accessible to anyone with a telephone connection, and priced like local voice service. We believe deployment of such a platform will spur the development of innovative new information services, and maximize freedom, competitiveness, and civil liberties throughout the nation.

   The EFF is testifying before Congress and the FCC; making presentations to public utility commissions from Massachusetts to California; and meeting with representatives from telephone companies, publishers, consumer advocates, and other stakeholders in the telecommunications policy debate.

   The EFF believes that participants on the Internet, as pioneers on the electronic frontier, need to have their voices heard at this critical moment.

   To automatically receive a description of the platform and details, send mail to archive-server@eff.org, with the following line:

   send documents open-platform-overview

   or send mail to eff@eff.org.

---

6. The September/October 1991 issue of The Humanist has a cover story regarding Cyberspace, rights and freedoms on nets such as Usenet, and makes reference to Craig Neidorf, Jolnet, Prodigy and other matters.

---

7. A Virginia Beach restaurateur plead guilty to illegally taping a telephone call by Governor L. Douglas Wilder and said he arranged for the tape to be delivered to the staff of Senator Charles Robb, D-Va., hoping it would be damaging to Wilder and politically helpful to Robb.

   Robert Dunnington, a onetime social companion of Robb's, admitted in federal court that he intercepted a 1988 car phone call by then-Lt. Governor Wilder as part of his hobby of monitoring and recording cellular calls.

   From February 1988 to October 1990, Dunnington overheard and taped hundreds of calls and, his attorney said, it was "just happenstance" that Wilder's call was picked up. (Washington Post)

---

8. A Federal District Judge in New York ruled that a computer-network company is not legally liable for the contents of information it disseminates. While the decision could be influential because it tackles free speech on an electronic network, it is not clear how the ruling would affect bulletin boards ^S^Qon which users add comments. The decision concerned an electronic gossip column carried by CompuServe. In the decision, the judge stated "CompuServe has no more editorial control over such a publication than does a public library, bookstore or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so." (Wall Street Journal, October 31, 1991)

==Phrack Inc.==

Volume Three, Issue Thirty-five, File 12 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN           Issue XXXV / Part Three           PWN
PWN                                             PWN
PWN            Compiled by Dispater             PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Prodigy Stumbles as a Forum...Again

by Mike Godwin (Electronic Frontier Foundation)

On some days, Prodigy representatives tell us they're running "the Disney Channel of online services." On other days the service is touted as a forum for "the free expression of ideas." But management has missed the conflict between these two missions. And it is just this unperceived conflict that has led the B'nai B'rith's Anti-Defamation League to launch a protest against the online service..

On one level, the controversy stems from Prodigy's decision to censor messages responding to claims that, among other things, the Holocaust never took place. These messages--which included such statements as "Hitler had some valid points" and that "wherever Jews exercise influence and power, misery, warfare and economic exploitation ... follow"--were the sort likely to stir up indignant responses among Jews and non-Jews alike. But some Prodigy members have complained to the ADL that when they tried to respond to both the overt content of these messages and their implicit anti-Semitism, their responses were rejected by Prodigy's staff of censors.

The rationale for the censorship? Prodigy has a policy of barring messages directed at other members, but allows messages that condemn a group. The result of this policy, mechanically applied, is that one member can post a message saying that "pogroms, 'persecutions,' and the mythical holocaust" are things that Jews "so very richly deserve" (this was an actual message). But another member might be barred from posting some like "Member A's comments are viciously anti-Semitic." It is no wonder that the Anti-Defamation League is upset at what looks very much like unequal treatment.

But the problem exposed by this controversy is broader than simply a badly crafted policy. The problem is that Prodigy, while insisting on its Disney Channel metaphor, also gives lip service to the notion of a public forum. Henry Heilbrunn, a senior vice president of Prodigy, refers in the Wall Street Journal to the service's "policy of free expression," while Bruce Thurlby, Prodigy's manager of editorial business and operations, invokes in a letter to ADL "the right of individuals to express opinions that are contrary to personal standards or individual beliefs."

Yet it is impossible for any free-expression policy to explain both the allowing of those anti-Semitic postings and the barring of responses to those postings from outraged and offended members. Historically, this country has embraced the principle that best cure for offensive or disturbing speech is more speech. No regime of censorship--even of the most neutral and well-meaning kind--can avoid the kind of result that appears in this case: some people get to speak while others get no chance to reply. So long as a board of censors is in place, Prodigy is no public forum.

Thus, the service is left in a double bind. If Prodigy really means to be taken as a computer-network version of "the Disney Channel"--with all the content control that this metaphor implies--then it's taking responsibility for (and, to some members, even seeming to endorse) the anti-Semitic messages that were posted. On the other hand, if Prodigy really regards itself as a forum for free expression, it has no business refusing to allow members to respond to what they saw as lies, distortions, and hate. A true free-speech forum would allow not only the original messages but also the responses to them.

So, what's the fix for Prodigy? The answer may lie in replacing the service's censors with a system of "conference hosts" of the sort one sees on CompuServe or on the WELL. As WELL manager Cliff Figallo conceives of his service, the management is like an apartment manager who normally allows tenants to do what they want, but who steps in if they do something outrageously disruptive. Hosts on the WELL normally steer discussions rather than censoring them, and merely offensive speech is almost never censored.

