# Blacklisted! 411

## The official hackers magazine

INSPIRING MINDS TO THINK OUTSIDE THE BOX...

# Hacking With a Proxy Server

Helping people remain anonymous on the net

Also inside this issue:

**Hacking a Wireless Router**
**PDA Security**
**Defcon 2004 Recap**

VOLUME 6 ISSUE 4 FALL 2004

Blacklisted! 411 v6i4
$5.95 U.S. $7.75 CAN


*This publication is dedicated to all of those before us who built the foundation for the hackers of the world to express themselves openly and without prejudice.*

*While we attempt to continue in our quest to obtain knowledge and understanding, we invite you, the reader, to join in and share any thoughts you may have regarding the magazine, hacking, life, work and anything else that you feel is important enough to be shared.*

*We're not going to knock anyone down for asking questions or ridicule the steadfast elitist folks who believe that knowledge should not be shared. We believe knowledge should in fact be shared with one another, no matter how trivial the information may appear to be. After all, knowledge is power.*

*Think back to the way it was, when hackers stuck together and had a good time. An amusing time when hackers shared their stories of exploration and ultimate conquest. A wondrous time when hackers were considered the good guys and looked up to by those not fortunate enough to understand the technology around them. A simple time when a hackers harmless efforts gained a new understanding of technology issues and the praise from their peers and superiors alike.*

*That time can still be NOW. Hackers of the world unite and exercise your freedom to disseminate information!*

# *Blacklisted! 411 staff & contributors*

## Editor in Chief
*Zachary Blackstone*

## Assistant Editors
*Alexander Tolstoy*
*Dave S.*

## Office Help
*Pixel Pixie, Jess, Lexus,*
*Dark Paladin, DoctorWHO,*
*MomoPi, Mr. Asshole*

## Artwork
*Derek Chatwood - A.K.A. Searcher*
*Kate O., Parallax,*
*Mason/Wolf*

## Distribution
*Greg, Boiler, Syntax, David B.*

## Photography
*CHS, Dark Paladin, Daniel Spisak*

## Forum Admin
*Spratt_*

## Writers
*ML Shannon, Goldfinger, BarfBag, Kingpin,*
*Double-O-Jake, Grandpa Hackman, Trash-00X,*
*Wild E. Coyote, TechnoHeap, Rogue,*
*The Crypt Phreaker, Erik Giles, Sam Nitzberg,*
*Mother Goose, Cactus Jack,*
*Bob Blick, Stank Dawg, MobbyG,*

**ISSN 1082-2216**



**Blacklisted! 411 Magazine**
**P.O. Box 2506**
**Cypress CA, 90630**

9035768ABBAJBVJB-0020

DBBL 01,07,32,41,52

**PRINTED IN THE UNITED STATES OF AMERICA**

## Blacklisted! 411 shout outs

*Doc Salvage*
*ECSC*
*oleBuzzard*
*Dark Tangent*
*DEFCON*
*Freaky*
*Blackwave*
*IrvineUnderground*
*Consumertronics*
*Wizguru*
*Greyhawk*
*Spratt_*
*The Underground Mac*
*Bobeeve*
*German*
*Big Dog*
*Skippy*
*Avatar*
*Neuromancer*
*Doc Jones*
*LineTech*
*Alaric*
*Short Circuit*
*Mingle*
*The Goldfinger*
*E. Coli*
*Group 42*
*SWAT*
*Trash-OOX*
*Doule-O-Jake*
*Ender Wiggin*
*TechnoHeap*
*GI Electronics*
*Briel Computers*

*....and a few ANONYMOUS people*

## Inside this issue



## Additional information


**How to Contact us:**
Blacklisted! 411 Magazine
P.O. Box 2506
Cypress, CA 90630

**Subscriptions:**
$20 U.S., $24 Canada, $35 Foreign
Check or Money Order (U.S. Funds only)

**Articles:**
Blacklisted! 411 Articles
P.O. Box 2506, Cypress, CA 90630
*(Include name & address—we PAY for articles)*

**Letters:**
Blacklisted! 411 Letters
P.O. Box 2506, Cypress, CA 90630

**Distribution and Sales:**
Blacklisted! 411 Distribution
P.O. Box 2506, Cypress, CA 90630
Email: sales@blacklisted411.net

**Advertising:**
Blacklisted! 411 Advertising
P.O. Box 2506, Cypress, CA 90630
Email: advertising@blacklisted411.net

**World Wide Web:**

**Website:** http://www.blacklisted411.net
**Store:** http://store.blacklisted411.net
**Forums:** http://www.bl411forums.com

# *Blacklisted! 411 introduction for those of you who are new…..*

**Who we are… and were…**

The question often arises on the subject of, "How did it all start?" in reference to our magazine and it's history. In response to this popular question, here is a quick history lesson of *Blacklisted! 411* magazine, including names, dates and little known facts which have, thus far, been hidden away for years…

*Blacklisted 411* magazine dates back to October 1983 with a group of friends from a Southern California high school that shared a common interest. We were all into our Atari computers, Commodore computers, electronics, sciences, arcade games, etc. We built projects, hacked into this n' that, came up with grand ideas and tried to make them into some sort of reality. The group started a monthly hackers "disk magazine" (an early form of what is now known as an e-zine) called "*Blacklisted 411, the hackers monthly*". This may sound strange today but circulating information on disk was the best way to get it out without all the cool toys of today. We didn't have the internet to send it out, and no one had printers that could print anything other than plain text (and didn't even do that well). With a disk based system we could send text files, primitive graphics/pictures, and utilities more easily and it could be copied by anyone who had a compatible computer. At our peak we distributed 150 disk copies <per month> of the disk magazine, though there is no way to know how many were copied by others.

Eventually modems caught on and we began to distribute the monthly via crude BBS systems. Using the power of a Commodore 64, we put up a *Blacklisted! 411* info site, which anyone could log into without handle or password. It was a completely open message center. Using X-modem or Punter file transfer protocols, you could download the latest *Blacklisted! 411* files or read/leave "messages" which later became known as a "message base" and has evolved into what are now commonly known as "newsgroup postings" or "forum postings". We had only one message center, no email capability & only 1 phone line. Primitive, indeed. Effective, however.

Around 1984 we purchased a 9 pin dot matrix printer that could <gasp> print basic graphics. We experimented with printing out copies of the *Blacklisted 411 monthly* and copying them at the media center at the high school. The media center staff graciously allowed us to make these copies free of charge which was very cool at the time. We'd pass these out at the local "copy meets" (an interesting phenomenon of past times - hordes of computer users would meet at a predetermined location and setup their computers with the sole purpose of copying software and exchanging this software with each other). We'd leave a pile of our magazine copies anywhere we were allowed to do so. One popular location was next to the Atari Gauntlet and Gauntlet II arcade games strategically located at 7-11's all over the place. We're only guessing here, but we think people photocopied our copies and then those were photocopied, etc. There's no telling just how many generations of early printouts of *Blacklisted! 411 monthly* made it out there.

Years went by and *Blacklisted! 411* evolved. The short life-span of the printouts was both a great success and a miserable failure. No matter where we left them, they were taken - and taken quickly! The feedback was awesome in that people wanted more. The interest was very high, but our inability to meet this growing demand was completely overlooked. We had to officially pull the plug on the printout experiment and we stuck with electronic files. It was really the easiest way to go. The *Blacklisted! 411* info site grew into a 2-line system. This was a big deal in 1985. By that time, information was almost exclusively passed around by modem (unofficially on paper) and we were still releasing disks at this time.

June of 1987 marked the end of *Blacklisted! 411, the hackers monthly*. Our last disk based magazine was distributed that month. Now that all of us were out of high school and onto college, work and the bigger/better things in life, nobody had the time or inclination to put any effort into the disk based magazine anymore. The once thriving *Blacklisted! 411* group broke up and people went their separate ways. Naturally, we all assumed this was the end and *Blacklisted! 411* would never come back in any form.

In the summer of 1993, one member (and the original editor-in-chief), Zack Blackstone, felt it was time to revive the *Blacklisted! 411* concept, but this time do it as a print magazine. It was extremely difficult to get started because the group was no more. He was the only one of the original group members remaining that had an interest in bringing the hacker group and magazine alive again. With some money, will to make it happen, and with the help of some top of the line (at the time) computer gear and page layout software *Blacklisted! 411* was reborn. *Blacklisted! 411* Volume 1, Issue 1 was released in January 1994. *Blacklisted! 411* was finally BACK. The issues were released monthly and distribution was small. After a year passed, it was decided to try a quarterly format in an effort to increase distribution. During that year Zack managed to get in contact with many of the old group members and they are now active staff members once again.

In 1999, we published what was to be our last issue of *Blacklisted! 411* (Volume 5, Issue 4) for many years to come. We didn't know it at the time, but many pitfalls would ultimately cause the demise of the magazine. After 4 years of regrouping and planning, *Blacklisted! 411* magazine is back in print form again. We are one of the oldest group of hackers still remaining and releasing gathered and compiled information within the hacker community and the mainstream community as well. We still have the same hacker mentality and code of ethics from the 80's. Hackers are not thieves - they're curious people. We are not elitist hackers by no means and no question is a stupid question. We're not going to knock you down, call you a "lamer" "lamah" or give you crap for being a newbie! Every hacker started somewhere. We remember this most fundamental fact and we will never forget it.

***What's Next…***

**Community**

Over the next few months a lot will be happening. We are becoming more active in the Hacker Community. As we are based in the Los Angeles area, we are building relationships with the local Hacker groups such as LA2600, SD2600, twentythreedotorg, Irvine Underground and more. We will be attending and sponsoring Hacker Conventions and Conferences. The first being the Layer One Convention, June 12-13, at the LA Airport Westin. We will have a booth at this event where we will be selling subscriptions, current and back issues of the magazine, and other swag. We will also be having several "convention only" promotions so look for us there.

**Magazine Development**

A major effort is being made to increase our exposure to the Hacking and Information Security Community. Our distribution goals are for the magazine to break 100K copies distributed each quarter sometime next year. Based on the demand, and orders from distributors we are on the right path. We are seeking and hiring freelance writers, photographers, and editors to increase the quality and scope of the magazine. Additionally, we have people who are actively trying to promote the magazine both inside and outside of our close community.

**Merchandising / SWAG**

We wish to have a whole series of *Blacklisted! 411* themed swag and merchandise. This includes stickers, apparel, posters, and whatever else our creative minds can come up with. Input, help, and direct submissions for this will be accepted and appreciated.

**Charities**

*Blacklisted! 411* is run by real people who care about other things aside from hacking. No, really. In the spirit of helping people and organizations outside of our community, *Blacklisted! 411* Magazine has officially donated to the local chapter of the Ronald McDonald House charity. After all, children are our future. *Blacklisted! 411* Magazine wholeheartedly supports the Ronald McDonald House mission and their programs. Additionally, we've donated heavily to the Westminster Parish Festival, specifically with the intent to help support their youth programs and special classes for the mentally and physically handicapped.

If you have questions, comments, articles, ideas, flames, general "screw you guyz" messages or wish to offer support in some way, please contact us immediately and let's see what we can do. Thanks for your support, hackers! ***BL411***

## *Letter from Zachary Blackstone, editor-in-chief…..*

Welcome to another issue of Blacklisted! 411 Magazine.

Has another three months gone by already? Yep. That's right. We've made our way to the Fall 2004 issue and it's getting better. The content is cleaning up to reveal the true hacking articles we like to publish and the number of contributors has increased tremendously.

So much has happened since our Summer issue—nothing but good things. Most notably, the amount of response and feedback we've been getting. The Fall 2004 issue's distribution officially puts Blacklisted! 411 back in the position to lay claim that we're the most widely distributed hacker magazine on the planet! Thank you to everyone that made this possible so quickly.

We've taken the time to make our presence known at both the LayerOne convention and the DefCon convention. Alex, my assistant editor, and some staff managed to attend both conventions. If you came by and said HI to us, thanks - we appreciate it. Everyone generally welcomed us with open arms and allowed us to take our place among the community with little resistance. A few people approached us with some preconceptions, but those ideas were quickly laid to rest and we made more new friends.

We received many new subscriptions, picked up new writers and generally made friends with a lot of new people. That's right. While our real reason for attending the conventions was to make our presence known among the community and to contribute back into the community, it couldn't be helped. We sold some subscriptions and back issues. Thanks for the support, guys! In addition to this, many of you voiced your support for what we're doing and subsequently made contact with us after the event(s) to offer your support in various tangible ways. From articles to artwork and everything in between, it's greatly appreciated!

People have been dumping off stuff for us to review and play with. In fact, I decided to write about some of the more interesting stuff in this issue. You can read about it and, hopefully, find some of these things useful. Many other groups and media have been contacting us to arrange interviews and possibly exchange material, ideas to work toward some sort of mutually beneficial arrangement.

One of the big news items of ours is the fact that our website has recently expanded to include a FORUMS section that all are welcome to join and participate in. People kept asking for it, so we made it a reality. Spratt_ of UGM networks put the forums together for us and he's the official Admin for the site. The forums will finally bring the Blacklisted! 411 magazine media to a new level, offering additional means for our community to express themselves, exchange their ideas and offer their opinions in an open medium.

We've always been about technology and offering the newbie a means to start their hacking careers on the right path as well as the old school hackers a place to call home. In fact, hundreds of old school hackers have taken the time to contact us and express their gratitude that we're doing what we are, providing the hacker, old and new alike, a place to congregate and that we're not all about the b.s. 'leet haxor script kiddy hacker wannabe's.

It's a great feeling to know that what we do is appreciated by so many people. The only way we know this is by the feedback we get from all of you. So, keep it coming. If you have any comments or suggestions, by all means, please let us know as soon as possible. Some of our readers suggested that there wasn't enough technical material in the latest issue of which I agree whole heartedly. Our magazine has always included a bit of information from the fringes, which has given the magazine the gritty underground reputation it's had for so long. However, the last issue was a bit over the top with more than the usual non-hack for reasons of marketing & targeting specific user groups. The material content will revert to more technical reading starting with this issue, the Fall 2004 edition.

Part of my usual routine, I've been on top of the gossip with the grapevine and I've read and listened to just about every review and piece of commentary on our magazine since our return. Overall, people are generally happy we're back with only two real gripes.

One, which I just addressed above, was about the content which is a resolved issue as far as I'm concerned. The next, which came from only three people, one of which was very persistent in his constant nagging on the topic, was that our tagline of "the official hackers magazine' was inappropriate for two reasons:

1. The hacking content was not enough to qualify.
2. We don't have any reason to make this claim.

Let's put this gripe to rest right here and right now.

1. The magazine has always been about hacking. Period. Sometimes the fringe material which somewhat fits into the social engineering concept—which has long been established as a hacking relevant topic—is heavy from issue to issue, but we've since decided to tone it down and push back into the technical side of the magazine which people apparently liked better and want to see more of . Ok, resolved. See, that was good constructive criticism.

2. We do have a real and specific reason for using the tagline of the "official hackers magazine" The original need for this was because of a knock-off of our zine, but that's long since passed. Now, here and today, Blacklisted! 411, granted only first available in disk format, was around *well* before any of the other hacker magazines still available today. Second, with our distribution for the Summer and now the Fall issues, we have the undeniable right to make this claim if based solely on the fact that we now have higher distribution than *any* other hacker zine on the planet. Nobody touches us! That's it. It's done. Get over it. 'nuff said.

Yep, that was pretty much it for the gripes. Pretty standard stuff, I suppose. Either way, we shut down both topics with ease and we can now move on to bigger and better topics.

Again, don't forget to visit our forums available from our main website: http://www.blacklisted411.net

All in all, I'd say this has been a great summer for us all over here at Blacklisted! 411 magazine. I would be sorely mistaken if I didn't realize that it's because of each and every single one of you, our readers, that Blacklisted! 411 is where it is today. So please understand that myself and the rest of the staff over here sincerely thank you for your continued support and feedback. THANK YOU.

***Blacklisted! 411 Magazine***
***P.O. Box 2506***
***Cypress, CA 90630***

***- Editor***

### *Notes of interest:*

**- We currently have all of Volume 1 back issues available at this time.**
**- Volume 5, Issue 3 and Volume 5, Issue 4 is still available in very limited quantity.**
**- We're no longer offering any t-shirts, baseball caps or bumper stickers, but we're accepting design ideas for new swag.**
**- Deadline on all articles, letters, artwork and ads for Volume 7, Issue 1 is November 21st, 2004.**
**- ALL classified ads are now FREE and are limited to space constraints per issue. First come, first served.**
**- We're a PAYING MARKET for articles we use! We pay $25-$600 depending on size, quality & use of photos.**

## *Letters and comments from our readers…..*

Blacklisted! 411,

I have a question that I am having great difficulty finding the answer to. I recently picked up a copy of your mag at borders and am pleased to see it out again. I think the last time I even saw one was like 100 years ago. I really enjoyed the article The Ear by M L Shannon, anyway.

I am trying to learn security and I am testing my own windows network... I was able to find my FTP port open and when I typed ftp://myip in the browser it showed that I was connected but did not allow me to browse anything. It was just like it was blank. My question is why does it not allow me to browse things like C:\ or any other directory and how can that be exploited.

Every time I ask this on a message board people are like "get a firewall" and I never get the answer to my actual question. I never did install a trojan to see if I could actually upload and get in for fear of exposing a backdoor into my network. I am a beginner at this and am just trying to learn.

Great mag by the way and plan to get a subscription soon. It was kind of funny when I bought it because this grey bearded guy who was running the cash register said "you'll like this one better than 2600" it was kind of freaky but way cool. Peace.

**Mike P.**
**Routed: Internet**

*I believe you're missing some important background information for an adequate answer, but I'm going to attempt to answer you regardless. Let's assume you are running XP and have an FTP server setup on the machine. If this is true and you're getting the results you've described, you need to go into your FTP server config and set the sharing to whatever areas you want available to be served up.*

*If you're not running FTP on your machine and you ftp:// yourip, it will error out and then give you a blank screen - where you can't do anything. Somewhat the way you described. If this is the case, you need to setup a server on your machine. XP has a server option, too. Open up your control panel, click on add/remove> windows components> iis services> ftp service and away you go.*

Blacklisted! 411,

Hey guys what's up? Just wanted to drop you guys a line or two or three. I picked up my first Blacklisted Mag today at my local Borders. When I first saw it I thought that 2600 had changed the name of their mag cause I had never heard of the blacklisted brand before. After skimming through it I had to buy the mag so that I can start my collection. I have a few comments about my first issue of blacklisted to bestow on the rest of the community. I for one can not and will not consider myself a "hacker", "cracker" "hax0r" or any of that. I am very much interested in the art and the culture of "hacking" though. I emphasize these word explicitly because from time to time friends and family like to call me a hacker because of the knowledge that I do have dealing with computers. I get pissed off at them and try to tell them that I am not. It doesn't work in the least. The general idea people have (especially with myself) is that just because I can fix just about any computer problem that I come across that it makes me a so called "hacker".

Now some might ask why I get pissed at the fact that I am considered a "hacker" amongst family and friends. Well it is simple I have knowledge, yes. But the ones that made the "hacking" community what it is have superceded anything I could ever do. They took their knowledge and made it a skill, a art form, a culture, a way of life. They have contributed to the scene in many numbers of ways and have put a lot of time and effort into their knowledge and understanding of the inner workings or things. Myself, I have not. The things that I know and that I pick up have come natural to me. I have not really reached out to learn the inner workings of thing or have contributed to the scene. I have read up on things because I was a little curious and I even held a stance on the whole Kevin Mitnick ordeal.

Why do I/did! do these things? I did them because I feel that as an American that freedom of speech and freedom of expression, while being one of our rights, the only way you truly have them is if you are a undergrounder. I support these people because they are the ones that have stepped up from the foot of big brother and didn't care. Myself I am actually afraid to dig too deep into anything for the simple fact that one slip up and my life can be taken from me instantly. Not physically, but socially. I would love nothing more than to broaden my knowledge and horizons, but you have to start somewhere. And with these days and time you can't trust a soul, and the ones that say you can trust them don't want to help you out any. Now I am 24 years old and I have been using a computer since I was in the first grade. To the "hacking" world I am a newbie, a lamer. But to you intellectuals out there I am knowledgeable and willing to learn so to you guys that are intellectuals I thank you for your time and your dedication.

Sorry about the rambling I get into those from time to time, but read it and my point is there. That while some like to run around calling themselves "hackers" there are some out there that do respect you guys for what you do and what you have done. I am one of them....

I plan on doing what I can to hook you guys up with some graphic designs cause it is my way of helping out those that truly deserve it. Thank you.

**NilCode**
**Routed: Internet**

*Nilcode, thank you for your thoughts and comments. While you may not care to carry the title of hacker, you obviously share in the ideals of the hacker community. Continue on your quest to learn at whatever pace makes you feel comfortable. You're, apparently, well versed in the technology around you and you're a hands-on kinda guy, so the remainder of your journey should be a cake walk for you.*

*Thank you again and we look forward to your graphic design work.*

Blacklisted! 411,

I'm looking for newer ways to make long distance phone calls from payphones. The ol' generated tones on the tape recorder do not work in Oklahoma anymore.

Can you point me in the right direction?

**Drkdaiz**
**Routed: Internet**

*I once saw a movie, I think it was an 80's movie, where a teenage girl was standing on her head, talking on a phone to her best friend. I didn't think much of it at the time, but your question reminded me of it. You really might want to try something like this. Maybe you'll start a new trend and become the figure head of this talent. We'll be sure to look for you on the news. Ha—ha...*

*Anyhow, if you're talking about red boxing….it's pretty much dead. In case you didn't know, red boxing and the like is fairly well know to be quite illegal. We would recommend*

*staying as far away from this type of activity as possible. Ok, that being said, you might want to try Phone Losers of America (http://www.phonelosers.org/) if you want more information on payphones. If anything, it's an interesting website full of strange and amusing information.*

Blacklisted! 411,

I found the latest issue in the Borders Bookstore in New Britain, CT; the same place I bought it off the shelf five years ago. Congrats on your return to the scene! Your magazine was one of the few I missed dearly when it ceased publication back in 1999, and I am glad to see it return; especially since the other "hacking magazine" lacks substance and is uninterested in getting any. This time, a MO will be sent out to you so I don't miss an issue.

My main interests are hardware hacking, telecommunications systems, and radio communications monitoring. (I send occasional pieces to Scanning USA Magazine.) I am working on a few articles along those lines that are more hacker-oriented, and when they are complete I will forward them off for your perusal.

On an interesting historical note, I used to attend the 2600 Meetings in New York City during the early 1990s when Blacklisted 411 first came out and 2600 started going downhill. Eric Corley was all perturbed about this "new" hacker zine that was "copying" him. It was then that I first saw a copy of Blacklisted 411. I examined your periodical and had to bite my tongue because the first thought that popped into my head was "This blows 2600 away." After that meeting, I was having dinner with some of the old-schoolers (TAP-era) who used to show up at the meetings and they all commented on how much better Blacklisted 411 was compared to 2600. So, you can credit your competition with getting you some readers <lol>.

Anyway...best of luck with your return! I look forward to hearing from you and seeing more issues. Best Regards,

**"Berkshire" Tom**
**Routed: Internet**

*Hey man, thanks for the contact. We appreciate your kind words and look forward to hearing from you again. We're very interested in bringing back the hardware hacking aspect of the magazine which is why we've included a couple of project articles in this issue. Our hope is that this will spur a new generation of hardware hackers into jumping onboard, creating new, more interesting project ideas to share with everyone.*

*As for the stroll through history. It's been so long since we first put out a print form version of our magazine that the memories and details of the events ensuing shortly thereafter are becoming somewhat fuzzy - for me, at least. I definitely recall that our return as a print form magazine (or zine) created quite a stir among certain people and organizations. The best part was people from the old days making contact with us and congratulating us for returning to the scene and finally taking the big step from a disk based magazine to a print based magazine. It was an exciting time for all of us to say the least.*

*Nonetheless, we came back and made people notice us. Most of our members, then and now, are old-school hackers (hardware hacking and digging into technology was our thing) which is why we have an appeal to the very old school hackers of yesteryear. We count on the old schoolers being here for us.*

*Additionally, our "newbie friendly" attitude gains us an audience that hardly anyone else out there can compare to. That's right, we go after the new blood! It seems to me that it's terribly short-sighted for others to automatically exclude anyone new to hacking that is truly interested in learning and joining our ranks. Admittedly, there are a lot of trolls out there to wade through, but in the end I think it's worth the effort if only a small percentage of those new recruits actually pan out. Call me an optimist, but I think it's great that the newbies want to join up and share in the fun.*

Blacklisted! 411,

The question that SkyFox88 asked was about the ANAC 955-1122. I have a friend that works for SBC. He told me that that number is good ANYWHERE in California. So I tried it from San Francisco to San Diego; it INDEED does work... peace-out,

**IQ411**
**Routed: Internet**

*Correction: 959-1122. Thanks for checking on it for us. Just for the heck of it, I tested it again. Still good. Enjoy. If anyone has any other known good ANAC's to share, please do so. It's all about sharing the knowledge, people.*

Blacklisted! 411,

In the current issue (Summer 04) on page 10 you gave a guy called Jason D. from San Francisco a list of hacker movies. But in my opinion you forgot to mention one real kickass TV-Series. It is called Bugs ( http://www.bugs.co.uk/ ) and was made from 1995 to 1999.

Maybe you could forward this mail/information to this guy Jason D. - I think it will help him. :-)

Btw: Blacklisted 411 rulez the world. :-)) Keep on working guys - I love your magazine ...Greetz from Austria,

**MacOS X**
**Routed: Internet**

*Thanks MacOs. Thanks for the article you sent in, too. It's been included in this issue. Jason, did you get this information? I'll admit that I've never heard of this TV series before now, but it's not uncommon for people in the U.S. to be totally unaware of TV shows in the U.K. It happens all the time. Anyhow, upon a quick look at the site and doing some additional research, I'd say that "Bugs" definitely looks interesting enough to at least warrant further investigation. As soon as I can find them available here in the U.S., I'll watch them and give you my opinion on the series. It looks like the series only made it through three seasons - typical with anything you happen to like watching, huh?*

*Though, the reader was asking about movies which is why I tried to limit myself to movies alone. If we want to expand into TV series, I could come up with a long list of interesting titles. However, most of them are just cool sci-fi series, etc.*

*After the last issue went to print, I thought of a few more movies I should have mentioned....but didn't. Hey, hindsight is 20/20 according to the experts. Anyway, I wanted to add the following:*

*The Italian Job, 2003 111min (I can't believe I forgot this one - it was a great "heist" movie!)*

*Oceans Eleven, 2001 116min (maybe not about hacking per se, but has a lot of social engineering topics covered - and I enjoyed the movie quite a bit!)*

*Gone in 60 Seconds, 2000 117min (how is this movie hacking related? Beats me. I don't seem to recall. But I do remember liking the movie....so I had to mention it)*

*Catch me if you can, 2002 141min (total social engineering movie—loved it)*

*Paycheck, 2003 119min (I'd have to say it's one of Ben's better movies. Maybe not completely hacking, but worth a look—main character reverse engineers his own destiny with a selection of mundane items. Thought it was very interesting.)*

*And, just for the heck of it. Here's a few movies you should see if you haven't already:*

*Terminator 2, 1991 137min (forget the lame hacking aspect, it's just a cool friggen movie)*

*The Saint, 1997 116min (has some interesting lock picking and fraud scenes)*

*Ok, I think that's about the last of the hacking-related movies I can think of. Anyhow, thanks for the input, MacOS. It's appreciated.*

Blacklisted! 411,

I'm new to the game. I would like to know how to hack with my PDA. Something easy to drive me to learn more. Thank you.

**crippledZero**
**Routed: Internet**

*Ok, hold on everyone. Before you guys jump all over him, let's try to dig into this question a little. I'm going to assume that this reader either wants to HACK the PDA itself or just watched T2 and wants to have a handheld hacking device al-la free money from the ATM of some sort....? Just for the fun of it, let's direct everyone to a few sites of interest.*

*First on the list is PDA Street ( http://www.pdastreet.com ). This one's a no brainer - they have lists of hardware, reviews of hardware and a FORUMS section with a crapload of threads on just about every pda, palmtop and pocketPC out there. You're mileage may vary from subject to subject, but it's worth a look.*

*Next is FireWall Guide ( http://www.firewallguide.com/pda.htm ) - they have a bunch of articles on PDA security. Interesting read.*

*Last is pdaPhoneHome ( http://www.pdaphonehome.com ) - look on their forums and you'll find a lot of interesting threads.*

*Oh yeah, we have an article on PDA security in this issue on page 18 ...just in case you're interested. Ok, so that's it. Do some research and enjoy your PDA. If anyone out there has any specific ideas or material to offer on this topic, speak up. www.blacklisted411.net Thanks*

Blacklisted! 411,

Great to see you guys back after so long. 2 quick questions maybe you can help me with.

1. Do you have any data on BART cards? Im looking for info on the magnetic strip on the back. Is it Hico? Loco? Id like to explore these cards a bit but don't wanna buy the wrong reader/writer.

2. What happened to THUD magazine?

thanks!

**Lint**
**Routed: Internet**

*Unfortunately, I don't have any current information on the Bay Area Rapid Transit (BART) cards or the mag stripe type. However, I read an interesting story on the subject last year. I had to dig a little, but I found a link to it:*

*http://www.pushback.com/Wattenburg/bio/creditcards.html*

*It's about Bill Wattenburg and his role in the whole BART card controversy back in the 70's. I know it's old news, but it's still rather interesting.*

*If anyone has any information to add to this topic, go for it.*

*As for THUD. It went out of print the same time Blacklisted! 411 did (last part of 1999). We have not brought THUD back to the market....yet. Give us time to get Blacklisted! 411 where we want it to be and we'll bring back THUD eventually. It will happen. One thing at a time.*

Blacklisted! 411,

The Tone Dialer on the cover of your summer 2004 issue does not look like the standard Radio Shack 43-146. Is it custom made or is some other company making tone dialers again?

**Jack H.**
**Routed: Internet**

*The tone dialer on the cover of the Summer 2004 issue is a Radio Shack model 43-142. Back in the day, these were easy to modify into a red box. The advanced programming features allowed the user to program many different amounts of coin values. Naturally, the one pictured on the cover is in fact a NON modified unit, capable of doing nothing more than it was originally manufactured for. It was used for nothing more than a prop for the cover shot. Where can you get one of these? Look on ebay. I've seen them there from time to time and they usually sell for about $5 - $10.*

Blacklisted! 411,

Found your latest mag at Borders. Man, I've been waiting for you guys to come back forever. Welcome back! I have a few quick questions for you. I was on IRC and heard of a new underground hacker show called DougTV out in your area somewhere. The guy logged out of the chatroom before I was able to get anymore details. Do you know where I can find it? Do you know if it's any good? Do you know them personally or are you involved with them?

**MetaBawlz**
**Routed: U.S. Mail**

*Sure, I've heard of DougTV. It's done by none other than DOUG and, yes, he's in our area. We know who he is but we don't know him personally nor are we involved with the production of his show. The first episode is available on his site located at the following URL: http://www.dougtv.org Real tough to figure out, I know. Anyhow, I watched the first episode and was mildly amused by the antics. There was actually some gritty-but-good phreaking examples and information in the episode. I thought the intro, music & opening credits as well as the ending credits were very well done. All in all, I think Doug is onto something and hope he continues working with his show. It's worth a look.*

Blacklisted! 411,

I read your article (Cloak & Dagger), it was pretty good. Glad to see the magazine is back. It was easy for me to find where I am, Bay Area coming 'So-Cal' soon. Anyways, I was surprised to see you wrote about Cloak & Dagger from what, I think you said 1984. That movie is based on an older title called, go figure, Cloak and Dagger. I went to buy the movie you were talking about, because I had extra money. Anyways I ended up buying the wrong one, the original. I have to say, it was pretty good. I haven't seen the version you were talking about yet, but the one I saw was classic. The director is Fritz Lang, and it was originally filmed in 1946.

You could look it up at IMDB. It was about WWII spies and nuclear weapons. It had a lot of pretty cool stuff, even if it doesn't still apply to today's world. You should pick it up... If you give me some more info we can swap titles when I come to Southern California. Not sure if that's where you are, but let me know. Oh and it had this really hot girl, Lilli Palmer, but in old fashion styles there was only kissing. I guess it's sexier that way, without all the modern BS, and porno we have nowadays. Well I look forward to your email. If Goldfinger can't be contacted let me know, and sorry to take your time. Thanks for the reading.

**Marv31**
**Routed: Internet**

*Thanks for your input. Your letter was forwarded to Goldfinger.*

Blacklisted! 411,

Hi Guys. I'm thinking about learning PERL and wanted to know if you could suggest any good reading on the topic. I'm interested in links and books on the subject Thanks and I look forward to seeing your next issue!

**AlphaOne**
**Routed: Internet**

*All right. I can respect your need for more information on this subject. You can try any of the following sources to help in your desire to learn Practical Extraction and Report Language (PERL).*

*Books on PERL:*

*Learning Perl, Third Edition*
*By: Randal L Schwartz, Tom Phoenix*
*ISBN: 0596001320*

*Perl Cookbook, Second Edition*
*By: Tom Christiansen, Nathan Torkington*
*ISBN: 0596003137*

*Perl Pocket Reference, Fourth Edition*
*By: Johan Vromans*
*ISBN: 0596003749*

*Learning Perl Objects, References & Modules*
*By: Randal L. Schwartz, Tom Phoenix*
*ISBN: 0596004788*

*Advanced Perl Programming*
*By: Sriram Srinivasan*
*ISBN: 1565922204*

*Mastering Algorithms with Perl*
*By: John Macdonald, Jon Orwant, Jarkko Hietaniemi*
*ISBN: 1565923987*

*Mastering Regular Expressions, Second Edition*
*By: Jeffrey E.F. Friedl*
*ISBN: 0596002890*

*Programming Perl, Third Edition*
*By: Larry Wall, Tom Chrisitansen, Jon Orwant*
*ISBN: 0596000278*

*CGI Programming with Perl*
*By: Gunther Birznieks*
*ISBN: 1565924193*

*Links to PERL sources:*

*Roberts Perl Tutorial - http://www.sthomas.net/roberts-perl-tutorial.htm*

*Perl Tutorial - http://archive.ncsa.uiuc.edu/General/Training/PerlIntro/*

*Another Perl Tutorial - http://www.scs.leeds.ac.uk/Perl/start.html*

*I think that should get you going in the right direction. Enjoy all the reading.*

Blacklisted! 411,

Hello I am a new reader of your excellent magazine, i just had a question which will probably be simple for you to answer so here it is:

I was wondering what computers (or what it is) have the black screen with the cool looking green text, was it just computers way back when or was it a special program? You usually see it with source code, if you still don't know what I'm talking about it is on the cover of a book called "Hacking The art of exploitation" by Jon Erickson. And is it possible to get it back on modern day computers? Thanks, I will always read your mag.

**KnightRider**
**Routed: Internet**

*I think the answer you're looking for is the old monochrome monitors from the early days of computing. Most of the dumb terminals used monochrome monitors. Heck, there were monochrome monitors made for Atari, Commodore, Apple, etc.. You can get the same effect today with any terminal software or just about any program that displays/edits text. Whatever program you decide to use, simply set the background to black, foreground to green and you will essentially have the same effect.*

*Speaking of the book "HackingL The Art of Exploitation", it's a really good book for anyone interested in network security. I enjoyed this book quite a bit. The book provides an in-depth technical look at exploits, including a step by step tutorial on how to write your own exploit code. It's very clear and concise, even for the newbie. It's available for $27.17 from Amazon - well worth the money. Good luck.*

Blacklisted! 411,

Ahlo, friend. Your last issue for the summer was fantastic. Thanks for the utterly informative read. Can you guys help me out? I'm trying to find an ANAC for San Antonio, TX area (210 area code). Also where can I get information on schematics for all colored boxes?