But even if Prodigy doesn't adopt a "conference host" system, it ultimately will satisfy its members better if it does allow a true forum for free expression. And the service may be moving in that direction already: Heilbrunn is quoted in the Wall Street Journal as saying that Prodigy has been loosening its content restrictions over the past month. Good news, but not good enough--merely easing some content restrictions is likely to be no more successful at solving Prodigy's problems than Gorbachev's easing market restrictions was at solving the Soviet Union's problems. The best solution is to allow what Oliver Wendell Holmes called "the marketplace of ideas" to flourish--to get out of the censorship business.

- -

Computer Network to Ban 'Repugnant' Comments
~~~~~~

>From Washington Post

Prodigy has been charged with allowing "antisemitic slurs" to run on its network. Prodigy officials said they would *not* censor discussion of controversial subjects, such as the one that has been raging over the net for several months -- whether the Holocaust was a hoax.

The controversial message that was labeled "repugnant" included the statements: "Hitler had some valid points...", and "...whenever Jews exercise influence and power, misery, warfare and economic exploitation [are the result]". There were six other messages that the Anti-Defamation League of B'nai B'rith are complaining about. The Hitler message was not available to all subscribers, it was just personal mail between users. The person who received the mail brought it to the ADL's attention.

Civil liberties groups have compared computer networks to telephone companies, which do not censor calls. However, Prodigy officials object to that analogy, saying it is more like a newspaper, and that Prodigy must judge what is acceptable and what is not, much as a newspaper editor must.

Prodigy officials take the position of, and I quote, "we were speaking in broader terms ... we were focused on the broad issue of free expression".

More on Proctor & Gamble August 15, 1991
~~~~~~~~~~~~~~~~~~~~~~~~

by Randall Rothenberg (New York Times)
Further Reading: Phrack Inc., Issue 33 , File.12, "Proctor & Gamble"

Law-enforcement officials in Ohio have searched the records of every telephone user in southwestern Ohio to determine who, if anyone, called a Wall Street Journal reporter to provide information that Proctor & Gamble said was confidential and protected by state law.

The investigation goes far beyond examining the telephone records of current and former employees of the giant consumer products company, an inquiry the Hamilton County prosecutor's office confirmed on Monday. The Journal reported the scope of the investigation Thursday.

The prosecutor, Arthur Ney Jr., acting on a complaint by Procter & Gamble, ordered Cincinnati Bell to turn over all the telephone numbers from which people called the home or office of the reporter, Alecia Swasy, from March 1 to June 15.

The situation began sometime before June 17 when Procter & Gamble, which makes Tide detergent, Crest toothpaste and other familiar supermarket products,

asked the Cincinnati police to determine whether current or former employees were leaking confidential corporate information to The Wall Street Journal.

On Monday the newspaper reported that the company had been bothered by two news articles published on June 10 and June 11 written by Ms. Swasy, a reporter based in Pittsburgh who covers Procter & Gamble. The articles cited unidentified sources saying that a senior executive was under pressure to resign from the company, and that it might sell some unprofitable divisions.

But a spokeswoman for Procter and Gamble, Sydney McHugh, said Thursday that the company "had been observing a disturbing pattern of leaks" since the beginning of the year. She refused to elaborate, but said the decision to pursue legal action was reviewed at several levels in the company and was made by Jim Jessee, a corporate security officer.

Two Ohio statutes protect the unauthorized disclosure of trade secrets. One makes it a felony to transmit formulas, customer lists or other tangible pieces of information that would be valuable to a company and its competitors. But another, broader law makes it a misdemeanor to disclose "any confidential matter or information" without the company's consent.

The Cincinnati police approached the Hamilton County prosecutor's office, which sought and received from a grand jury a subpoena for telephone records.

A copy of the subpoena, dated June 17, was given to The New York Times by someone involved in the case who insisted on anonymity. The subpoena ordered Cincinnati Bell to "identify all (513) area code numbers that have dialed" Ms. Swasy's home or office telephones in Pittsburgh during an eight-week period that started on March 1.

Cincinnati Bell serves 655,297 telephone numbers in the 513 area code, in an area covering 1,156 square miles, said Cyndy Cantoni, a spokeswoman for the company. In the company's entire jurisdiction, which also covers parts of Kentucky and Pennsylvania, about 13 million toll calls are placed in an average month, she said.

Ms. Cantoni said she could not comment on what Cincinnati Bell turned over to the authorities, but said the company routinely complied with subpoenas. Under normal procedure, the company's computers would have automatically searched its customer list and printed out only the originating numbers, and not the names or addresses, of calls to Ms. Swasy's numbers, Ms. Cantoni said.

The Wall Street Journal, which is published by Dow Jones & Co., reported on Monday that neither Ms. Swasy nor executives at the Journal were informed of the subpoena by the authorities.

Neither Terry Gaines, a first assistant prosecutor, nor Ed Ammann, a police department colonel involved with the investigation, returned repeated calls to their offices.