**Jackosama**
**Routed: Internet**

*I have two ANAC numbers available for the 210 area code. They're 830 and 951. Your mileage may vary on these as I am unable to personally test them. Please report back and let me know if these do in fact work. You can also use 800-444-4444. If anyone else has suggestions for Jackosama, let me know. As for the color boxes, you can find schematics and instructions for some of them here: http://www.textfiles.com/phreak/BOXES/ Hope you have fun.*

Blacklisted! 411,

Hi guys, great try. The summer edition is almost worthless to me as I can't read the small type and I got tired of trying to use a magnifying glass. I even copied the pages using "enlarge" to try and read it. If you are going to have a larger print version out for Winter, I'll subscribe. Good luck.

**Dave**
**Routed: Internet**

*Thank you for your input. We get this complaint from time to time - very seldom, though. Unfortunately, there's just not enough of an issue with this aspect of the magazine to warrant a major change like this anytime soon. Doing so would greatly affect the look of the magazine as well as, more importantly, seriously cut into the amount of information we can print in each issue. With all of that said, I'll keep in mind that there are a few people out there with bad vision who have trouble reading our magazine and try to make some changes just for them. Again, thanks for your comments.*

Blacklisted! 411,

Hi guys. I recently picked up your summer issue and have to say I loved it! I can't wait to see your Fall issue. I heard from someone at the local hacker meet that there is a way to get free 411 calls from payphones but nobody could tell me how. Can you get free 411 calls like the old days?

**Spire**
**Routed: U.S. Mail**

*Hey Spire. Actually, yes it is true. Pick up the phone receiver, dial 411, wait for the "deposit" message, briefly hold the hook down (and LET GO) and you'll be connected to 411. It's really that simple. It works around here just fine on the Verizon payphones. I don't have any information on the SBC payphones—whether it works or not.*

Blacklisted! 411,

I was screwing around on the internet doing my daily routine and noticed that StankDawg of BinRev has started up a hacker show called HackTV. Is he working for you guys or something? Has he started up your show again or is it a coincidence that the name is the same as yours? I watched it and thought it was decent. It's awesome seeing more episodes of HackTV again. Laterz

**Hitman**
**Routed: Internet**

*Yeah, I saw HackTV too—it's just a coincidence regarding the name. StankDawg is part of the DDP and not "working" for us. However, he did submit an article on Universal Studios Florida which made it into this issue. Anyhow, I did a review of the show in this issue, located in the "review corner" on pages 30-31. While my overall reaction to the show is somewhat mixed, I think what he's doing is great and support him all the way. I hope he sticks with it. For those of you who have not seen it, check it out: http://www.binrev.com. As a side note, DougTV also had it's debut episode released recently. I answered someone else about it in a previous question, but the URL is http://www.dougtv.org. Check it out too. I think it's pretty cool that so many people are starting up their own underground hacker shows. It's cool to be a hacker in the new millennia.*

Blacklisted! 411,

Hello. You asked for comments and suggestions. Here's one. Start including more tech information, projects and shit like that. The stuff you people used to print. The last issue was really good and had the 411 "feel" but it was seriously lacking in the tech. dept. if you know what I mean. Don't get me wrong. I love your mag to death and I want to see it stay around for a long time to come. Just bring back the good technical stuff back soon.

**German**
**Routed: Internet**

*You'll be pleased to know that this issue will be much like you (and several others who commented) asked for. We've included a couple of projects: one for a DTMF tone decoder project and one for an LCD serial terminal project. Ok, so we've brought back projects like you asked. That was easy More tech information, you ask? Incredibly, we've brought that back, too. Mind you, we don't have BBS lists anymore, but we're including more technical material now and in each future issue. We're going to trim back the social engineering material somewhat, continue to stay away from the politics and try to keep it all about the technology. Just the way hackers like it. Enjoy and thanks for the suggestions.*

*A message to everyone else. Keep the comments and suggestions coming, people. If you don't like something about the mag or want to see something new and you don't SAY anything, how the heck are we going to know about it? Keep it real, hackers!*

Blacklisted! 411,

Guys u rule! BL411 is awesome . Yeaaaa!!! Here my wishes for the future. I hope some of them will be realized:

For the website:
- a kind of hacker board would be kickass

For the zine:
- more technical stuff (hacking releated) on one hand
- and some kind of real hacking stories on the other hand. I mean something like "And then I hacked into that computer. Damn man, that gave me a flash ...". That's always nice to read. Can't await the next issue, greetz

**Skynet**
**Routed: Internet**

*You were one of the voices that made these changes possible. Yep, we've added a forums section on the site. Go sign up and use it! This issue of the mag has more tech info in it. Enjoy!*

Blacklisted! 411,

Hi guys! Nice to see ya back! What about an technical article like some cool hardware hacking (printer, router, phonebox, eg...) in the next issue? Would be great. I really miss those things ...

By the way: Your website roxxx too !!!

**Santa**
**Routed: Internet**

*Thanks for the input, Santa. We've included tech material in this issue. We have an article on hacking a wireless router by MacOS and some do it yourself projects. Enjoy.*

Blacklisted! 411,

I picked up the latest issue and was rather pleased. I'm an old fan, well at least I've been reading since volume 3 This mag still has the BL411! "feel" to it, though it has stepped back a little in technical content (which may be good for first time readers). This is only a small complaint and your product is far better than the stuff 2600 puts out. As long as you continue to publish technical articles with that seedy BL411! feel, I'll tolerate the fluffy stuff without complaint. Thanks for returning to the scene!

**V0lsung**
**Routed: Internet**

*Thanks for your comments. This seems to be the theme of the messages we've been getting lately. I think it's a sign. You're trying to tell us something? Anyhow, we hear ya, we hear ya. More tech material. Done.*

Blacklisted! 411,

Wow...commercialization of the underground....heh... cheers.

**Zenfrequenxy**
**Routed: Internet**

*Is that how you see it? Unfortunately, that is somewhat shortsighted on your part, IMO. We're another voice for the hacker community. Somewhat loud, we not only help the hacker be heard but allow hackers a place to share their ideas and experiences. New or old, all hackers are welcome to participate.*

Blacklisted! 411,

I am a buyer of 2600.com zine, but I must say that your site is very helpful and has a lot of resources and I like how you share the wealth as far as your links to other sites, the other hacker zine has links but nothing like this. I will definitely push for my friends to invest in your zine. See I am starting a newbie club in Paterson New Jersey, and your site would definitely be our source of origin but with your blessing of course. So e-mail me if i have your permission to refer all my new geeks to your data, and yes I know the hacker ethics and I promise no malicious newbie mistakes. I believe in learning to learn and being informed. So holla at me.

**DrEyDaY_35**
**Routed: Internet**

*Hey Dreyday_35. If you want to raise up the Blacklisted! 411 flag at your meeting, go for it. We don't make this as a requirement to start a meeting or to get listed with us. As long as your meeting is hacking related you can be listed. When you have the details of your meeting ready, forward them to us so we can include your meeting in the back of of the mag.*

*For everyone else: If you have a hacker meeting running right now and want to be listed in the next issue of Blacklisted! 411, you need to get in contact with us and let someone know about it. You don't have to be a "Blacklisted! 411" meeting to get listed—as long as you run a hacker meeting, you're a shoe-in. It's important that you contact someone ASAP if you want a listing in the Winter 2004/2005 issue.*

Blacklisted! 411,

So glad that BL411 is back! A little part of history still with us. Great job on the site too, can't wait for the discussion boards.

**GrandpaHackman**
**Routed: Internet**

*Thanks for the kind words. You'll be pleased to know that the forums are up as of the writing of this response. Also, I enjoyed your article on hacking with proxy servers. Go check out the forums: www.blacklisted411.net*

Blacklisted! 411,

Ok first your mag rocks and I been reading it since when it was out before in black and white, but what you really really need here is a forum.. There just aren't enough good hacker forums anywhere anymore, and we need a community! PHPBB or Invision Free would be great.. :) If yer host is any good it probably has the MYSql DB and php support u need.. Add a couple of useful mods and it'd be awesome!

**Al B.**
**Routed: Internet**

*Thanks for the input, Al. The forums are now up. Enjoy!*

Blacklisted! 411,

I was just referred to this site by one of the forums I frequently visit. All I can say is that it is nice to have a magazine that lets you know what is going on in the world of hacking. Just like the editors, I and many others share tons of the same interests and being updated with the latest news and technology is great. Good luck and I will be sure to spread the word. Until next time…

**Sublime Infidel**
**Routed: Internet**

*Thank you for taking the time to comment. Fortunately, the ideals and interests of hackers are common among hackers (of course), electronics enthusiasts, computer users, amateur radio buffs and just about anyone interested in technology in any field or capacity. It's really interesting who we hear from and what they do and how it relates to what WE do.*

*In an effort to help in the cause (sharing our common interests), we've officially started up the Blacklisted! 411 forums which is now in operation at the time of this response. You should sign up and use the site. Naturally, you should spread the word about the forums whenever you have the opportunity.*

*Thanks for the support!*

Blacklisted! 411,

I'm glad to have found your magazine at my local bookstore. I've never seen your magazine before the Summer 2004 issue, but I have to say that I'm very impressed. The conspiracy/social engineering articles was a little on the heavy side in my opinion, however, I understand how it relates to hacking and why you included it. I know I'm a nobody, but I wanted to suggest that you should write more about technical related subjects which would appeal to a larger audience. Either way, you got me hooked. I can't wait to see your next issue. I have only one question for you. What other hacking magazines (or zines) are available, if you don't mind telling me about your competition?

**Greedo**
**Routed: Internet**

*Welcome aboard. I hear what you're saying. We've decided to drop some of the non-hacking related material and focus more on the technical material. We had a lot of response on this subject after the Summer issue was released. It's understandable as we had quite a bit more of the non-hacking material included in that issue - in fact, more than any other issue previously released if memory serves me. Anyhow, suggestion accepted and acted upon. Hope you are pleased with this issue. As for your question, there are several other print hacker magazines available today.*

*2600 - http://www.2600.com This one has been around forever and is very well known.*

*Binary Revolution - http://www.binrev.com/ This is a limited run hacking zine available online only.*

*DIG Magazine - http://www.digzine.com/ This is a limited run hacking zine available online only.*

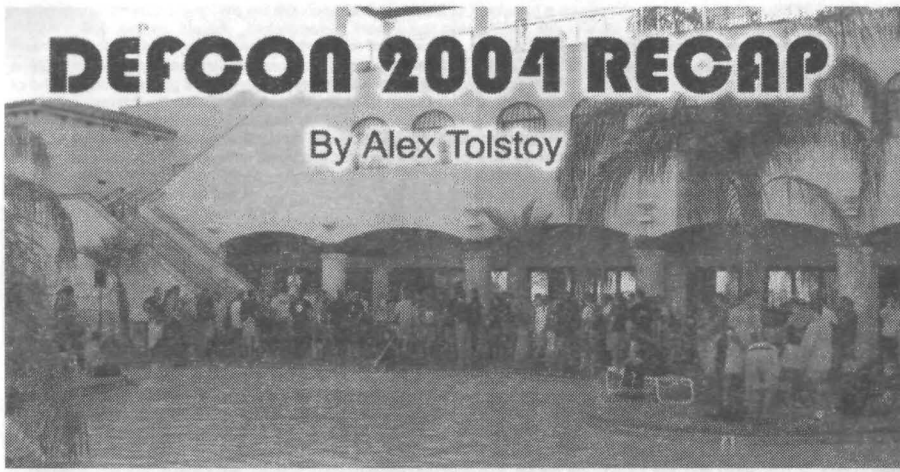
*Nuts & Volts - http://nutsvolts.com This is an electronics magazine, but related enough to hacking to mention.*

*Phrack - http://www.phrack.org This is an electronic hacker magazine (e-zine) that recently made a run of their current issue in print form! NICE JOB!!!*

*Wired - http://www.wired.com This is the corporate voice for the hacker community. Eh….*

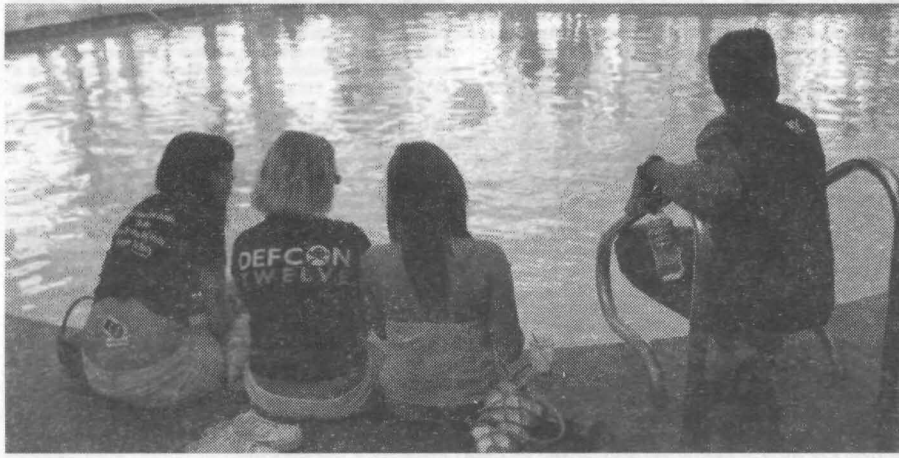
# DEFCON 2004 RECAP

By Alex Tolstoy



**Intro**

This year, I had the opportunity to attend Defcon 12 as a representative of Blacklisted 411 Magazine. I have personally attended Defcon since DC 7 - the first year at the Alexis Park Hotel, where it has been for the last 5 years. It has become a yearly tradition for Hackers, Crackers, Phreakers, Computer Security Specialists, Law Enforcement Agents, and a whole multitude of others to travel to this Hacker Mecca known as Defcon. It never ceases to amaze me how far people will travel to attend this event. I have chatted with attendees from Australia, Western and Eastern Europe, Russia, Japan and Korea. Each year, the convention grows from the previous year; grows in attendance, grows in infamy, and grows in the hype. And this year was no exception.



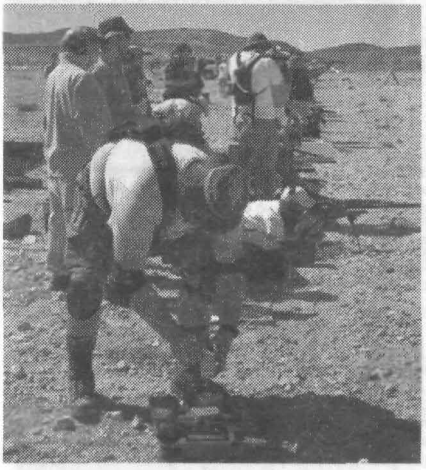

**Parties**

As was expected, Saturday night was *the* party night. First were the pool parties. The Alexis Park Hotel has three pools and there was music playing at each one. The back two pools had full DJ setups and there was a variety of Techno / Industrial / Dance playing till whenever in the morning. At each DJ station there was the usual dancing crowd and people just kicking back, enjoying the music. There were a large number of people in the pools enjoying the music and the scene. At one pool, there was a game involving glowsticks being thrown back and forth with people at each end making quite an effort to catch them—even if it meant going over or around other people. I admit getting sucked into this game and, considering it was still 90 degrees at night, it was a good way to cool off.

A number of groups had parties in the larger rooms in the hotel. The list of parties is too long to name and I don't recall all of them, anyway. I spent time in the Irvine Underground party where Freaky was doing his best to keep the party going and the two strippers that were there didn't make his job too difficult. I then went, literally down the halls, looking for loud music and found another 3 or 4 big parties. Unfortunately, I did not get the name of the people or groups throwing them. By this time, I was getting a little tipsy and headed over to the supposedly biggest party at Defcon; the *Ninja Networks Party*. I would have liked to review the Ninja Networks party, but in the spirit of Elitism they were allowing only people who had their special stickers into the party. Apparently, I was not *Elite* enough. That's ok, I have been promised a pass next year.

The main event for Saturday night was the Black and White Ball. The organizers of Defcon setup an entire hotel ballroom as a big party. It is a themed event with no street clothes allowed. Most people tended towards the gothic / industrial dress, but there were quite a few very original outfits. They had a DJ spinning music and, when I was there, an electronica band was playing. I stayed in there for quite a while and got out on the dance floor a little as I have been known to frequent Industrial clubs in Hollywood. There was something in the air that did NOT agree with my lungs. I suspect it was something in the fog juice the AV Company was using, but I am not sure. I have been exposed to foggers for years and have never had any problems before. However, I have had this problem the last 4 years at the Defcon Black and White, so I don't know. Unfortunately, due to this, my visit to the Black and White was cut a little short. Regardless, I have to say that it was one of the better entertainment events I have attended.

The great thing about Defcon is that it's not just a convention, it's also a Hacker themed *party*. You attend the conferences during the day and party your brains out at night. As with all such things, sometime people go to excess. A few paramedic calls for alcohol poisoning aside, Saturday Night was a blast and will be remembered by many.



**Shoot**

One of the events I look forward to each year is the Defcon Shoot. I own a number of weapons that go bang in the night and the Defcon Shoot is one of the better shooting events I have been to. It is held in a place called the "quarry" which is about 10 miles outside of town. The terrain makes it an ideal place to shoot, surrounded on three sides by hills. I made the executive decision to not man the booth during the shoot to give myself and the others a chance to make it to the shoot.

What always amazes me about the Defcon Shoot is the variety of weapons that show up. It ranges from .22 pistols to the big bore 50 cal rifles. As a California resident, it's difficult to see the larger weaponry in action as most of them are covered by the *very restrictive* states Assault Weapons Ban. One of my favorite pieces was a 50 cal bolt-action rifle brought by Noid, one of the Defcon goons. The round itself is intimidating, saying nothing of the actual rifle. Most of the time, he was firing the rifle with a noise suppressor and, even with that, ear protection was required. When the suppressor came off and the standard muzzle break was put on, the shockwave was impressive. It was definitely felt as well as heard. Others were showing off their AR-15's, AK-47's and a laundry list of other impressive weapons.

One of the coolest (literally) things was the Bus. One of the Defcon Goons owns an old Southern California RTD bus that he got off an auction a few years back. The bus is driven to Defcon each year. The bus is loaded with people who want to go to the shoot but don't want to drive. It's parked just behind the firing line. Those who are done shooting or are not shooters, sat in air-conditioned comfort watching all the action. It provided a well-needed hideaway from the 110-degree heat of the Las Vegas summer.

Unfortunately, the shoot was finished early due to Police Action. Seems someone complained about "explosions" being heard at the shooting site. The first sign of the impending visit was a small helicopter that was hovering nearby. Shortly after, it was followed by a single officer from Las Vegas Metro Police in a SUV. He informed us of the complaint and wanted to know if we were setting off "explosives". While there was some Tannerite (Exploding Targets) in use by our group, I doubt that was what the complaint was about. It seems that there was another group around the bend, in an area considerably more exposed, that was shooting off larger amounts of Tannerite and other things that go boom. Luckily, while the officer was talking to the shoot coordinators, the other group set off a particularly large explosive while our line was quiet. The Officer left to investigate, however he made the request that we should refrain from shooting until he checked out the other group. The decision was made to terminate the shoot as we did not know how long he would take. Of course, waiting in 110-degree heat was not much of an option. Overall, the shoot went very well and, except for it ending about a half hour early due to the Police visit, everyone seemed to have had a great time. Thanks to CHS and all the other range staff for putting on a great event.

**Booth**

As this was the first Defcon since we have resumed production of Blacklisted! 411, it was decided that a booth at DC12 would be the best means to promote the magazine and get out the word. The logistics were daunting, as our promotional staff was pretty thin. It fell on me to man the booth for the majority of the time. With a little help from friends, it all came together.

We were placed next to a group, whose name I think was "Jesus Phreakers". They had a display of several religious books and bibles. They were also giving away mini CD ROMs containing hacking tools, a copy of the bible in electronic form, and several media files of religious sermons. I was not the only person to see the irony of a "Hacker" magazine selling its wares right next to a group preaching Christianity. The concept of distributing religious work with hacking tools raised more than one eyebrow.

While manning the booth, I talked to number of people in the hacking community about the magazine. Almost all were very positive and were glad to see us back in print. The common theme was that they wanted to see more media voices in the hacker scene, less politics from that media (which is one of our core goals), and that the media cover more wide-ranging topics. Most said we were doing just that and it was appreciated.

Some of those I talked to had constructive criticism. I just want to say that such criticism, as long as it is constructive and suggestive, will always be considered here at Blacklisted! 411. We are not so set in our ways that we will not consider it when given. However, as there are as many opinions as there are people in our community, there will always be suggestions that we cannot act upon. This brings us to the few people who had negative comments. Most of those were centered on the "Information Must Be Free" argument, which we are in some way wrong by charging for what we do. I understand that argument, however I do feel it reflects a little lack of realism on their part. I for one do not have the money just sitting in my pocket to pay exorbitant printing fees, or the money to pay people to write for the magazine, or the money to pay my mortgage without working. This is what I do, at least partially, for my living. So, I say that we try to make information *inexpensive*, but it is unrealistic for all information to be FREE.

I would consider the booth to be an overwhelming success. We handed out a few thousand free copies of the Summer 04 issue of Blacklisted! 411, took in a few hundred new subscriptions, and sold hundreds of back issues. This more than covered our expenses in going to Defcon, and allowed us to give a little back to those who helped run the booth. Thanks go out to the Dark Paladin, Fire Opal, and Vicious Chia Pet for helping this year.

**Conclusion**

This years Defcon was, like always, better than the last. The entire DC staff did a good job putting on a event for 6000 hackers from around the world. I look forward to next year. The public relations for the magazine gained from our attendance is priceless. We are planning on running a booth at Defcon next year and I have already lined up more staff to run the booth. And what booth would be complete without a few zine girls? If all goes well, we will be attending a few other conventions around the US, so look for announcements at www.blacklisted411.net.

# Authentication Devices for your Mac

*by Barfbag*
*barfbag@theblankpages.com*

**Forward**

In this article I will discuss how to construct ID cards, usb-key's and an auto logoff solution, which can enhance the balance between security and usability on your machine. Although I will focus on applying these devices and methods to a Mac, it should be trivial to use similar tools to get them working on a unix, linux, or even windows platform. The hope is that by employing these tactics, you will make your security features easier to use and more secure.

**Making Cheap ID Cards**

Personal identity cards have become common in the workplace to authenticate physical security, as well as facilitate secure two factor authentication for logins. I'll show you how you can setup your own system for your home or small office using a printer and less than $50. The system revolves around a barcode scanner which used to be given away to Radio Shack customers and Wired magazine subscribers.

I am of course talking about the infamous :CueCat (yes the colon is part of the name). The :CueCat was given away so consumers could scan advertisement's barcodes which would take them to the advertiser's site. Of course every scan was tracked by Digital Convergence, the makers of the :CueCat. Soon after the :CueCat was released, hardware hacks were discovered which decoded the :CueCat's output. 'De-clawing' the :CueCat is beyond the scope of this article, but there a lot of information on how the hack is performed which can be found online.

How does the system work? Simply, barcodes are printed onto cards which can then be decoded to numbers when scanned. The best part is that the :CueCat works seamlessly by dumping its scan through the keyboard input, meaning that it can be used whenever you would normally type. Here is a list of parts you will need along with approximate prices.

**Items to buy**

| | |
|---|---|
| :CueCat | $3.49-6.99 each, on ebay buy-it-now, already de-clawed |
| USB to PS2 adaptor | $11.99 (needed for Mac, unless your :CueCat is USB native) |
| Laminator | $20.00 4" Laminator |
| Laminator Stock | $4.99 for 100 credit card sized sleeves |

**Other stuff you might need**

Exact-o knife
Old credit card (for tracing)
Index cards
Printer
Paper
Tape

Start by downloading a barcode designing program. I recommend "Barcode Generator" for Mac OSX, which can be found on versiontracker.com. Use the program to encode an arbitrary number using the UPC-A barcode type. Next print the barcode onto an index card. This can be done by taping the card to a sheet of paper which already has the barcode printed on it, that way it will be easy to line up the index card with the spot that the barcode will be printed. Then simply reload the paper and

index card assembly and print again. I cannot be held responsible for and printer malfunctions this may cause, so if you want to play it safe just print the barcode on normal paper, although it wont be quite as stiff. Next, cut the index card to the appropriate size using an old credit card and an Exact-o knife. Laminate the card using the directions that came with the laminator (RTFM). Laminating the card will help protect is, as well as make for a smoother scanning surface. Finally open a text document and scan your card a few times until you get a long string of digits to appear, you might want to do this a few times because occasionally you will get a bad scan.

When done you can set your password to this number and then whenever you wish to login to this account you have only to scan your card. For more security you may want to set your password to the number generated by the scanner + your normal password. Then effectively you have two factor authentication, something you have and something you know. Of course this will require you to enter you password after scanning your card but it will stop people from simply scanning your card and stealing your login password.

**USB Thumb-drive Key**

I have seen many of those little USB thumb drives on the market which can hold anywhere from thirty-two megabytes up to a gigabyte. A few of these devices can even be used as a login key for your computer. Unfortunately, to my knowledge, none support this login key feature for the mac or unix/linux distributions. To fix this I wrote a small perl script which can easily be configured to control access to just about anything using any compatible USB drive. In the default example I have the script set to kill any shell logins unless the key is connected.

Begin by creating a local key file, stored in the root or home folder, and one on the usb-drive. Be sure to set these files to be accessible only by root (chmod 700). The key files can contain anything as long as they match. Note in OSX drives are mounted in the /Volumes directory.

```
# echo "my secret password" > /root/key.txt
# chmod 700 /root/key.txt
# cp /root/key.txt /Volumes/usb_login_key/key.txt
```

Then simply put the key paths into the perl script:

```
#!/usr/bin/perl
# usbkey.pl
# A quick 'n dirty validator
# Coded by Barfbag
# Copyright, (c) 2004 Team Blank. All Rights Reserved
# Anyone is free to modify or distribute as long as credit is given

$USB_KEY_PATH = "/Volumes/usb_login_key/key.txt";
$LOCAL_KEY_PATH = "/root/key.txt";

while(1==1){
    $kill_switch = "0";

    if(-e $USB_KEY_PATH){
        if(-e $LOCAL_KEY_PATH) {
            open(USB, $USB_KEY_PATH);
            open(LOCAL, $LOCAL_KEY_PATH);
            $local_key = <LOCAL>;
            $usb_key = <USB>;
            close(USB);
            close(LOCAL);
        }
        else{
            $kill_switch = "1";
        }

    }
    else{
        $kill_switch = "1"
    }

    if(($local_key != $usb_key) || ($kill_switch == "1")){
        #Violation, Add your actions here
        $status = `killall login`;
    }
}
```

Running the command from root in the background can be accomplished by:

```
# ./usbkey.pl &
```

And thats it. You could can easily script your own actions into the script to make almost any part of your box react to the usb key. All you have to remember is to store your usb-drive in a safe place in order to keep you key private. Better yet format it with an encrypted file system:

<http://www.bsdnews.org/03/cryptusb.php>

**Creating a proxy-log-off with a cell phone**

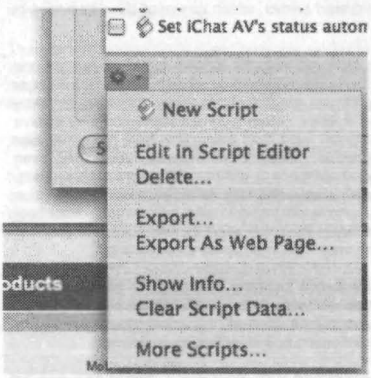
The idea here is to make your cell phone automatically tell your computer to logout when you walk away. To do this you will need the following:

Bluetooth enabled cell phone
Bluetooth enabled Mac
Salling Clicker ($20) http://www.salling.com

For those that don't know, bluetooth is a wonderful short range wireless protocol designed to eliminate wires between computers and peripherals. Using a brilliant program called Salling Clicker (for OSX) you can control your computer from your phone. Salling Clicker allows you to script your own actions that can be executed manually, or triggered by actions like leaving the area or receiving a call. Follow the directions to install and setup the program with your phone and then follow these instructions.

1. In the Salling Clicker control panel click the *Phone Events* tab.

2. Click the small gear icon near the bottom of the panel and select: *new script*




3. Name the script: Logoff when away
4. Right click on the new script and select: *Edit in Script Editor*
5. Delete the default script and replace it with this:

```
on left_proximity()
        tell application "SEC Helper"
                show screen message "Logout" duration 1.5
                ignoring application responses
                        tell application "loginwindow"
                                «event aevtrlgo»
                        end tell
                end ignoring
        end tell
end left_proximity
```

6. Close the script save it
7. Click *Apply Now*, in the Salling Clicker Panel

Although this will not save you the trouble of logging back in when you return, it is a pretty sweet hack providing you have the hardware. It should be noted that this script can fail if you have unsaved documents open when you leave since OSX will ask if you want to save them before you logout.

---

***Barfbag is the admin of Team Blank, a macintosh underground programming team. His texts have been posted on various sites around the mac underground. He enjoys programming and caffeine and can be contacted at barfbag@theblankpages.com***

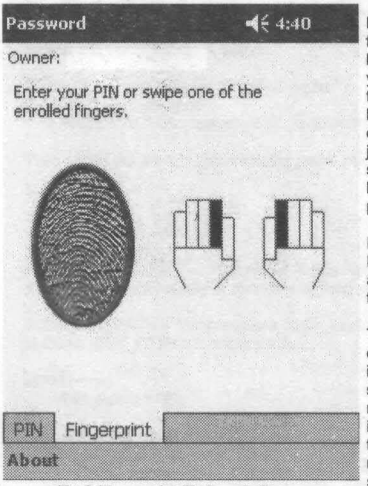
# PDA SECURITY

*By Sam Nitzberg*

Personal Digital Assistants – PDA's are quickly becoming more capable. They are starting to routinely command tens or hundreds of megabytes of memory, have processors in the multi-hundred MHz range, and can communicate through multiple networking mechanisms. With this power comes a variety of security issues. This paper discusses a variety of security issues that relate to PDAs.

**Biometrics**

The 5400-series iPAQ PDAs feature a fingerprint biometric system for recognizing its owner. The way this system works is to have the owner pull his finger across the sensor. The sensor contains an infrared sensor, which can read the differences in heat caused by the ridges in the fingerprints as a basis for user recognition.




**iPAQ Fingerprint ID Sample Screen**

HP actually recommends that you train the system using more than one finger, and I think that this is an excellent practice. Should your finger become injured or damaged, you can still obtain your data. Yes, in theory you could lose your finger entirely. More involved strategies may involve training the system to recognize more than one finger, from more than one hand. If this doesn't provide sufficient redundancy, you could even experiment with toes. If that approach is still not sufficient for your needs, just put the PDA down, walk away, and stay away from me. If you have someone going after you who is prepared to take your fingers from both hands, and toes if necessary – then you need to hire a security team to protect you while you carry your PDA in an armored briefcase.

I would expect additional software involving biometrics to be released for PDAs. This would include software to take advantage of voice-stress analysis models, visual recognition, and all the conventional biometrics that may be used for authentication and identification purposes.

The book, "How to Do Everything with Your iPAQ Pocket PC" has an entire chapter that addresses security configuration and issues for the iPAQ. This chapter discusses built-in security tools, securing the iPAQ, sign-on security, and commercially available products, including signature-recognition systems. I recommend this book for anyone wanting an introduction to these topics, as well as anyone wanting to quickly come up to speed on the use of the iPAQ, and the variety of hardware available to make the best use of a PDA. There are also other related books in the series.

**Cryptography**:

If you have data that you want to keep private, some thought should be given to your cryptographic options. If your PDA is stolen – especially if it has removable media, cryptography may be all that keeps your data secret.

Pocket GnuPG is a port of the Gnu Privacy Guard encryption software. This is intended as a patent-free alternative to PGP (Pretty Good Privacy) software, and is supported in multiple platforms. You can migrate your data between your PC and PDA, accessing it through a single cryptosystem. There are additional options, including a number of commercial systems for cryptography on PDAs, and the decision to use any cryptographic product should balance your needs against the threats your data may face.

**Wireless**

The iPaq 5400 series has built-in 802.11b wireless networking, as do some Toshiba PDA models, and some other Pocket PCs. Wireless sniffing programs such as MiniStumbler (the Pocket-PC version of NetStumbler) are available, and will identify wireless access points, as well as whether or not they are configured to use encryption. If your PDA does not have built-in wireless networking, you still have options available. iPAQ "expansion sleeves" are available that allow the iPAQ to use PCMCIA-format wireless cards. For PDAs that do not take PC (or CF-factor cards), there are also wireless cards now available to occupy the SD ("Secure Digital") memory slot that is often available.

A word of warning about wireless connectivity – it's a two-way street. Once you connect to a network, your handheld may be scanned and probed. Even if your PDA is only going to be on friendly networks, it's not a bad idea to occasionally run a vulnerability scanner such as nessus (http://www.nessus.org) against it.

**Bluetooth**

There are a number of security issues associated with Bluetooth communications mechanisms. These topics include man-in-the-middle attacks, eavesdropping and impersonation, and denial-of-service. A paper referenced below (Bluetooth and its Inherent Security Issues) is a very fun read on this topic.

More commonly mentioned in the media are issues related to Bluejacking, Bluesnarfing, and Bluestumbling. These relate to having a device scan for available Bluetooth devices, and recording data relevant to their, and also describe surreptitious methods for obtaining data from Bluetooth-enabled devices, without authorization or notice being provided to the owner of the device.

**Infrared**

Many PDAs have infrared ports. These are relatively low-bandwidth communications ports using the infrared part of the spectrum. Any PDA that has an infrared capability will also have settings to manage it. If you do not plan to use your infrared capability, ensure that the appropriate settings have been disabled. If you are a member of the tinfoil-hat crowd, you may also want to cover the infrared emitter's/receiver's port with duct tape, or a similar material, capable of blocking infrared.

**Warwalking**

Programs such as Ministumbler (for Windows CE), and Kismet (for Linux), can both be run on Pocket PCs. These programs allow you to walk freely with your wireless-equipped PDA while it records available data (name, MAC address, signal strength, the use or lack of WEP encryption, the location if you have GPS gear, and other related information).

**Virtual Private Networking**

There are a number VPN client products available to load on your PDA to use to connect to your home system (or corporate systems) via encryption. I am not recommending any, but if you want to remotely connect via your PDA to administer or maintain systems while you are away, or to access data remotely, be sure that you have the appropriate crypto in place. The free product VNC (Virtual Network Client) client-side application is also available for the Pocket PC platforms.

**Audit**

I am not aware of any real operating-systems level auditing capability for either Windows CE, or the Linux distributions available for handhelds. As PDAs are used in more and more mission-critical applications, I would expect to see these features appear. Still, if these handheld devices are being used to connect to databases over secured networks, some steps can be taken to perform auditing at the database.

**PDA Phones:**

With the continuing emergence of "smart phones," worms and other security hazards may become a headache. Already, a worm that spreads between phone has been devised; this worm targets phones with the Symbian operating system, and uses Bluetooth as its conveyance mechanism.

A German firm, GSMK mbH - Gesellschaft für sichere mobile Kommunikation mbH, produces the Cryptophone. This is a very-special PDA phone: it uses two cryptographic algorithms (AES and Twofish) to ensure security. Should a flaw be revealed in one cryptosystem, the other still affords strong cryptographic protection. The Cryptophone also uses open-source products, and its source code is available to all. More information is available from the company's web site; the web address is provided below. I would recommend that anyone interested in secure cellular telephony take a look at their web site

The Cryptophone

**The Open Microphone Problem**

Hopefully, no one is out to get you. Depending on how tricked-out your model is, it may have a speaker, microphone, camera, Bluetooth, large amounts of memory, and wireless networking capabilities. You've got a machine capable of recording, possibly storing, and transmitting a significant amount of audio and even video. Show your PDA the respect it deserves - it may be watching you. There are two papers on the Open Microphone problem on my personal web page.

**Taking another Road:**

If you are adventurous, there is another way to work with PDAs and apply your computing knowledge. You can get your hands on a copy of Familiar Linux for your PDA, and install it. You can leverage your knowledge of Unix to securely run client software and applications on your PDA. My iPAQ 3970 with expansion sleeve (which provides support for two PC-cards) serves double-duty as a wireless file server with both a wireless networking card (802.11b), and a 5-Gig hard drive on a PCMCIA card (this is made by Toshiba).

Not to be overlooked are opportunities of running certain key Unix-base network analysis tools – even over wireless networks. Running nmap from a wireless handheld is just plain fun.