Alan F. Westin of Columbia University, an authority on technology and privacy issues, said the legality of the Ohio authorities' search for the Procter & Gamble whistleblower may depend on how the investigation was pursued.

If Procter & Gamble turned over the names and phone numbers of present and former employees to the police and the police matched that list against the numbers they were given by the telephone company, the rights of other, uninvolved parties may not have been violated, Westin said. But if the police learned the names of people unaffiliated with Procter & Gamble who called the Journal's reporter, he said, or if they turned over a list of numbers to Procter & Gamble for research, some Ohio residents' Fourth Amendment protections may have been sullied.

"When technology allows you to run millions of calls involving 650,000 telephone subscribers through a computer in order to identify who called a person, potentially to find out whether a crime was committed, you raise the question of whether technological capacity has gone over the line in terms of what is a reasonable search and seizure," Westin said.

Expert Fraud Shares Tricks of His Trade October 7, 1991

by Bob Reilly (New York Times)

PHOENIX -- A freelance writer didn't think the $333 that Forbes magazine paid him for a one-page article was enough money so he used his personal computer to duplicate the check in the amount of $30,000. And, the check cleared.

A handyman fixes a bedroom window and gets paid by check. The handyman copies down the homeowner's bank account number, name, address and check number sequences and sends $4.95 to a company that prints fancy colored checks. The handyman masters the homeowner's signature and then proceeds to cash the checks after they arrive.

American Express and Mastercard traveler's checks are duplicated on a colored photostat machine and spent in hotels and restaurants.

A man rents a banquet room in a hotel for $800 and gets the bill in the mail a few days later. The man sends in a check for $400 with the notation "paid in full" written in the lower left-hand corner. The hotel cashes the check and sends a notice to the man saying $400 is still owed. The man refuses to pay the $400 and wins in court because the law says by cashing the check the hotel conceded the debt was paid.

White-collar crime amounts to more than $50 billion a year, said Frank Abagnale, who cited the examples at a business-sponsored seminar in the Phoenix Civic Center. By contrast, bank robbers, who get most of the media attention, abscond with a paltry $450 million, he said.

Abagnale is said to have conducted scams and frauds in 26 nations. Known as "The Imposter," he now advises government and industry. He says he served six years in jail in France, Sweden and the U.S. for his crimes, which included writing bad checks for more than $2.5 million.

"As technology improves, so does the ability to commit fraud," said Abagnale.

He claims that at 16 he impersonated an airline pilot, at 18 was a chief resident pediatrician in a Georgia hospital, at 19 passed the Louisiana state bar exam and served as an assistant attorney general for the state.

Abagnale also claims he never flew an airplane or treated a patient but along the way used false names to get jobs and pass bad checks. He claims he even got a job at age 20 teaching sociology at Brigham Young University, beating out three Ph.D.s for the job.

"I was always just one chapter ahead of the class," he said. Demeanor, style, confidence, clothes and the overt display of wealth also help the con man, Abagnale said.

Abagnale claimed he got one teller to cash a napkin because he drove up to the bank in a chauffeur-driven Rolls Royce and entered wearing a $600 suit and all the confidence of a billionaire. The feat was recorded for television by CBS, he said.

Another time he supposedly put the numbers of the bank account he was using on a bunch of deposit slips, placed the deposit slips in a bank for public use, and in one day alone more than $40,000 was deposited into his account by unsuspecting customers who picked up his slips because they had either run out of their own or hadn't yet got their own deposit slips.

Abagnale asserted that there are several ways to discourage fraud, including:

-- Use checks that are impossible to duplicate on a home computer.
-- Don't cash checks that don't have at least one rough edge.
-- Scan travelers checks by looking for impossible to reproduce pictures or symbols that can only be seen at eye level or by wetting the back, left-hand side of an American Express traveler's

check, which will smudge if it is authentic.

Abagnale is known as the author of a book called "Catch Me If You Can."

"I always knew I would eventually get caught," he said. "Only a fool believes he won't. The law sometimes sleeps, but it never dies."

Abagnale claimed he started a life of crime when his parents divorced and he was forced to choose between living with his mother or father. He said he couldn't make the choice and ran away.

Dumb Jocks Learn First Lesson of Phreaking October 17, 1991
~~~~~~

>From Associate Press

Four current Ball State University basketball players have admitted to investigators that they charged a total of $820.90 in unauthorized long distance calls. School officials announced the preliminary findings in the first phase of their report the the NCAA. What the investigators found, in regards to the unauthorized calls, was the following information:

Person	Yr	Calls	Cost
Jeermal Sylvester	Sop	255	$769.93
Chandler Thompson	Sen	28	$ 45.14
Michael Spicer	Sen	3	$ 4.43
Keith Stalling	Sen	1	$ 1.40

Investigators reported three of the men said former players had provided the long distance credit card numbers or authorization codes on which the calls were made. The fourth player Keith Stalling, could not explain how his call had been charged to the university. Head basketball coach Dick Hunsaker reiterated that neither he nor the coaching staff had made available the numbers that were assigned to the coaches.

"When this problem was first discovered back in August, it came as a shock to me," Hunsaker said. "I'm disappointed with the judgement of the players involved, but I'm glad we're getting to the bottom of it quickly and clearing it up before the season starts."

"Our attention now will focus on former players and other people not connected with the basketball program who might have used the same credit cards and access numbers," said the university's auditor. The investigation that began in August was conducted by the Ball State university's auditor and Department of Public Safety. The investigation started one week after a routine review of telephone records by athletic department officials. At the time, investigators said the total cost of the unauthorized calls was in the thousands of dollars.

Silicon Government in California October 28, 1991
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

>From UPI Sacramento

California unveiled an easy-to-use computer system Wednesday that is designed to tell people about such topics as statewide job openings, where parents can find child care and how to re-register a car.

Officials described the experimental "Info/California" program as an information-dispensing version of an automatic teller machine at a bank. It will operate in Sacramento and San Diego as a pilot project for the next nine months.

Users will obtain free information on a variety of state services as they touch the television-like computer screen to evoke an on-screen narration and color graphics in English, Spanish and potentially other languages.

"It literally puts state government at our fingertips," a computerized image of Gov. Pete Wilson said at a Capitol news conference.

Secretary Russell Gould of the Health and Welfare Agency said the system may be especially useful to announce job openings as the economy rebounds from the recession. Job-seekers will need a fourth-grade literacy level to use the machine, which will refer them to Employment Development Department offices for follow-up.

Director Frank Zolin of the Department of Motor Vehicles said the system will benefit 20 million drivers who want vehicle registration renewals, vanity license plate orders and faster service.

John Poland, Central California manager for IBM -- the state's partner in the project -- said that besides telling the public about job opportunities, it will allow Californians to order birth certificates and get information about education, transportation, health and welfare at more than one site.

During the nine-month trial, people will use the system at 15 kiosks in Sacramento and San Diego that will be similar to, and eventually integrated with, local system kiosks such as those in the courts in Los Angeles and Long Beach, and for community services in San Diego and Tulare counties.

Info/California was authorized under 1988 legislation. It is based on an experimental touchscreen network in Hawaii that 30,260 people used over a six-month period.

The state spent about $300,000 on the project, and IBM invested about $3 million to develop the technology. By performing functions now done by humans, the system may ultimately replace some state workers and produce cost savings for taxpayers.

"We're working smart here," Gould said. "This may diminish some of the need for new state workers."

Digital Tapes Deal Endorsed by Music Industry October 30, 1991
~~~~~~

>From (Congressional Monitor)

Record industry executives joined with retailers and consumer groups in endorsing legislation (S 1623) that would pave the way for widescale introduction of digital audio tapes into the U.S. marketplace.

For the first time, consumers would be allowed to legally make copies of prerecordings for home use.

The agreement would allow artists, songwriters, and record companies to collect royalty fees on the sale of blank tapes and digital audio recorders.

In addition, an electronics chip will be placed in the recorders to prevent anything other than the original recording to be copied.

In testimony before the Senate Judiciary Committee's Subcommittee on Patents, Copyrights, and Trademarks, pop star Debbie Gibson said that many artists had been concerned that digital copying could spell the end of a profitable music industry.

Unlike conventional tapes, digital audio recorders allow consumers to make a perfect copy of a prerecording. The record industry says it already loses $1 billion a year in sales due to illegal copying. And, the industry says, unchecked digital technology would dramatically increase that figure.

Electronics manufacturers and retailers won the assurance that they will not be sued for copyright infringement due to the sale of blank tapes or recorders.