**Conclusions:**

Since PDAs are small, convenient, and less-powerful than larger systems, some will grossly underestimate the potential harm that can result if they are lost or have their security subverted. However, there are opportunities for users to protect themselves, and for the manufacturers to craft more security into their systems.

**References:**


Bluetooth and its Inherent Security Issues
http://www.giac.org/practical/GSEC/Tu_Niem_GSEC.pdf
Tu C. Niem

Cryptophone web site
http://www.cryptophone.de/

How to Do Everything with your iPAQ Pocket PC, Second Edition, Osborne McGraw Hill
Derek Ball, Barry Shilmover

PDA Security 101
http://www.intranetjournal.com/articles/200304/ij_04_07_03a.html

Serious flaws in bluetooth security lead to disclosure of personal data
http://www.thebunker.net/release-bluestumbler.htm

Speaker Intent Analysis System
http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220040093218%22.PGNR.&OS=DN/20040093218&RS=DN/20040093218

Worm ready to wriggle into smart phones
http://zdnet.com.com/2100-1105_2-5233517.html

Bluefire Disables Bluetooth and Infrared Device Communication With New Version of Mobile Security Software
http://www.pdatoday.com/more/1505_0_1_0_M/



***Sam Nitzberg is a computer security analyst who has presented and published on subjects relating to information security, information warfare, and technology and society. His papers and presentations have been conducted in both national and international venues, and most recently, he has presented at the Fifth Hackers on Planet Earth Conference in New York City. His website is at http://www.iamsam.com, and he may be reached at sam@iamsam.com.***

# Electronic Surveillance: Introduction by example

A series of articles written exclusively for Blacklisted! 411

**By M L Shannon**

Hal is an electronics technician who works for a medium size company that produces, among other products, machined parts for manufacturers of hard disk drives. One evening, he is watching a movie about submarine warfare in which there are scenes where the sonar operators are able to identify other subs by the unique sounds or 'signature' they make,. This is a combination of mechanical vibrations and noise from the propellers, called 'cavitation'. The signatures of known boats are stored in the ship's computer.

The operator has detected a Russian sub, and is explaining to the eXecutive Officer that not only has he identified it, but that the sub has had some repairs made recently to the propeller shaft and bearings. That alone, that small bit of information is useful in intelligence as there are only so many ports at which the repairs could have been made, it helps track the vessel.

So, Hal gets to thinking about this and comes up with an idea. After searching the Internet he is unable to find any reference to someone having already thought of this - his idea is to design an inexpensive contact microphone - the "hear through walls" type with a small circuit board containing various audio filters and an interface.

*The microphone would be attached to the hard disk drive and the interface would feed the internal sounds of the drive to the filters and then to a specially developed application. When the drive is brand new, the software makes a signature just like was done with submarines in the movie. And as it is used over a period of time, wear on the spindle and bearings will cause these sounds to change. So, if such a device were to be rigorously tested under lab conditions over a period of time, it would be possible to make a series of these signatures, fine tune the audio filters and be able to predict when a drive is about to fail. The savings in preventing lost data to corporate America would make this a profitable venture*

Suddenly, Hal is all fired up and decides to build a prototype. He starts by using a contact microphone that he had amongst his piles of electronics stuff, which is clamped to the drive, and a stock audio equalizer cannibalized from an old stereo. A small Data Acquisition Device, a sample sent by the Dataq Corporation takes the output from the equalizer and feeds it to an RS-232 port my mounting the Dongle inside the tower case. Then he begins testing various applications that will sense changes in the sound over a period of time and alert the user when it indicates the drive might crash.

It seems to work and, encouraged, Hal starts making improvements. Instead of the Dataq, he decides to make it less complicated by feeding the microphone output directly into his Montego sound card. Unfortunately, none of the available applications he has been able to find are suitable for processing and analyzing the sounds. And since Hal is not a programmer, he takes what he has built so far, along with his notes, to work and presents it to the CEO of the company. The boss says he will pass it on to the engineering department for them to determine if it is feasible to produce.

Hal didn't hear anything from the CEO for a few weeks, but there were rumors floating around that the company was going to take Hal's idea and run with it. So, he arranged to see the CEO, wanting to know how much the company was willing to pay for his idea.

The CEO advised Hal that ownership of any such inventions that applied to the company's products, and made by any employee of the company automatically reverted to the company.

Hal didn't believe this to be true; he was not asked to sign any kind of agreement to the effect that his company would have first rights to any ideas or inventions he might create- so he started to argue with the CEO only to be told that the law was behind the company and that there was nothing he could do about it and that if he wanted to keep his job he would forget about his 'fantasies' and get back to work.

Like hell!

Hal decides to fight the CEO and that evening he gets together with a few of his hacker friends to draw up the plans of battle

Since he doesn't know how far the company has gone in building a prototype or whether or not they have consulted a patent attorney, and as several weeks have passed since he made his presentation, it becomes a race against time. He has to find out.

So, together they consider their options. Since Hal has access to most of the entire plant, including the back room where the router and telephone wiring are installed, but unfortunately not R&D lab, they consider several methods.

- Use a surveillance transmitter hidden in the CEO's office
- Tap the CEO's phone
- Install a rogue Access Point in the company wireless LAN
- Intercept the CEO's alpha-numeric pager messages

***

Having read The Bug Book, Hal knows that in the real world of electronic surveillance, it is sometimes difficult if even possible for an operative to obtain the specific information that they need. Other times, it is very easy; it depends on many things.

And, being an electronics technician, he knows how much work is involved in designing and building a transmitter. "Why reinvent the wheel"? , he asks himself and so he visits a local company that makes commercial wireless microphones.

Removed from its bulky housing it, along with enough AA batteries to power it for at least a month in a series/parallel configuration, it fits neatly inside the back of a large picture frame in the CEO's office.

Transmitting on 172.450 MHz it can be received by most scanners, but then there is the matter of recording the transmitted conversations.

This is handled by using a PRO-2006 scanner running RadioMax software from Data Delivery Devices, formerly Future Scanning Systems- it converts the audio to MP3 on Hal's extra notebook computer he keeps in his workshop at the company. So, the entire operation is automated running 24/7 so Hal needs only to burn the MP3 files to a CD after work and take them home to listen to at his leisure.

Hal knows the CEOs pager number and from that, with a little social engineering, is able to find the company that provides his service. A couple hours work and he builds a four level decoder and with a scanner and an old Pentium II laptop, he builds an intercept system. Then he sends alpha-numeric pages to the CEO with a unique string of characters and lets the pager intercept program run in search mode till it finds that string. He now knows the Capcode of the target pager. It takes only a few hours, after which he sets the program to capture every message sent to the CEOs pager and print it out on his home computer.

In the late night meeting with his hacker friends, the idea of installing a rogue Access Point generates a lot of enthusiasm. Everyone agrees this would be not just the coolest way to get the goods on the CEO, but also the most effective.

Probably true, Hal agrees, and while he knows the basics of wireless networking, he certainly is not an expert. So, his hacker friends go over the methodology- how Hal will be able to pull this off.

The first step, they explain, is to use a PCMCIA card on yet another portable computer (Hal only has two, both being used, so one of the girlgeeks offers to loan him one she is not using right now) that has a card with an external connection, and a little 6 dB antenna made by SMC.

While the hackers are working on the details, as well as a case of Heineken, she runs home to get it. While she is gone, the group considers a wiretap.

The phone tap is problematic.

The company has a digital electronic system with muli-line phones and Hal is not familiar with it, nor does he have time to learn.

And even if he did, there is no easy way to string a pair of wires from the CEOs desk to Hal's workshop. So, he would need to use a bug attached to the phone, but with two transmitters operating in the same location it would require the monitoring system, Hal's 2006 scanner, to scan back and forth between the two frequencies. This could result in lost information.

So, that is out.

Girlgeek returns and fires up the laptop, showing Hal how Network Stumbler works and then gets into how Hal may need to

learn details of the company LAN, the router, how many LAN segments there are and which hosts are on what segment. It has been a long night and Hal is getting dizzy hearing about DHCP and MACs and a bootable Linux CD called 'Auditor' so they decide to call it a night.

The woman who maintains the network is a friend of Hal's- they went to college together, and so he will probably be able to get the answers he needs. Tomorrow, he will ask her to have lunch together.
Meanwhile, time to crash.

Over the next few days, Hal used what he already knew as well as what he had recently learned, and went about setting up his electronic tools of self defense.

***

Mills Thomas is a patent and trademark attorney, sitting at his desk, waiting for a client who has an appointment at 3 PM. He knows that this is about a new hardware utility but no more than that and he has never before met the client, the CEO of a local company.

The intercom buzzes- it is his secretary advising that there is a gentleman in the reception area insisting that he has to talk to you right away, that it is a most urgent matter... aren't they all... but Mills still has a few minutes and agrees to see the man.

As he is shown into the office, Mr. Thomas makes the usual observations, first noticing that the man with the frizzy blonde hair and drooping mustache seems upset, nervous ...not unusual for someone consulting an attorney ... Before he get a chance to ask anything, he greets you by name, explaining that an associate had recommended you.

He takes a seat, and opening his attaché case, spills some papers on the floor. Apologizing, he leans over to pick them up, then begins his story. His father, his very wealthy father has recently died and the terms of his will are - well, he explains, he has been left nothing and he insists that the will must be contested…

... he rambles on as he takes a cigarette pack from his shirt pocket.

The attorney interrupts to inform him that smoking is not permitted in the office... ...he mumbles something about quitting and tosses the pack in the waste basket ... and that he is not a probate attorney. "My specialty is patents and trademarks".

He turns and looks at the lawyer, an expression of surprise on his face, and apologizes- explaining that he thought you specialized in probate law.

He jumps out of his seat, walks to the window and looking out grasps the edge of the drape, still rambling on about his damned father until you take his arm and escort him to the reception area.
Where the CEO has just arrived.

Across the street, a few minutes later, the distraught man climbs into a Dodge van parked in sight of the attorney's office window. He removes the yellow wig and with a grunt, tears off the fake mustache. Hal then settles into a chair in front of a fold-down table. On it is an Icom R-8500 receiver and two scanners, each with a cable from the audio output feeding into a notebook computer that is recording the transmissions that the radios are picking up.

When Hal was picking up the papers he 'accidentally' spilled, he placed a transmitter under the lawyer's desk using double sided adhesive. A very special bug once made by International Micro, that has a pre-emphasis circuit. It amplifies the higher audio frequencies to eliminate the 'talking inside a barrel' distortion.

The cigarette pack he tossed in the waste paper basket contained another transmitter, an inexpensive one. When he went to the window, he installed the third listening device; an old Deco Industries UX-50 crystal controlled bug with a hook attached that he hung on the inside of the drapes.

Also under the desk, Hal left behind a cell phone. Not an ordinary type, this one was special.

In the space of ten minutes, Hal placed four listening devices. And now, he is hearing and recording everything being said in the lawyers office.

***

When the CEO was presented with the recordings of his conversation with Mr. Thomas, he was outraged. Hal was told to get back to his job and that he would be called back later. After the CEOs attorneys arrived Hal was called back to the office and advised that he would be prosecuted for violation of various federal laws including but not limited to the Electronic Privacy Communications Act, and the Omnibus Crime Control and Safe Streets Act of 1968. He was then told that even if he were not prosecuted, the tape and its contents would not be admissible as evidence if Hal were to sue. And of course Hal was fired.

Obviously, Hal was able to get what he needed since Mr. Thomas would have asked the CEO a number of questions before he began the complex process of applying for a patent. Such as whether the CEO or someone in his company was the true creator of the product, and if an employee, was a document signed that assigned rights to such ideas to the company.

In legal court authorized electronic surveillance, the operatives can listen for a certain period of time, called 'minimization' but if the intercepted conversation is not directly related to the suspected crime being investigated, then they are required to stop the interception and continue it after a certain interval.

Since Hal's interception of 'wire or oral conversation' was not legal, he was under no such restrictions. And anyway, since his installation was automated, he captured everything. And, indeed, much of what was spoken concerned the theft of Hal's intellectual property.

And the transmitter in the picture frame captured talk of activities that would have been more than a little upsetting to the CEO's wife, had she known about them.

Hal got his job back, along with a nice raise, but the patent matter still had not been settled and again, the company attorneys reiterated to Hal that the information contained in the recordings was not admissible as evidence in court.

Technically, this is true. However. Due to a quirk of the law, under some circumstances, if the contents of the tape are broadcast by a radio or TV station whose programming was intended for the public domain, it may now be admissible as evidence. Even though it was illegally obtained. And Hal has, as he explains to the lawyers, some media connections, including but not limited to some of the alternative FM radio stations. This is 'iffy' and subject to the Judge, and of course to appeal to a higher court, but this alone was sufficient to cause the company attorneys to reconsider. Which they did.

Hal has his own company now, producing the patented device that analyzes the internal sounds of disk drives and alerts the user when a crash is predicted. He has a good life with a substantial income. Enough for he and Girlgeek to live well and later, maybe produce a kindergeek or two.

***

Yes, while it can be very difficult for a spy, or a hacker, to obtain the information they need, sometimes it works out that way. Access to the place to be bugged, availability of the right equipment that will work for the required period of time, knowing how to cover their tracks and avoid being caught (especially true in wireless hacking) and finally, how will the operative be able to use the information obtained through the listening devices to their advantage; whether it is blackmail or being able to have it introduced as evidence in a court of law.

And yes, electronic spying whether it is a bug, a wiretap, a 'special' cell phone conveniently left behind, or hacking into a wireless network, is usually against the law.

And while these laws are ignored, violated on a daily basis by those who have no other way to fight those who oppress them, it is not necessarily morally wrong. So, why should this knowledge, this technology be denied them? when it is readily available to government and corporate America who ignore and violate such laws on a daily basis, and in every single case that the public hears about, get away with it.

---

***M L Shannon is a SF writer, author of several books on electronic surveillance from Paladin Press. ...graduate of a 2 year college in electronics, former countermeasures sweep technician, has been guest speaker and made a few radio and TV appearances...***

# Hacking a wireless router

## by Robert Peloschek a.k.a MacOS X

The today's possibility to download firmware updates for wireless routers from their manufacturer's websites is, as you will certainly see in the following article, a cool thing. You can not only keep your router up-to-date, but also easily have a closer look at your devices firmware. The search for hidden secrets, backdoors and security flaws becomes in such a way a simpler thing.

So one rainy summer evening I took my Apple iBook and started hacking my D-Link DI-624 Wireless Router (Revision B).* My intention was to prove, that even a router, that is secure, stable and reliable (as many computer magazines like "NextGen Electronics" or "Wired Magazine" tell), can easily be accessed without the knowledge of the administrators username and password.

**Examination of the firmware**

I decided to start with a close view into the routers main software. Therefore I downloaded the most current firmware (Version 1.28) from the manufacturers website and decompressed the *.bin file (which contains the compressed firmware in an old kind of ARJ Format) with the Aladdin StuffIt Expander. The outcome of this decompression process was a file called "nml.mem".
Briefly, after I had opened "nml.mem" in a normal text editor I found out that the router works under a real time operating system called "ThreadX" from ExpressLogic. However, there were much more amazing things to find in the firmware. For example, have a look at the following part of the firmware (*Fig1*) and guess what attracted my attention ;-) :

```
[...] ïcreateïïNet access lockïunknown flashïïïrestore def timerïïïNet heap lockïïïlock
NETïïïïunlock NETïïLOGFILE.TXTïNATLIST.TXTïCONFIG.BINïïCHKLST.TXTïïRemote Managment http
ServerïïïïRemote Managment Telnet ServerïïAllow to Ping WAN
portïïdefaultï0.0.0.0ïadminïïïïïïïDI-624ïïuserïïïïDMZ Hostïïïï%02x- [...]
```

*Fig1: Part of the routers firmware*

Bingo, you have it! The four filenames logfile.txt, natlist.txt, config.bin and chklst.txt attracted my attention. I was able to download two of them by simply loading the page *http://ip_of_the_router/filename.txt*. And believe me, that was really simple to find out, cause the administrators web interface can be obtained in a similarly way. The other two files in *Fig1* (logfile.txt and config.bin) were only accessible by the admins password – and that was not what I was looking for. Nevertheless, let us have a look at the two files (*Fig2*, *Fig3*) I was able to download:

```
curr time : 92
0) TCP 10.0.0.138:1723 <-> 10.0.0.140:1024, out_port:60019, last_use:70
1) UDP 0.0.0.0:0 <-> 192.168.0.110:49939, out_port:60016, last_use:38
2) UDP 0.0.0.0:0 <-> 192.168.0.110:49938, out_port:60014, last_use:38
3) UDP 0.0.0.0:0 <-> 192.168.0.110:49937, out_port:60013, last_use:38
4) UDP 0.0.0.0:0 <-> 192.168.0.110:49936, out_port:60008, last_use:37
5) TCP 66.102.11.99:80 <-> 192.168.0.110:56677, out_port:60007, last_use:84
6) TCP 66.102.11.99:80 <-> 192.168.0.110:56676, out_port:60006, last_use:84 [Ő]
Monitor Port1: 1720, m_tick=0
Monitor Port2: 1503, m_tick=0
```

*Fig2: natlist.txt (http://192.168.0.1/natlist.txt)*

*Fig2* shows a part of the file natlist.txt, which contains the amount of seconds the router is up and a list of all open NAT connections.

```
LAN MAC = 00-80-C8-12-62-0C
WAN MAC = 00-80-C8-12-62-0D
F/W = 1.31
Date = Tue, 25 Mar 2004
AR5 WLAN MAC = 00-80-C8-1B-07-71
AR5 F/W = 3.0.0.43A
AR5 Domain = 48
AR5 SSID = RPNet
Watch Dog = 0
Restore Default = 0
```

*Fig3: chklst.txt (http://192.168.0.1/chklst.txt)*

Chklst.txt (*Fig3*) contains information about the MAC-Addresses of the Router, the SSID used, the current firmware version and other stuff.

As you can see, there are amazing things in the firmware, which are accessible for everyone connected to the router via LAN and/or WLAN. Unfortunately, I was not able to obtain more information via HTTP. Therefore, I decided to carry on with a port scan (which would possibly show me some interesting open ports).