Computer Cryptography: A Cure For The Common Code
~~~~~~

Anyone can sign a postcard, but how do you sign a piece of electronic

mail? Without a "signature" to demonstrate that, say, an electronic transfer of funds really comes from someone authorized to make the transfer, progress towards all-electronic commerce is stymied. Ways of producing such signatures are available, thanks to the technology of public-key cryptography. They will not work to everyone's best advantage, though, until everyone uses the same public- key system.

It is an obvious opportunity for standards-makers -- but in America they have turned up their noses at all the variations on the theme currently in use. The alternative standard for digital signatures now offered by America's National Institute of Standards and Technology (NIST) has brought a long-simmering controversy back to the boil.

Public-key cryptography could become one of the most common technologies of the information age, underpinning all sorts of routine transactions. Not only does it promise to provide the digital equivalent of a signature, it could also give users an electronic envelope to keep private messages from prying eyes. The idea is to create codes that have two related keys. In conventional cryptography the sender and receiver share a single secret key; the sender uses it to encode the message, the receiver to decode it.

In public-key techniques, each person has a pair of keys: a disclosed public key and a secret private key. Messages encoded with the private key can only be decoded with the corresponding public key, and vice versa. The public keys are published like telephone numbers. The private keys are secret. With this technology, digital signatures are simple. Encode your message, or just the name you sign it with, using your private key. If the recipient can decode the message with your public key, he can be confident it came from you. Sending a confidential message -- putting electronic mail in a tamper-proof envelope -- is equally straightforward.

To send a secret to Alice encode it with her public key. Only Alice (or someone else who knows her private key) will be able to decode the message. The heart of any system of public-key cryptography is a mathematical function which takes in a message and a key, and puts out a code. This function must be fairly quick and easy to use, so that putting things into code does not take forever. It must be very hard to undo, so that getting things out of code does take forever, unless the decoder has the decoding key. Obviously, there must be no easy way to deduce the private key from the public key. Finding functions that meet these criteria is "a combination of mathematics and muddle," according to Roger Needham of the Cambridge Computer Laboratory.

The greatest successes to arise from the muddle so far are those using functions called prime factorisation algorithms. They are based on the mathematical insight that, while it is easy to multiply two numbers together, it is very hard to work backwards to find the particular two numbers which were multiplied together to produce some given number. If Alice chooses two large prime numbers as her private key and publishes their 150-digit product as her public key, it would probably take a code-breaker thousands of years to work backwards to calculate her private keys.

A variety of schemes have been worked out which use this insight as the basis for a workable public-key code. Most popular of these is the so-called RSA algorithm, named after the three MIT professors who created it -- Ronald Rivest, Adi Shamir and Len Adleman. It has been patented and is sold by a Silicon Valley company, called RSA, that employs 15 people, most of them ex-MIT graduate students. Faculty firms are to computer start-ups what family firms were to the industrial revolution. RSA has attracted both academic praise and a range of heavyweight commercial customers: Microsoft, Sun Microsystems, Digital Equipment and Lotus Development. But, despite repeated applications, it has never been endorsed by those in government. Rumors abound that the codebreakers in the National Security Agency have discouraged standard-setters from recommending RSA because they do not want to promote the use of codes they cannot break. RSA, for obvious reasons, does not discourage the rumors. Whatever the reason, the standard-setters at the NIST have sidestepped the debate over RSA with their new algorithm, DSA. As set out in the standard, DSA verifies the identity of the sender, but does not encrypt the message. It appends to the message a number calculated from the message and the sender's private key. The recipient can then use this number, the message and the sender's public key to verify that the message is what it seems.

The NIST says that this technique is well suited to "smart cards" and other applications where there is not a lot of computing power available for working out codes. Because it hopes that DSA will be used for verifying the identity of everyone from welfare recipients to military contractors, its flexibility is a boon. Meanwhile, however, more and more companies are choosing a public-key cryptography system for communicating confidentially -- often RSA, sometimes something different. Someday, probably soon, governments will want to choose, too. Watch out for fireworks when they do.

SWBT Sends Off First "Cross-Country" ISDN Call
~~~~~~

>From Southwestern Bell Telephone

The nation's first "cross-country" public network ISDN was placed last week, courtesy of SWBT. The historic first call was the result of a two-year joint effort among SWBT, BellSouth Corp., US Sprint and Bellcore. SWBT's Advanced Technology Lab originated the call, which used US Sprint's digital facilities in Burlingame, Calif. The call terminated at a BellSouth switch in Atlanta, Ga.

Using an ISDN video application, SWBT's trial director Ken Goodgold was able to see and talk to BellSouth's David Collins. "With this test, the geographic limits of ISDN-based services were stretched from a few miles to cross-country," Goodgold says. "We began with protocol testing and service verification, two key parts of the process," Goodgold says. "That required an extremely complex series of technical tests. The Advanced Technology Lab staff worked for months performing the tests leading up to the first successful call."

Last week's test call was significant from a marketing perspective as well as a technical one. That's because it demonstrated the economic benifits of using ISDN for video information. "The cost of a long distance call is approximately the same, whether it's a voice transmission using a regular phone line or a video transmission using ISDN," Goodgold says. "That means a big reduction in cost to arrange a videoconference." US Sprint joined the test because ISDN has evolved beyond the local stage, says Terry Kero, the carrier's director of InfoCom Systems Development Labs. "After today, it will be technically possible to make an ISDN call across the country just as it is possible today to make a regular long distance call," Kero says.

~~~~~~

== Phrack Inc. ==

Volume Three, Issue Thirty-five, File 13 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN           Issue XXXV / Part Four            PWN
PWN                                             PWN
PWN            Compiled by Dispater             PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

The Media Monopoly

by Dispater

As we all know, more technology means more and more legal questions. It is important not only to understand the economic but social impacts of the recent "Telco-TV" issue. I think technologically the idea of transmitting audio/video signals through phiber optic line is fascinating and a great technological triumph. However, how will society benefit by having an even smaller number of owners controlling the media? There is already a media dynasty due to policies established in Ronald Reagan's presidency.

Today almost all of the media is controlled by 18 global corporations. That is down from 23 in 1990 and down from 50 corporations in 1983. The trend is very scary. In the United States there are around 25,000 different media voices. This includes newspapers, book publishers, television stations, radio stations, movie studios, and magazines. However we should not kid ourselves into thinking that there are 25,000 different owners. Is it fair to that 23 companies have so much power over our lives? It is incredibly dangerous to allow this trend to continue. We must stop this trend and "bust up" the media as it was done in the pre-Reagan era.

If you are concerned about this issue I strongly urge you to read "The Media Monopoly" by Ben Bagdickian. It is published by Beacon Press and runs around 300 pages in length.

Phone Companies Could Transmit TV Under FCC Plan — October 25, 1991

by Edmund L. Andrews (The New York Times)

In a surprising and controversial move to promote cable television competition, the Federal Communications Commission proposed today that local telephone companies be allowed to package and transmit television programming.

The proposed rules, which were unanimously endorsed and are likely to be adopted within a year, would expose cable companies to the most threatening competition yet. But they could benefit cable television consumers, many of whom have seen their bills double and triple in recent years.

The cable industry vowed to fight the proposals and threatened to challenge the rules in court if they are adopted. Telephone companies, eager to enter a lucrative new business, applauded.

"Today's action will create competition and offer consumers more choices," said James R. Young, vice-president of regulatory and industry relations at the Bell Atlantic Corporation. "Let's hope it's a beginning to the end of turf wars."

In essence, the commission recommended that telephone companies be allowed to offer "video dial tone" over telephone lines that would carry programming produced by outside companies. Consumers could view whatever programs they pleased and would be charged accordingly.

Initially, telephone companies would serve primarily as a pipeline, not

producing the programs. But the commission said telephone companies should also be allowed to organize and package video services, as long as they make their networks available to all programmers. The commission also opened an inquiry on whether to let telephone companies produce programs.

The idea of allowing so-called video dial tone service has long been a favorite of the FCC's chairman, Alfred C. Sikes. Congress, which is weighing regulatory legislation to rein in cable process has shied away from the issue. Today's action makes it more likely that lawmakers will have to reconsider the role of telephone companies in television.

Before cable companies would feel much impact from today's FCC proposal, however, most telephone companies would have to spend billions of dollars to install new fiber-optic transmission lines and switching equipment that could carry large volumes of television material. Analysts have estimated that the cost of converting every home in the country to a fiber-optic line would be $100 billion to $200 billion and that it would take at least five years.

Most large telephone companies, including all of the regional Bell companies, already plan to replace their copper wires with fiber over the next two decades. The immense business opportunity posed by the $18 billion cable television market is likely to accelerate those plans.

High-capacity communications lines that reach every home in America could radically alter the distribution of entertainment and enable people on home computers to tap distant libraries and obtain information in seconds.

"Both program providers and consumers would have chances they don't have today, without the bottlenecks provided by cable companies and without the bottlenecks of broadcasting," said Richard Firestone, chief of the FCC's common carrier bureau.

The move was immediately attacked by the National Cable Television Association, which threatened to challenge any new rules in court.

"Until and unless the telco's monopoly in voice telephone is ended, no level of Government safeguards against cross-subsidies will be effective," said James P. Mahoney, president of the cable association.

The most controversial issue, which the FCC raised for discussion without recommendation, is whether telephone companies should be allowed to produce programming, a much bigger business than transmission. Many Bush Administration officials favor such a move, but television broadcasters and producers bitterly oppose it. Officials noted that such a shift would require changes in the Cable Television Act of 1984.

"Among the top two or three concerns of ever cable operator has always been head-to-head competition against local telephone companies," said John Mansell, a senior analyst at Paul Kagan Associates, a marketing-research firm that monitors the cable industry.

For telephone companies, the move could be a windfall. Steven R. Sieck, vice president of Link Resources Inc., a market-research firm in New York, said, "It's by far the largest market opportunity among the whole collection of information services" for telephone companies.

It remains unclear, however, whether the new rules will survive in court. The Cable Television Act of 1984 bars a telephone company from owning a cable television franchise in the same market. The FCC ruled today, however, that the law does not prevent a local telephone company from transmitting programs produced by other companies and that it does not bar long-distance carriers in any way.

The Bell companies have lobbied strongly for legislation that would allow them to enter the cable business, and several companies have invested in European cable franchises. In addition, Pacific Telesis Group, which provides local phone service in California, already holds an option to buy a controlling interest in a Chicago cable franchise, which could be [sic] permissible since it is outside the company's telephone area.

The commission also handed down a ruling that could give telephone companies an important price advantage in future competition with cable operators and could prompt protests from local governments, ruling that neither a telephone company nor a video programmer needs to pay franchise fees to local governments.

Under the cable act, by contrast, local governments can charge cable operators a franchise fee as high as five per cent of revenues.