**Let the port scanner do the work ;-) ...**

Full of enthusiasm I started the port scanner (or exactly said the port scanner GUI for "nmap") "NMapFE" on my Mac. First, I scanned the TCP ports, and well, the result was not amazing at all - only the regular TCP port 80 was open. After that, I scanned the UDP ports and the result was, as you can see in *Fig4*, damn pleasing:

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-07-16 02:12 CEST
Interesting ports on 192.168.0.1:
(The 19994 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
53/udp open domain
69/udp open tftp
1900/udp open UPnP
6221/udp open unknown
6280/udp open unknown
13120/udp open unknown
Nmap run completed -- 1 IP address (1 host up) scanned in 101.314 seconds
```

*Fig4: Output of the nmap port scanner*

From the six open ports you can see in *Fig4*, especially the open TFTP port attracted my attention. Therefore, I decided to have a look at the firmware again. This time I especially focused on the TFTP related part. I had the feeling that I had overseen something in the firmware before.

BTW: The UDP scan was too much for the router – it completely crashed after the scan of 19994 ports (*Fig4*). To make my router work again I had to disconnect it from the power. Therefore, make a note: If you like to crash a D-Link DI-624 wireless router, just make a port scan. So much about the reliability of the device… ;-)

**Downloading with TFTP**

The fastest and easiest way to find the TFTP related part of the firmware was to do a little search on the term "TFTP" with my text editor. The result of my search was the following lines of the firmware (*Fig5*):

```
[Ö] ÏÏÏÏTFTP Server: couldn't open file
ÏÏÏÏUnknown transfer IDÏFile already existsÏDisk fullÏÏÏÏSee textÏÏÏÏFile not
foundÏÏAccess violationÏÏÏÏÏIllegal TFTP operationÏÏNo such userÏÏÏÏUDP send failedÏUDP
alloc failedÏÏÏÏBad len (too short)Ïshort data from peerÏÏÏÏRcvd unexpected data blockÏÏ
ÏÏÏbogus tftp error textÏÏÏfile read errorÏUDP send failedÏUDP alloc failedÏÏÏÏ Ï ÏRetry
limit exceeded, giving upÏretry limit exceededÏÏÏÏzero length fileÏÏÏÏTransferred %lu
bytes in %u.%u secondsÏÏrÏwÏÏrbÏwbÏÏar5maco.datÏar5eepo.datÏ0x%4x -
%02x:%02x:%02x:%02x:%02x:%02xÏÏÏdbgout.txtÏÏSmurf Attack DetectÏPacket [Ö]
```

*Fig5: Part of the routers firmware*

Again, like in *Fig1*, you can see three different filenames, that seem to be interesting. First, I tried to download them with the common *http://ip_of_the_router/filename.txt* method I mentioned before, but unfortunately, it did not function this time. Then I had a brilliant idea: I thought something like "Hey, that's the TFTP part of the firmware. Let's try to download these files with a TFTP client".

Therefore, I started MacTFTP on my iBook and tried to download ar5maco.dat with it – and boom – the file download did function. (Ar5maco.dat is not very spectacular by the way; it just contains the WLAN MAC Address of the router.)

Next, I downloaded ar5eepo.dat and found out, that it contains some information on the wireless card used in the router (it is an Atheros Communications, Inc. AR5001-0000-0000 Wireless LAN Reference Card). Finally yet importantly, I downloaded dbgout.txt, which seems to be, as you can see in *Fig6*, a debug log of the router:

```
System starting ...
Primary instruction cache 16kb, linesize 16 bytes.
Primary data cache 16kb, linesize 16 bytes.
vtclk = 99532800
clkdiv = 3
Scanning bus 00
Found 00:58 [1282/9102] 000200 00
Found 00:60 [168C/13] 000200 00
```

*Fig6: dbgout.txt*

Next, I decided to investigate the firmware update function of the DI-624.

**Destroying the routers firmware**

Normally the firmware of a router is updated with the routers integrated TFTP server, which can be accessed via a password protected "web interface". However, I wanted to upload the firmware without using/knowing the admins username and password. Therefore, I decided to use the "Send" function of MacTFTP instead of the routers web interface to do a firmware update (*Fig7*).

I was excited when the upload of the firmware started. It seemed that I had prove, that it is possible to do firmware updates without the knowledge of the administrators username and password. But then something strange happened: The connection broke when 99,9% of the upload was done. My first thought was "Damn, I have destroyed my whole routers firmware".

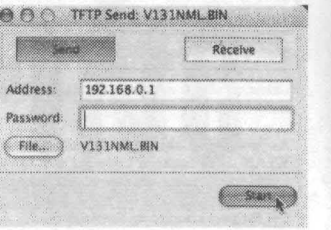
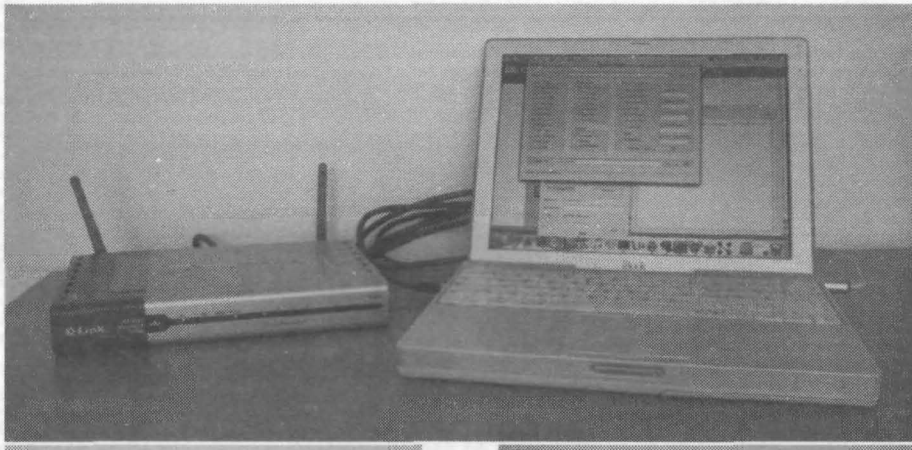
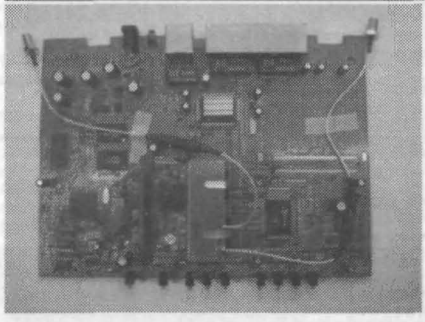


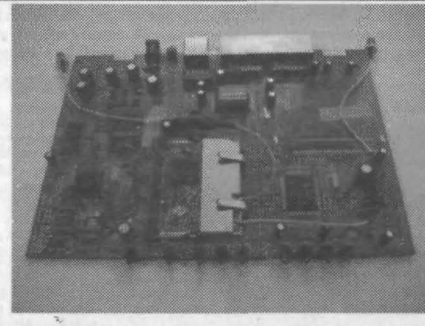

*Fig7: Uploading a firmware with MacTFTP*

Fortunately, as I found out a bit later, not the whole firmware was destroyed. Only the WAN port seemed to be affected by the incomplete firmware update, because every time I tried to access the Internet nothing happened, but the red error LED "M2" on the routers front started to blink. The only way to revive the router was to upload the firmware again with the integrated firmware update function of the router.

I guess that some kind of flag must be set that the firmware upload functions properly (which is only done when the integrated TFTP server of the router is used for the update). Nevertheless, every kiddie with a computer, a WLAN card and a TFTP client can destroy the firmware of the router – and that is a real big security flaw.







**Conclusions**

It is amazing how many secrets and security flaws one can find in a modern router. Without knowing the administrators username and password

- one can simply destroy the whole routers firmware with a TFTP upload
- or download information about the MAC addresses of the router, have a look at the open NAT connections, etc.

Now it is up to you to find the secrets and security flaws in your router at home or anywhere else. Here are some tips for you, to make your hacking adventure a lot easier:

- You will need a text editor with a search function, a port scanner, a TFTP client, and maybe some kind of decompression software (if the firmware is packed).
- Scan the firmware for files with the endings *.bin, *.bak, *.dat, *.db, *.txt and *.htm(l). Often these files contain interesting information.
- A port scan can help you to find interesting open ports.
- Try to download things via HTTP and TFTP.
- Try to upload something via TFTP (Note that this can destroy your routers firmware!!!)
- Finally, you will need the patience and obsession of a good hacker. ;-)

At last, I have to say to all the peeps out there – Keep the Mac Underground strong! Peace.

**Links**

D-Link DI-624 - http://www.d-link.com/products/?pid=6
NmapFE port scanner - http://sourceforge.net/projects/nmapfe-osx/ (for Mac OS X)
MacTFTP - http://www.mactechnologies.com/pages/downld.html (for Mac OS > 8.6)

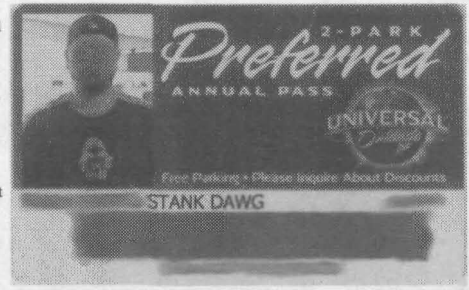
** All information tested twice with the current official firmware 1.28 and the new unofficial firmware 1.31.*

# 0wning Universal Studios Florida

*By: StankDawg@binrev.com*

No, I didn't call this article "Hacking Universal Studios Florida" because this is more or less a list of interesting things you may not have known about Universal Studios. Most of this information came through Social Engineering and repeat visits to the park. This will not tell you how to get free passes, or anything like that. I will tell you some neat little tricks and fun things you can do once you are in! This is a very difficult article to organize, so I thought the best way to do it would be to simply give you a list.

1) First, I should tell you that I have a season pass. This means that I can come and go to both parks (Universal Studios Florida and Islands of Adventure) as much as I want during the year. If this sounds like it could be useful to you, you might be interested to know that they will put any name you want on your season pass! Most people simply don't ask, but when I confronted them with my nickname, they had no problem putting it on the card. The rule is "as long as you answer to it" (which I do). So if you want to cross that line to uber-geek, have a pass like mine.




You can also request that they shoot you with your 2600 shirt or hat on, or whatever else you think of. I have done this on several occasions, and every person was very accommodating of my requests. The only thing they wanted was my face on the card, obviously so they could make sure that it was me using the card. You might be pushing your luck with a profanity-laden T-shirt.

Another tip for annual pass holders is that you get a discount on food and merchandise as well as tickets to the park. If you do not have one, ask someone who does or hook up with me and I will help you out if I can. I am usually glad to hook up with friends at the park. Now, before this sounds any more like a commercial for Universal, I will move on.

2) Single rider lines are the quickest, easiest way to get through those long lines. If you are willing to ride by yourself, you can use the single rider line and jump to the front of the line…well, almost. Also, I have found that you usually have no problem getting 2 or 3 people still able to sit together, so the term "single rider" is not exactly true. If it is a rollercoaster, usually you get stuck sitting next to some sweaty fat chick because there was only one seat left. On most rides or shows, however, it will pay off big time. If you have more than 2 or 3 people, you are on your own.

3) Express Pass was a computerized system to reserve a time for you to come back and get in line. When it first rolled out, it was AWESOME! When you scanned your pass, it would give you a ticket with time on when to come back and you could go straight to the front of the line. Basically, it held your place in line for you. Well, problem one was that the estimations were very short in the first rollout. We were able to get tickets that were basically immediate! It would give us a 5 or 10 minute time to come back for a ride that had a 2 hour line! Once you got out, you could go right back to the machine and get another ticket and ride again in another 5-10 minutes! They put a stop to that quickly and added a limitation that put an automatic limit of at least a 1 hour wait. So our next step was to get a ticket for the first ride, then go to the next ride while we waited and get another ticket. We continued this throughout the park. By the time we got all of our tickets, we came back to the first ride and started the nonstop ride frenzy. This was also put to a stop by setting in a time limit on how many tickets you could have outstanding. Why am I telling you about stuff that doesn't work any more? I want to save you the time of bothering with this waste of technology. You will thank me.

4) Lockers are scattered all over the park to store your belongings in while you ride. This sounds like a nice idea, right? But the deal is that they are free for a certain amount of time. They estimate the ride wait and give you 1 hour (for example) to put your stuff in a locker while you wait for the ride. If you don't get back in time to get your stuff out, you get charged to reopen the locker. So besides this little underhanded hostage tactic to get your money, it still may be a useful thing for some people to have so I hesitate to reveal this logistical nightmare. I hope none of you abuse this, but I will let the information be free and hope that you don't use it to be an ass.

The simple premise upon which the lockers work is flawed. You go up to a touch screen and request a locker. The computer automatically assigns you an available locker number and prints out a pass code (6 character, numeric) for you to access that locker later, when you return. When you are ready to pick up your belongings, you again go to the touch screen and enter in your pass code and it will electronically unlock the correct locker. If you are thinking of brute forcing the password, you are thinking the wrong way. It would take quite a while on this manual system. Yes the potential exists to accidentally guess a valid pass code, but again the odds are very low. If you haven't seen the flaw, allow me to explain. You see, the act of assigning the locker to someone first, allows the potential for someone to have a locker assigned to them, and then walk the hell off! That one locker is now locked forever! Actually, I found out via social engineering some of the managers that the park resets the lockers every night, but you would still cause a log jam at the lockers for that day. By repeating this pattern, a malicious person could create probably the world stupidest and most low tech Denial of Service attack!

5) One of my mottos is, "See a button, push it". I like to push buttons and see if any of the set decorations or parts actually does anything. I have never found any that have any little hidden "Easter eggs" in them, so if someone does, please email me. I saw this particularly cute girl on the Spider Man ride in IOA pushing furiously on a console of flashing buttons at the Spider man ride. I asked her what the buttons do, and she informed that even those buttons did nothing. She was just bored to tears and pressed the buttons just for the pure boredom of it. One game that I do like to play is to watch out in all of the sets and backgrounds for the rides if I can spot any payphones or computers. The line on Spider man has an interesting room full of desktop computers that are all running a spider man screensaver. I got the impression that they were all running the same TV feed and no actual computers were running. Those of you who

know me realize that I couldn't resist and I crawled over the divider and checked. The "computers" were apparently just props, and were all glued, right down to the keys on the keyboard. I couldn't be 100% positive but I suspect they monitors were just dumb terminals, or even more likely, just video displays looping a recorded tape.

6) As you can tell, employees there can get really bored from sitting in the same place, doing the same job all day. They are ripe for Social Engineering. Flirt with the girls, even the ones that you don't find attractive, to get information. Ask blunt straightforward question of employees, they are usually so happy to have anyone talking to them that they will tell you anything! I started flirting with this young lady at one of the rides and she started going through the computer that holds all of the pictures, and showed me some on the funny pictures that were in the computer of people on the ride. They pass the time by looking through the pictures of hot guys and girls on the ride. This is how those pictures of flashers on the Disney rides sneak out! (As a side note, the software that they use looks exactly like the kiosk software used in those Wal-Mart photo kiosks.)

7) Yes, but Stank, how do I 0wn the MIB (Men In Black) ride? I get asked this question more than any other. Ok, I really never get asked that question, but there are a couple of things you can do specifically on this ride to impress the chix0rz with your mad L337 skillz. The MIB ride is an interactive ride, like many at Universal Studios, that has you ride in a little ship where each of the 6 people have a gun in front of them to shoot alien targets. The special effects on this ride are less than special, but I guess they want you to be able to see where you are shooting. First of all, hold the trigger down. It makes it a lot easier on your finger and makes sure you get off the most shots possible. Secondly, aim for the eyes of the aliens. I have not been able to confirm this, but I think you get points for hitting the aliens in general, and I think you get more points for the eyes. You will notice them turn from green to red, so you should move on to another target. Another hypothesis I have is that you get more points for shooting the other teams ship. You will be going through the ride with other ships at the same time. Each ship has a target above it that causes the ship to spin and make it harder for them to shoot. I suspect that you get big points for that as well. Finally, the biggest way to get phat points on this ride is to RTFM, or in this case LTFM (Listen To…). The speakers are very faint, but if you listen closely at the beginning and quit fingering up the equipment, you will hear them tell you to press the button when you see the big alien boss. That would be the big red button sitting right in front of your non-observant self. At the end of the ride, press it when it flashes and you will get a mad 100,000 point bonus. No one ever does this and you can 0wn them and brag about your mad Counter Strike abilities. It is also possible that this button gives points at other points during the game, but I don't think so. If anyone finds more, come to www.stankdawg.com and let me know.

8) Wi-Fi is available for certain events. Not to the public, but for employees and vendors and such. On the way in from the parking lot, we passed a bunch of laptops sitting out with people trying to lure you into signing up for free credit cards or season passes or whatever else they are trying to sell. The first thing we noticed was that they had no network cables, indicating wireless. A quick check showed the presence of a wireless network with the appropriately titled SSID of "universal" which was WEP encrypted. Since we were there to ride rides, and have fun, we decided to leave that adventure for another trip. Once inside that network, who knows what kind of fun stuff can be found.

So, that should give you tons of fun things to do at Universal Studios (as if you didn't have enough already). Please don't use these tricks and be a destructive jerk. Just have some fun, learn how the system works, and tell them Stank sent ya!

Shoutz: w1nt3rmut3, Mr VTEC, dual_parallel, mi hermana, and everyone in the DDP!

---

***StankDawg is a senior level programmer/analyst who has worked for Fortune 500 companies and several large universities. He has been published in several printed magazines and numerous websites. He is founder of "The Digital DawgPound" (the DDP) which is a group of white-hat/gray-hat hackers who produce their own printed hacking magazine, radio show, TV show, and other projects at http://www.binrev.com/. "The revolution will be digitized"***


**Ok, so we're getting back into reviewing hacking related items again. Several people have suggested ideas and submitted material for us to check out and to comment on, hoping to make the items known to the rest of the community. So, with no further adieu, here's our review content for this issue of Blacklisted! 411.**

**Voice Changer**
**Classification: Tool**
**Cost: $249.00**
**URL: http://www.vikingint.com/voice.htm#a**

I've had this thing for almost three months now and I've been enjoying the heck out of it. It has several settings to "alter" your voice. I have a deep voice, but through this thing, I can have a nice high pitched voice or an even lower voice. I've checked out many of these things over the years and this is by far one of the better ones I've had the opportunity to test out. I can tell that it's of better quality if not alone for the fact that it does NOT have the annoying "whistle" usually accompanied by such devices. That's always kept me away from wanting to keep one of these around. In fact, it appears to work quite well, built very solid (metal case) and seems to have no real limitations that I can speak of. It's very easy to operate and runs on a simple 9V battery. This guy has an "acoustic" coupler which means you don't need to plug it into a phone to use, you simply place the speaker over the mouthpiece of the phone. A nice touch, but I would rather it have the capability to be permanently mounted to the phone, as well. The distortion level is pretty much next to nill—good thing!! From what reading I did, the unit also circumvents voice stress analysis? Don't know what that is? We'll have to do an article on it, then. The item is a little on the pricey side, but anything this good is worth the money. Anyhow, I find this unit to be absolutely top notch and give it a full recommendation to anyone.

**Terror Cell**
**Classification: Book [Unreleased at time of review]**
**Cost: Unknown**
**URL: http://www.terrorcellbook.com**

A new novel by author Erik Giles, Terror Cell pits an ethical computer hacker (the good guy) up against a couple of real bad dudes from the Middle East bent on doing what they do best—wreaking havoc. Filled with excellent writing style, incredibly well thought out characters in a very believable situation -and- unusually correct technical descriptions, Terror Cell is a great example of the kind of writing the people here at Blacklisted! 411 find to be intriguing. The technical aspect was notably accurate and nicely done. Exhilarating and satisfying, this new novel is worth your attention. Get your copy of Terror Cell right away, you'll appreciate the book.

**HackTV - Episode 01**
**Classification: Video [Underground]**
**Cost: Free**
**URL: http://www.binrev.com/hacktv/**

Several people recently told me about the fact that someone had done a pilot episode and then produced an official episode of a new show by the name of HackTV — yes, the same name we used for our in-house show back in the early days. This is done by the same people who produce Binary Revolution. Good, they're expanding. Not knowing what to expect, I downloaded a copy from their website and watched it right away. I was excited to see someone picking up where we left off so long ago. I was surprised it took so long, however. Anyhow, I watched the entire 30 minute debut episode with excitement. The episode has segments on wardriving, hacking your car, Wanco Message Director hacking (labeled "roadsign madness") and a segment on urban exploration bringing it to a close.

While I love the idea of the show, I'm not sure I can give it two thumbs up. Let me go through the episode and explain. First off, the War Driving segment was cool, informative and somewhat interesting....BUT the video shots in the car, while it was moving, was almost painful to watch—the shaking was unbearable. The hacking your car segment was nothing more than filler in my opinion. I couldn't believe what I was watching—swapping out the intake of the stank-mobile? Reminds me too much of the low rider truck craze of past times and the current muffler craze still going on today. Aaargh! The hacking angle was a stretch, but fine... I kept watching it. The next segment was an "anonymous" submission which included a fairly detailed representation of someone accessing a Wanco Message Director control box (you know, the portable message boards you see on the freeways and streets from time to time while they do construction) and entering in their own message. Given the material and the way it was portrayed, it was definitely "blackhat" in nature and I cannot approve of it. Blackhat puts the hacker in a very negative perspective which works against everything we're doing to bring the media into the know that hackers are not bad. This is a tragedy for all hackers. However, with that said, it was still interesting nonetheless. The last part was about urban exploration. A little dry, but it fits into the social engineering ideal, so it's appropriate subject matter. I fully support the concept of exploring your surroundings!! All in all, I thought it was a good show, though somewhat out there from time to time. When you have a chance, check it out and support these people as much as possible.

**4 Channel DTMF to RS232 DTMF Decoder**
**Classification: Tool**
**Cost: $104.00**
**URL: http://www.dschmidt.com/dtmf.html#4CH_DTMF**

A great little item brought to us by Dschmidt Technologies, this 4 channel DTMF decoder is useful in any number of ways. Most notably, decoding DTMF from 4 different sources simultaneously! If you're big into radio monitoring or have a need to keep your own phone line monitored, this wonderful piece of gear gets the job done. Running on anything between 7—24VDC, this decoded does it's job...very well. All of the decoding is pumped out through the RS232 port to your desktop for recording or to a terminal, your laptop, etc. And, yes, this little sucker will decode not only the standard 0-9 tones, but also the ABCD#* tones as well! How's that for cool. The inputs are exceptionally sensitive and pulls down tones easily. Each input is shared among a coming ground. Accordingly, you'll need to isolate each input if your audio sources do not already share a common ground. This is somewhat of a drawback that isolation isn't already included, but it's still a useful device. Check their site - they have other DTMF items for sale!

**8255 PC Interface Card**
**Classification: Tool [Available in kit form]**
***Cost: $49.00-$69.00***
**URL: http://www.boondog.com/**

What I have here is the "ensemble" version of this product made by Boondog Automation. I was given an evaluation unit to look over and comment on a couple of weeks back. I decided that it was finally time to break this sucker out and see what it can do. First, I need to mention that the applications manual is not only HUGE, but it's also well written—if you subscribe to the RTFM mentality, you'll appreciate this one! I'm also impressed with the quality of the build, as well—very nicely done, high quality. The manual shows you with fairly clear detail how to connect this device up to motors (DC and steppers), relays, transistors, LCD's, keypads as well as A/D and D/A converters. Within no time, I had this unit up and running (it requires an 8-bit ISA slot) which makes hooking it up to old PC's a snap. Finally, another good use for that old 486 laying around. Yeah, don't you still have some old 486's in the closet?

I had the unit controlling a bunch of mock traffic lights we have... that was kind of cool to see. I decided to lug it (and the computer it was installed in) home with me and rig it up to an X10 controller to see if I could make it control some of the X10 devices at the neighbors house across the street. I've been wanting to mess with their X10 stuff for months now—as soon as I realized they had X10 crap operating over there. That was somewhat amusing, but I cut the experiment short when my conscience started nagging me. It was a successful test. Why'd I do it? Because I could. No other reason. Do I need one?

Anyhow, something I really liked about this unit was the fact that all of the control lines and voltages (+/- 12, +/-5) are brought out to the small expansion board outside of the PC. It makes the process of expanding upon this device just that much easier. In addition, the people who designed this unit, so graciously opted to use standard plug in IDC connectors. If we decide to do something with this later on, this simple fact will make the hack much easier on us. I hate dealing with DB connectors that most of these controllers tend to have. So, I was pleasantly surprised by this discovery.

To bring this to a close, I think the 8255 PC Interface card is a great little device and fairly inexpensive for what you get. It's top notch, high quality merchandise with exceptional documentation and decent software to boot. Try this out if you've been wanting to get into home PC automation. It's fun. It's interesting. It's within the means of most people. Enjoy.

**Binary Revolution**
**Classification: Zine [Limited Distribution]**
**Cost: $5.00**
**URL: http://www.binrev.com/magazine/**

I first experienced this hacker zine back in mid 2003 with their 1.1 May 2003 release. A copy was dropped on my desk and I thumbed through it very quickly, thinking to myself, "cool another hacker zine!" It took me a couple of weeks before I actually sat down to read it. When I finally took the time, I was pleasantly surprised with the read. The information is fresh, on topic and in your face. Their articles are well written and the accompanying artwork is done quite well. I did some research and found that this was a publication done by DDP (Digital Dawg Pound) and it's available online only through their website—they are not available in your local bookstore. Since their debut issue in 2003, they've release two more issues: 1.2 and 2.1. 2.1 was released at the recent HOPE conference in NYC in July and was well received from my reports.

Their frequency of publication is unknown to me at this time, but appears to be somewhat sporadic, which is common in the hacker community. They obviously subscribe to the whitehat/grayhat hacker code of ethics and attempt to spotlight the hacker in a good way. This alone gets them my full support and respect. I don't have a copy of their latest issue, but the first two issues are well done and worth the $5. But don't take my word for it, go check them out, spend the $5 on a copy of their latest issue and decide for yourself. You may be pleasantly surprised.

**Phone Manager Plus**
**Classification: Tool**
**Cost: $79.99**
**URL: http://www.spygalaxy.com/phonemanagerpl.htm**

So, my last birthday rolled around and someone bought this little gadget for me. When I first saw it, I thought to myself, "oh boy, a caller ID box—they sure don't know *me* too well, do they?!" I stuffed it away and forgot all about it—sorry Jason. As it happens, I was going through my junk recently and came across this small device once more. For some reason, I decided to read the box...and then it hit me! What I suddenly realized was that it was *much more* than a caller ID box. What comes off as a simple Caller ID box, is actually a full fledged phone call logger—incoming and outgoing alike. I hooked it up and did some initial testing of the device. It keeps track of outgoing calls, up to 15 digits on any outgoing call made, in addition to the time the call was placed and the length of the call. That's so cool. The best part? It stores up to *2000* calls AND you can password protect the device to keep people from deleting information (ie: your kids, cheating girlfriend, etc). The price is a tiny bit on the steep side for the a logger, but it's decent, does the job well and I recommend this great little piece of plastic to anyone needing to spy on the outgoing calls in their home or business. It's fairly useful.


***By The Goldfinger***

*Have you ever saw a dumpster and wondered what kinda cool stuff might be lurking within it?* Has it ever occurred to you that companies and businesses throw away tons of stuff that is still in good condition, *sometimes still new?* Apparently, many people are into dumpster diving for fun and profit and a whole subculture has sprung forth from this odd endeavor.

Now, some of you out there are probably thinking, "ha, I know all about dumpster diving, but I wasn't looking for re-usable junk." You see, there are 2 types of dumpster divers. The hobbyist variety which includes all serious and legitimate dumpster divers, and then there's the Darkside Divers. I myself dabbled in the Darkside of the Dive in the early 90's. Professional carders and identity thieves are well aware that many banks and S & L's have little or no security on their dumpsters, and those receptacles of supposed trash are often full of private confidential information. Information that can be pieced together allowing one to open or empty bank accounts, harvest credit card information, and all manner of shady activities. (shudder)

We will not be focusing on the darkside divers, because that's not cool and its illegal so instead we will focus on dumpster diving as a hobby and as a means to save money, and salvage useable items. We will examine all the ins and outs of this activity. Aite then, throw on the Sanford & Son theme song, strap on your diving snorkel an lets dive in!

Definition: **Dumpster Diving** is an active search for what others have thrown away.

Dumpster Divers are people who search for things that other people have thrown out that are still useful, can be recycled, and have value.

Obviously, this activity is not gonna be for everyone, but it has become quite popular and is considered a great resource by many people. Living in 2K4, we kind of make the 1980's reputation for excess and waste look frugal, so I don't think we should look down on anyone that finds a way to utilize that "waste".

Not only do dumpster divers pick up stuff from the curbside, but they also dive into dumpsters at apartment complexes and behind shopping centers. Diving can be profitable in areas where aluminum cans have return deposits. Of course, your not gonna get rich doin it, but there is money to be made. Lots of the stuff you can find can be sold at rummage sales, pawned or sold for scrap.

NOTE: In case your not to bright (and that can't be the case if your reading this fine magazine!), dumpster diving has *absolutely nothing* to do with ACTUAL diving! You don't climb up on the side of the dumpster or on a nearby wall and *dive* into the dumpster. There are no judges, and doing a swan dive into the dumpster is a good way to split your wig!

The "diving" is metaphorical. Most people don't actually get in the bins. They have some sort of long pole which allows them to just lean over the dumpster and pull the items up to them...which brings us to the gear you'll need:

**Equipment**

Most divers use some kind of grabber stick. The best grabber stick according to the "Dumpster Lady", is the Unger Nifty Nabber. You can take a look at the Unger (or "Felix" as folks call it on the message boards) here: www.ungerusa.com
LM Colker Supply is a good source for 51" Ungers. 19.95 + s/h.

Identify yourself as a Dumpster Diver and get a discount! Contact them: 800-533-6561 or email info@lmcolker.com

You'll also want to bring the following gear:

Gloves

Flashlight (varies; I suggest going during the day as there is plenty of light)

Box cutter

Pocketknife

Dirt clothes (clothed you don't mind ruining)

Old towels

Trash bags

Duct tape

Duffel bags

Car (preferred but dumpster diving can be done without a car for storage)

Durable pair of shoes or galoshes

Wet wipes and Anti-bacterial gel are a good idea, were talkin' about dumpsters afterall.

It couldn't hurt to bring a small First Aid Kit either…