Explaining today's ruling, Mr. Sikes said, "We have segregation laws, and these segregation laws should be ended." He added that some cable companies were already installing optical fibers in their own networks, and that some were exploring the option of using their networks to offer telephone service.

The proposals mark the second major change in longstanding restrictions on the telephone companies' ability to move into new services. Less than three weeks ago, a Federal appeals court cleared the way for the regional Bell companies to begin providing information services, like news, stock and sports tables, immediately.

- -

Phiber Optic or Twisted Pair?
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by John J. Keller (Wall Street Journal) October 28, 1991

Expanding the nation's telephone network into a vast television broadcast system is going to cost tens of billions of dollars and won't be finished before the end of the decade, say executives at some of the largest phone companies.

But the scale of the project isn't stopping the phone giants, such as GTE Corp., Ameritech, Bell Atlantic Corp., and Pacific Telesis Group, from methodically exploring how to implement such a system.

The Baby Bells and GTE have spent several million dollars testing new systems that carry cable TV shows into homes via the phone network. The phone companies will spend many million of dollars more before they are satisfied that they have a service that matches the current voice phone system and tops today's entrenched cable TV monopolies.

Last week the phone companies were buoyed by a Federal Communications Commission plan to support a new technology called video dial tone, that would put the big phone companies into direct competition with local cable-television monopolies.

Phone subscribers could use such a system to dial up and order video programs from an entertainment company through the same wire that connects a typical phone call. More important, allowing the phone companies could generate enough traffic to fund "broadband" upper-capacity information highways that could someday carry TV, medical information, and even FM stereo channels into a home through a single wire, say the executives.

However, big hurdles remain. The FCC hasn't decided whether to let the phone companies participate in the programming end of the cable TV business. The phone companies argue that's a financial necessity, because cable TV companies would be reluctant to share the programs they now support and run them over a rival's network. In addition, the 1984 Cable TV Act, which prohibits phone company participation in the cable business, would have to be rewritten.

"We're encouraged by the FCC action, but it's not as complete a step as there needs to be made," said Larry J. Sparrow, vice president of regulatory and governmental affairs at GTE Telephone Operations, Irvine, Texas. Adds Kathleen Ahren, Nynex Corp.'s director of federal regulatory policy: "For us to build facilities without anyone to use them would be irresponsible... programming is essential."

There are also technical issues such as whether TV service to the home should be provided through a cable-TV-like coaxial cable or advanced fiber-
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

optic line. Either would require pulling out existing "twisted pair" wiring that now binds the phones in homes and most small businesses to the local phone network. Moreover, the phone industry must still hammer out technical standards for melding video transmission, which requires tremendous transmission capacity, with voice traffic, which uses far less.

The system that is finally built will require mountains of capital to transform the existing phone network into a high-capacity phone network of systems that pump signals digitally through fiber-optic transmission lines, which are glass wires. "We've seen figures that it would cost about $250 billion nationwide," says James R. Young, vice president of regulatory and industry relations at Bell Atlantic. Adds Ms. Ahern, "I don't think our plans would have us doing this in less than 20 years and if we do you're talking billions of dollars."

Pacific Bell, which spends about $1 billion a year on new network equipment, would see that annual tab jump by two to three times in the first several years of constructing a broadband network, says Michael Bloom, customer premise, broadband applications at the San Francisco-based unit of Pacific Telesis Group. But he notices that as equipment purchases grow and the technology is perfected the annual cost should drop down to current levels after about four years.

PacBell, like most other phone companies, already has installed fiber-optic "trunking" lines to carry bulk traffic between its switching centers. It has also begun replacing copper facilities in some neighborhoods, running optical fibers to the pedestal at the curb and then connecting to the regular phone home wires. Someday these lines will carry cable TV, but for now regulation restricts the phone company to voice and data transmission, says Mr. Bloom.

Someday this will change, says the FCC, which envisions a service where phone customers would turn on their TVs and find a listing of TV shows, movies, news and other programs, supplied by the phone company and other programmers and accessible via remote control.

Several phone companies are already testing such services. In Cerritos, Calif., GTE has built an elaborate network of fiber-optic and coaxial cables lines and advanced switching systems to deliver TV services to several thousand customers. One service, called "Main Street," allows a customer with a remote control to shop via TV, check a bank account and even seek information on colleges in the US. Another service, dubbed "Center Screen," lets 3,900 residential customers call for a movie or a TV show by dialling a special number. A third service lets some customers talk to one another through a videophone in the house.

"We've found [from the Cerritos tests] that our customers like full-motion video and not still pictures," which is all that's possible over today's regular phone lines, Mr. Sparrow says.

That's because regular conversation travels over phone lines at the rate of 64,000 bits a second. By contract, "reasonable quality" video, such as the kind that appears from a VCR tape, requires transmission capacity of at least 1.3 megabits to 1.5 megabits a second. High quality video will take capacity of 45 megabits to 90 megabits a second, he says. A megabit equals 1 million bits.

To save money and get as much capacity out of the existing copper-based systems, Bell Communications Research, the Baby Bell's research arm, has developed "video compression" technology which uses existing copper wire to deliver TV to the home. With video compression, a microprocessor squashes video signals so they can be sent through a regular phone line at the rate of 1.5 megabits a second. The little chip, which is in an electronic box attached to the phone line, looks at an incoming video signal, and filters out the parts of the moving image that are redundant. The chip codes and sends the parts of the signal that are different through the phone line to a receiving box, which decodes and reconstructs the image before projecting it onto the TV screen.

The cable companies hope to retaliate by providing phone service through their cable networks. They are funding research to develop switching systems

that can pass phone calls from one cable subscriber to another and out to customers using the regular phone system.

But the blood between the industries isn't all bad. Ameritech's Indiana Bell subsidiary and Cardinal Communications, an Indiana cable TV operator, are testing a fiber distribution system made by Broadband Technologies Inc, of Raleigh, NC. The system is being used to route video and phone signals over backbone fiber-optic lines and finally through coaxial and twisted pair lines attached to homes in Tipton Lake, a Columbus, Ind. residential development. Bell Atlantic is negotiating with Loudon Cablevision, a cable TV company in Loudon County, Va., to test the transmission of TV signals through phone company lines to 5,000-6,000 homes in The Cascades, a local housing development.

- -

Baby Bells as Big Brother November 2, 1991
~~~~~~~~~~~~~~~~~~~~~~~~

>From The New York Times

Two official decisions in October, one liberating and the other frightening, may shape telecommunications -- and America -- for decades. The liberating decision, by the Federal Communications Commission, proposes to allow the seven regional telephone companies to transmit TV programs.

If implemented, that proposal for video-by-phone would free families to tell cable operators, if they misbehave, to get lost.

The frightening decision, by a federal appeals court, unblocked the same seven "Baby Bell" companies from owning electronic yellow pages, video shopping and other information services.

Unless Congress intervenes, this decision will allow the Baby Bells to exploit their monopolistic stranglehold over residential phone lines and dictate what information reaches nearly every home. The same principle ought to govern in both situations: democracy needs diversity.

Technological advances have brought the nation to a regulatory crossroad. A single information pipeline -- perhaps fiber-optic cable, perhaps enhanced coaxial or copper wire -- may soon pour an unimaginable array of phone, video and data communications into homes. Whoever controls the pipeline controls access to American minds.

The best protection against Big Brother is to separate control of the pipeline from the information. That could be easily enforced by requiring that pipeline owners, like the Baby Bells, serve only as common carriers and lease pipeline space to information providers on a non-discriminatory basis.

Common carrier status is what the FCC proposal would achieve for video services but what the appeals court decision would foreclose for information services.

Congress seems unwilling to impose common carrier status. But Rep. Jim Cooper, D-Tenn., offers a second-best remedy. As long as the Baby Bells retain monopoly control over local phone service, he would allow each to sell information only outside its own region. His bill also offers stringent safeguards against anti-competitive behavior.

Yet the bill's provisions aren't as safe as common carrier status. The Baby Bells have frequently violated regulations; rules alone are unlikely to stop them from subsidizing forays into information services with funds extracted from captive rate-payers.

Contrary to their claims, the Baby Bells have no special abilities to provide electronic services. If they could sell video shopping for a profit, so could hundreds of other companies -- not one of which has the power to intimidate ratepayers because not one has privileged access to their homes.

Nor, as the Baby Bells claim, do they need to produce their own information services in order to fill capacity on fiber-optic cables they might
~~~~~~~~~~~~~~~~~~~~~~~~

lay.

The strongest argument the Baby Bells offer is technological. Only a single company, they contend, will be able to marry pipeline and information. But there's no proof of this speculation and besides, there are better ways to manage the problem.

The Cooper bill provides plausible protection against monopolistic Baby Bells, giving them ample room to compete but limited room to exploit.

Newspapers, including The New York Times Co., support the bill for competitive commercial reasons. But there is a much more important reason for the public to favor, and Congress to adopt, the Cooper bill: to protect the free, diverse flow of information on which democracy depends.

- -

Don't Baby the Bells November 10, 1991
~~~~~~~~~~~~~~~~~~~

>From The New York Times

Although the Bell companies are opposed by numerous groups, including the Consumer Federation of America, the cable television industry and existing providers of electronic information services, it is the newspapers that are its biggest opponents.

The publishers argue that the telephone companies can compete unfairly by subsidizing their services with money from their regulated telephone businesses and by imposing technical obstacles to competing information suppliers.

But one of their biggest fears is simply that the telephone companies could attract a large proportion of the classified advertising, a mainstay for newspapers, by offering cheap and easy-to-use electronic bulletin boards.

The newspapers are pushing Congress to adopt a bill introduced by Representative Jim Cooper, Democrat of Tennessee, which would not allow a Bell company to offer information services unless those services are already available to at least 50 percent of the people in the area over an alternative network.

As a practical matter, the bill would reinstate the information-service ban for all Bell companies for years, because of the difficulty in building an alternative network that reaches most customers.

To defend their position as more than a simple bid to keep out competition, the newspaper association has crafted a blunt advertising campaign around the slogan "Don't Baby the Bells."

In one ad, the association warns that the telephone companies could amass as much private information on customers as the Internal Revenue Service.

But while many members of Congress are worried about giving new powers to the Bell companies, the Cooper bill has thus far attracted only 24 sponsors, and most experts doubt the bill can muster enough support to pass even the House.

Meanwhile, the Bush administration strongly favors lifting the prohibition on information services and would probably move to veto a bill that kept it in place. The upshot is that newspaper publishers are in a difficult position.

A stalemate in Congress amounts to a complete victory for the Bell companies, because court decisions have already given them precisely what they want.

In Congress, however, aides to leading lawmakers say they are waiting in part to see how much popular and political strength each side can muster. "We want them to show us what they can bring," one staff member said about the publishers.

One lobbyist allied with the publishers said opponents of the Bell
~~~~~~~~~~~~~~~~~~~

companies were essentially trying to build up a bargaining position. "You could see this as the beginning of a minuet," he said. "The question is whether they will ever get into the middle of the floor and dance."