**How do I get started now that I'm equipped?**

Folks, d-diving is not rocket science so don't make it harder than it has to be. For most peeps the hardest part of any endeavor is getting up the nerve to do it. Start out by scoping out prospects.

Do a few "drive-bys" looking for likely dumpsters. Look for dumpsters that are free-standing and not the compactor variety. Compactors are those large dumpsters that are attached to buildings with a chute and have no visible openings. Steer clear of those. Apartment and office complexes have definite possibilities. There is loot to be had. Enclosures are ok as long as their not locked. If you happen to have bolt cutters, this wouldn't be a problem, but I don't recommend it. Your best bet is to stay away from locked enclosures.

Now that you've scouted, and found some good prospects, park your car grasshopper, walk over and look inside! Its that easy.

**Where should I dive?**

You can dive retail store, office, and residential dumpsters. Most folks choose to dive retail from what I gather. Any store that sells stuff that you want can be a good place to dive. Grocery stores, bakeries, and health food stores are by far the most consistent producers. You can find something almost every single day at these stores. Yes, I mentioned food stores because many people dive for food too. Personally, I wouldn't do it. But I bet it's a good skill to have and be able to do in the case of Armageddon for example. Or if the landscape of America was suddenly transformed like it was in Dark Angel. Dumpster diving for food would be about the most important skill to have, but since that's not the case yet, I'll stick to Arby's and Haloburger.

According to the **Dumpster Lady**; (excerpt taken from her site)…

*"Yes, some of us really dive for food. If you keep an open mind about this, food diving can end up making a huge difference in your life. Many of us get to the point where we just don't want to deal with any more nonfood "stuff". Then, we start thinking about diving for expendable items*

*The first day I dived for food, I had just been IN the store buying marked down 1/2 gallons of orange juice for $0.50. While I was doing the rest of my shopping, someone came with a cart and loaded up all the orange juice into a shopping cart. So, I hung around to see what happened to it. They wheeled the cart out and threw scores of gallons and 1/2 gallons of orange juice away...that were still 2 days from their due date. They were pasteurized. They were still cold. It was winter, so it was cool. I went to the dumpster and grabbed as many as I could carry. This experience was life changing for me. Where would you draw the line? Would you not buy the marked down OJ? Would you take it out of the guy's cart if he were a few feet from the dumpster and asked you if you wanted it for free? Would you take it out of the dumpster?*

*We food divers tap into the sad fact that we're throwing away 96 BILLION pounds of perfectly good food into land fills each year in this country. By EPA estimates, we're spending $4.8 BILLION a year disposing of that perfectly good food."*

Well, she makes a pretty good argument and she does have a point. Still, *that* aspect of diving isn't gonna be for everyone. If you want to talk more about it with a real pro, she's happy to answer your questions if you have any:

TheDumpsterLady@aol.com

**When to dive?**

Every diver has their own preferences. Some divers try to discover when stores take out the "trash" and wait for those times. This can be accomplished with a bit of pre-text calling.

Others simply wait till the stores close, but its really up to the individual. Some people don't want to risk being confronted, so they wait till later after the stores close. A lot of people, especially women divers, like to take a buddy. Having a partner can be an asset to assist with larger finds, and to act as a lookout, but most importantly, to have back-up in case of trouble.

**What to do if someone sees you…**

Were talking about *people you know*, and *people you don't know*. If you worried about people you know seeing you, then maybe you shouldn't be doing it. Some people care a lot, but still want to do it. According to them, it does get easier over time. They say that in time, you simply won't care anymore who sees you do it. If you got a rep to protect, your best bet is to dive far from home so that you don't run into anyone. Simple enough.

Now as for the people you don't know, were talking mostly about store employees. Evidently some of them can't stand divers, but most employees will just pretend they don't see you.

If someone asks what your doing, just say, "I'm looking for boxes". And be prepared to drop whatever your carrying. If your asked to leave, just say "ok" or "yes, sir", there's no reason to challenge an employee or cause drama. The dumpster is still gonna be there later when everyone's gone home, and its still gonna be there tomorrow, and the next day, and so on.
Don't cause static. If your asked to leave and never come back, then leave, and never go back.

If you do, its trespassing. Remember, there's a million other stores, and tons of stuff so don't even trip. Also, don't think you can circumvent this whole problem of potentially being confronted by asking permission to dive. This is usually a mistake and will usually be met with a NO. And once your told no, you can't legally go back. Asking permission is a mistake.

**Ninja stealth tactical diving**

Don't pull your car right up to the dumpster. This is like waving a giant flag over you that says "*Hey, I'm illegally dumping crap in your dumpster!*" Park away from the dumpster and stroll up to it. Approach quietly like ninja. Do not make noise. Night dives and early Sunday morning dives when many stores are short staffed could work to your benefit. Do not linger around.

A typical dive should last no longer than 5-7 minutes. To maximize the number of dumpsters you can hit in an outing, keep each dive at about 2 minutes. The longer you hang around, the better your chance of being confronted.

**Diving Buddies**

If you don't want to go alone, try to convince a real-life friend or family member to go along.
You can try to advertise for a buddy in your area using one of the AOL message boards or on the **alt.dumpster** newsgroup on the internet. Some divers are strictly loners though, and might not want to buddy up even if they live in your area. Some of these people have spent a lot of time developing their sources and they don't necessarily want to share them with others.
Dumpsters can end up getting locked if too many people start rolling them.

**I came, I saw, I got nada...**

Look, just cuz you went a couple times and didn't find anything doesn't mean your "unlucky" or your not good at it. Newbies often get discouraged their first week or two out because they didn't find anything or they might have checked a dumpster once or twice a week and got nothing. Heres what you should be doing:

* Look every day, or almost every day
*Persistence Pays
*Find dumpsters that are consistent providers
*Zen; become one with the dumpster, develop a "dumpster sense"

By looking daily or on a semi-regular basis, you will begin to discover the stores "toss-out" cycles and you will begin to recognize these patterns and know when to dive.

Not everything is in plain sight. Ya gotta poke around in there. Remember, your not gonna find cool stuff every time, but if your consistent, you will begin to see your efforts pay off.
All the pros say not to get discouraged, just keep at it.

**Legality**

The **first** thing you should do is find out if dumpster diving and scavenging are legal in your town and county. Diving is illegal in a few towns and counties.

You can try to call your local cop shop and ask. Most divers choose to call from a pay phone so as not to identify themselves to law enforcement

Often local law enforcement is not always aware of the exact laws. They might tell you that diving is illegal when the divers know for a fact that it isn't. Do your research.

Be respectful, and don't trip out. Don't ever dump your own trash in someone else's dumpster -- that's *always* against the law. If it says "No Trespassing", then don't. If a dumpster or an enclosure is locked, don't mess with it. Its not worth the hassle.

If you find that it's illegal in your area, then dive outside the city or county limits.

Obey your local laws an you'll be ok.

**Can I really find stuff? Will this really SAVE me $$$?**

A lot of veteran divers swear you can. They say if you stick with it, you can find more than you and 10 other families can use. There are folks out there that are practically supporting themselves off dumpster diving alone. The key is being frugal. And I guess that's what appeals to most of the people involved in this activity. Use the money your saving on things like college, home ownership, investments, retirement. Almost anything you could ever need can be found this way, and a lot of stuff you don't need can be sold or traded, so therein lies the profit the money you save from not having to buy certain things. All in all, in sounds like a interesting hobby and I bet it can become quite addictive.

# MY AMIGA IS STILL TICKING HOW ABOUT YOURS?

## A few more resources for your Amiga

***By MobbyG***

Unless you've been under a rock or been busy getting spyware and virii out of your Win XP box, you may have noticed that the Amiga has made something of a comeback, with the release of the Amiga OS version 4. Granted this comeback is small in scale and isn't going to bring back the glory days anytime soon. But it is remarkable enough that many die hard users and past fans now have hope for our beloved platform, while others are convinced that the Amiga they knew, is gone forever. To them I say, please keep your mind open. You never know if you may be surprised by something in the future.

This version of the OS is to take the Amiga into a new age in the spirit of the old Amiga, but is very different from the classic we know and love. For one, the Amiga has left behind the custom chipset that gave it the power it enjoyed in the old days. Now it's based on a Power PC chip and the ability to use "off the shelf parts". But it's still capable of emulating 68K cpus for older software so we don't have to say goodbye to our favorite applications and programs. Hell, if I still had my Kindwords floppies, I'd be using that instead of some M$ program to write this.

Anyways, here are some sites, lists and resources you can check out for info on the new OS4, what's happening with it now.

Mailing Lists

**http://groups.yahoo.com/group/amigaone/ :** This group is for talking about the new AmigaOne. The new motherboard that was released as the newest generation of the Amiga. This is a pretty active group and has lots of info on past problems and fixes.

**http://groups.yahoo.com/group/AmigaOS4/ :** This group, as you might guess from the name, is for talking about the new OS4. Even though it's still a pre-release, aka beta, it's still proving to be just as versatile and powerful as the classic versions of the OS.

Websites

Many of the sites I would recommend were already listed in the last issue of BL411. So I'll simply skip the descriptions and just give you a quick and dirty laundry list of the two I visit for most of my news.

**http://www.amigaworld.net & http://www.amiga.org**

These 2 sites constantly have up to date news and info on current happenings and news of interest to the Amiga community. If you don't visit these sites, you may be missing a lot. This is not to say the other sites are not any better or good enough. Just that these are the sites I like and recommend to anyone who asks me about the Amiga.

Software

I think it's pretty safe to say that no legacy platform has more software for it than the Amiga. And a good smattering of it can be found on Aminet. I would take down my Cnet BBS just to surf this site for literally hours to read and peruse the latest stuff uploaded during the week. This is quite possibly the best archive of software for the Amiga, post Fred Fish.

Hopefully this will get you a little fired up to dig out, dust off and fire up your old Amiga. Be it a 1000 or a 4000. There is still life to this platform and I hope to show you that starting with my next article. Till then, *"Make Mine Amiga!"*

'nuff said.

***MobbyG is also known to radio listeners in the Rapid City, SD area as Rich Lawrence, on Classic Hits! Q92.3 and their sister station Star 106.3. When not on the radio he's been known to play on his ham radios and runs a telnet BBS called Amiga-Z. MobbyG is also married with one daughter and another child on the way in May.***

# The Hacker Chronicles

An accounting of the life and events of a real honest to goodness old school hacker.

**** A series of articles written exclusively for Blacklisted! 411 ****

***By Cactus Jack***

Inspired by the recent re-discovery of Blacklisted! 411 magazine and at the request of my wife, I've agreed to write a quasi-autobiography of some of the goings on in my life that relate to hacking <both directly and indirectly>, from as far back as I can recall. Amazingly enough, I recall everything from the time I was a few months old up until right now, thirty some odd years later. Very few people have a memory like mine, but those who do should use their gift to teach, instruct and entertain others. If anything, simply detailing experiences and providing a lesson in history would be more than adequate in helping the cause. With this in mind, I intend to detail as much of my life as possible, noting the many hacker related experiences I've had. I hope you enjoy the read.

**The very early years**

Like many old time hackers of today, we tend to have started our careers early on in life. Apparently, I was no exception to this general rule. According to my parents, I was a "very curious baby". They had 7 kids before me, so I figured they knew what they were talking about. I didn't cry much — I was a happily curious baby — but rather focused much of my energy on trying to get into anything and everything I could, leaving a wake of pulled apart toys and misplaced items behind me. Many of my early life photographs depict a kid wanting nothing more than to get into the thick of it. I was especially adept at taking things apart by the time I was only a year old, utilizing my fathers tools whenever possible. This was a serious problem for my family, yet they couldn't seem to stop me. It wasn't for lack of them trying to, either.

I routinely checked out the television, stereo system and heating/cooling systems in our home. Naturally, I had to make control adjustments as often as possible and note the resulting changes made. I was specifically interested in the television and how so many things and people could be inside of it. I recall having the most impossible to overcome urge to take these things apart, but there was no way I could manage to do it covertly as too many people were around to witness it and to *stop me*. I filed it away and decided to tackle these items at some later point in time.

It wasn't until another couple of years passed that I moved on from taking everything apart (and terribly upsetting whomever owned whatever I took apart) to being able to put things back together again. This made the task of learning from my parents belongings much easier since they were usually none the wiser that I had taken their stuff apart in the first place. That television continued to evade my attempts to be dug into, however.

I was somewhat distracted by our telephone, though. This ominous looking device, connected to our wall with a long wire, ringing every so often and containing voices of people I knew (my older bothers, babysitter, etc) perplexed the shit out of me. I took it upon myself to play with this thing as much as possible and soon found myself understanding how to place calls to people. I spoke to people I didn't know, had conversations with the operator and loved every minute of it. My conversations usually went something like this:

Other person: Hello? (sometimes, they'd answer with "so and so speaking")
Me: Hi
Other person: Who is this?
Me: Jack
Other person: Who?
Me: JACK
Other person: Oh. Why are you calling me Jack?
Me: I'm just pushing buttons.
Other person: <laughing> Oh. How old are you?
Me: I'm three.
Other person: Three? Where are your parents?
Me: At work / At the store / At wherever, etc
Other person: You shouldn't be playing with the phone Jack.
Me: I know. They told me that.
Other person: You should listen to them.
.....etc, etc.

Most of the time, they'd just keep talking and talking, trying to get me to either hang up or to agree to not call again. Nobody ever hung up on me surprisingly. Sometimes, mostly if it was a woman on the other end, they'd happily talk to me and tell me things about where they lived and worked, their kids names and things you wouldn't normally think they'd openly tell you about. At least, not today anyway.

I loved calling the operator to no end.

"OP-ER-A-TOR speaking, how may I assist you?" — every single time without fail.

The operator, she was so easy to get a hold of, with a single flick of the dial. I say "she" because when I was three years old, in my hundreds of calls to the operator, not once did a male operator ever answer the other end. The operator was always super nice to me and always seemed to have a good sense of humor about me calling them. Further, she always appeared

to know who my parents were, or at least my father, by name. I figured at the time that my dad was just a really popular guy and everyone knew him not knowing they could trace calls back to the owner of the line. The operator is the person who, ultimately, was able to answer most of my questions about the phone, how and why it worked. The first question I had was how she got into my phone exactly and more importantly how she was able to get back out. Of course, I was laughed at, but she graciously took the time to explain things to me. It didn't take long for me to understand the phone quite well. Before I knew it, I was an expert phone user.

My phone calls to the operator became somewhat well-known among the operator pool and I started to get a reputation. I didn't know this or realize it until my father mentioned it to me one morning while we had breakfast. While I was gobbling up my cereal, he explained that he was aware I had been making a *lot* of calls to the operator and that he was told about it, but I wasn't in trouble for it. He wasn't mad at me, just slightly amused by what I had been doing without his knowledge. He told me that I shouldn't let my mother ever catch me doing it because she wouldn't be as understanding about it. I agreed to be careful and not let her catch me. No problem.

While making my rounds dialing random numbers one day, I found that if I got a busy signal <and did not hang up> I could hear other people pick up their phones — no doubt to dial someone else. I'm not sure why I just didn't hang up when I heard the busy signal — maybe it was because I had no idea what it was, but I knew it meant I wasn't going to get someone on the other end. However, while I was listening to the "funny sound" as I referred to it as, I could hear "clicks"...click.... Click... click....click.....click... "dammit, why do I have a busy signal!!" I suddenly heard someone say. The man continued to pick up and hang up, getting more angry each time he did it. Eventually, three or four other people were doing the same thing. I just sat and listened, quite entertained. Naturally, I assumed I was the cause of their discomfort and was not about to hang up that phone!

After awhile, I started to get bored and I decided to say hello to someone when I heard them complaining into their phone. The other person, a lady, was surprised she heard someone and asked me who I was. I complied and told her who I was without thinking of any consequences for doing this. She *knew me,* and more importantly, she knew *my parents*! She asked me what I was doing and I told her I was listening to my phone. I don't think she knew I was the cause of her problem, but she told me I was too young to be on the phone and asked me to please hang up. Before I had a chance to say "Ok" someone else had joined into the conversation. Anyhow, to bring this topic to a point, before I hung up the phone, there were maybe three others speaking to each other, identifying themselves and then asking each other if they had any idea what the heck was going on with the phone. After a few minutes of this, it just wasn't fun for me anymore so I hung up. I picked it up *again and there was nobody on the line, just a dial tone. Oh well.*

Over the next few months, I tried this a many more times and always got the same results. It provided me with much entertainment.

I was awaken fairly early in the morning one day by the sound of heavy machinery working just outside of my home. I wandered to my window so I could see what was making all of the noise. All I could see were some big trucks with huge spools of wire and a lot of people wearing orange clothes. After I had some time to wake up and ask if it was ok to go outside and see what was going on, I headed straight to the first orange clothed person I could find. I bombarded the man with several questions, mostly wanting to know what was going on. He explained that they were installing a new traffic signal for the intersection. I then asked if I could have any of the leftovers. He agreed to let me take anything from a specific pile. I ended up with a massive pile of wire by the time the installation was complete a week or two later.

I watched them install the control box for the traffic signals and asked questions. I also paid close attention to how everything was hooked up. The guys must have thought it was cute or funny that I was so interested in what they were doing or maybe they needed some cheap labor. Either way, they immediately put me to work. They had me "test" the *push to walk* buttons for them. It wasn't much, but I sure was excited to be part of what I perceived to be a massive undertaking. I was able to get some free tools out of it, too. All I had to do was ask and they handed over some of their old tools. This was the first time I received something I saw as worth a lot just for asking. This was a big deal to me and helped mold me into who I am today.

By the time I was four years young, I was gathering up heaps of materials from our garage, the junk drawer, the neighborhood trashcans and from anyone who had something I thought was "interesting" and I stored all of my choice items in my backyard. By interesting, it usually meant that the item was some sort of technology. Back in those days, technology wasn't anything like it is today; we didn't have home computers or anything *really* cool just yet. However, there was plenty of wire, switches, air conditioning controls, lights, etc. If it was available for free, I had a few in my collection.

I had no idea what I was going to do with all of this junk, but I couldn't stop myself from collecting it. Day after day, I would troll the neighborhood and bring back my treasures. Eventually, my search expanded to tools, lumber and hardware (nails, screws, etc).

One early weekday morning during the summer, just before I turned five, I found myself at a neighbors trash heap, overlooking a dead television they intended to *throw away*. I had finally found myself something substantial to bring back home and tinker with. Back in those days, all televisions were huge. There was no way I was going to be able to move this thing, no matter how big I was for a four year old. I ran back home, picked up a few choice tools, trotted back and proceeded to disassemble the television as much as possible before the trash man showed up. After maybe an hour of hard work, I had myself a metal chassis with tons of tubes and wires. I had never seen a tube before this day. I was pleased with myself and what I had picked up for the day. I happily added it to my collection.

My collection continued to grow, week after week. So, my birthday finally came along. I turned five, had a decent birthday and got some TOOLS. It was the best birthday ever.

Shortly after my birthday, we moved to the other side of the city, close to a golf course and the foothill area. Before we made the move, my parents decided it was time to rid themselves of my collection in the backyard and proceeded to take everything to the dump. I was extremely unhappy about this predicament and began to have a fit. However, I was appeased by an offering from my father. He promised that once we made the move, he'd give me their old stereo complete and working. I agreed and shut up.

We made the move, I got my stereo and I was thrilled. Ok, so I was in a new place and quickly made some friends (Jason, Jeff, Steven, Michael and his brother Troy—yep, still remember them). With some friends handy, I began to explore the area and found my way into every crack and crevice of my immediate surrounding. You know, the normal things a kid back then would do. In fact, back then it was fairly normal for a 5 year old to go roaming around the neighborhood without any cause for alarm.

Anyhow, within the first week I was there, I was sitting on the front lawn and saw a huge airplane <maybe 6-8f ft wingspan> slowly moving down my street. I hopped to my feet and quickly ran up behind it as fast as I could. I followed it closely, looking it over as best I could without touching it. It sped up and eventually took off, me chasing right behind it the whole time until it was in the air. Then I stopped to watch it fly around. I was convinced a small animal or creature of some sort was operating the plane—you see, I already figured out people couldn't shrink themselves to get inside of small devices and it was clearly too small for a person to fit into it. So, I diligently watched this place fly around for maybe 15 minutes and the then it came back down, landing on my street again. Once more, I was right on top of it. It sped up, slowed down, turned around the corner...I kept up with it no matter what. The noisy contraption finally slowed down to a crawl and an older man came up to me and the plain, laughing vigorously. He was obviously the owner of the plane. I had a zillion questions for him. It was that day I learned about remote controlled devices. I was truly amazed by this concept and the idea further intrigued my curiosity.

One day a few weeks later, I got ahold of a butter knife and I had this great idea of taking apart a *frog* I had just captured from a puddle of water which crept under the sidewalk next to the front door of my home. Instead, along the way to the awaiting frog, I noticed the doorbell button on the wall and after a quick eyeballing of the button, I decided it was ripe to be investigated a little more. I proceeded to pry the button off with the knife (and my wet, froggy hands) to see what was underneath. What was about to happen, I hadn't conceived in any way. I managed to get myself a pretty good jolt! This was a pivotal point in my life as I had never known about *electricity*. That small shock opened up my mind to more questions than I ever had previously.

Yeah, I know. You're still thinking, "Take apart a frog with a knife? Are you disturbed or something?" What can I say, I was a five year old boy. Anyhow, due to my new found engrossment, I decided to release the frog back into the puddle. Accordingly, he readily swam away. The frog had survived the day.

When I had a chance, I explained to my parents what I had done and asked them to explain to me what it was that I felt and why I felt it. They failed to explain to me how and why it works, but what they did tell me was that "electricity" was what I had felt and that everything around the house — the television, the stereo, the lights — all ran on electricity. Whoa! I had finally made a connection between everything. I immediately asked if the phone ran on electricity too? YES. The car? NO, not exactly. Ok, but I was getting the idea.

Now I was *really* interested in things. There was no stopping me from that point on.

In the next installment, I'll take the reader on a tour of my experiences from age five on up through my early teens. Hope you're enjoying the accounting of my life thus far.

# SERIOUS SALVAGE - PART IV

## THE ART OF LOCATING QUALITY SALVAGE ITEMS

**By TechnoHeap**

Greetings fellow collector. This is the fourth and most likely the final installment of an ongoing article on the subject of locations where one can find awesome deals on components, equipment and parts.

I have been collecting, buying and reselling integrated circuits (otherwise known as "chips"), electronic parts and equipment since the early 1980's. In the time that I have been doing this, I have grown to know first hand many sources who deal in LESS THAN WHOLESALE priced chips, computer equipment, electronic equipment and parts. That's right, these items are available for pennies on the dollar and this is literally, not figuratively speaking. Some of the things you will be able to find at rock bottom prices: Intel, AMD, NEC and DEC gold chips, MacIntosh computer equipment, EPROMs, EPROM programming equipment, vintage computers, chips, parts, newer equipment, computer parts, brand new excess inventory chips...the list goes on and on.

Have you ever wondered about those $300 - $400 Intel C4004 chips for sale on ebay and wonder to yourself how much you could get them for if you knew the sellers source? How does $40 per POUND sound to you? It takes quite a few of these chips to add up to a pound, so you can see the potential. The going rate for "gold" chips is in the range of $20-$45 per pound and you can buy this stuff all day long at those prices... IF you know where. The sources I will reveal generally don't care what the chips are, only their bulk value. This is where a person with the right knowledge can make a killing regarding resale of the same items.

I've seen these sources come and go by the dozens over the years. What few of these sources remain have been a very well kept secret among the few in the know and to my knowledge, nobody has ever revealed these sources in an all in one information article before. What is about to be revealed to you isn't "fluff" like a lot of other informational articles or those "e-books" provide, you know the ones *that claim they're going to reveal wholesale sources to you and you end up finding out it's just a bunch of useless, and I use this term* loosely, information. Anyhow, the information I will provide you with is specific hardcore rock bottom priced sources which other people use to obtain the parts they resell - even EBAY sellers! You can use this information right now and make money immediately! Furthermore, it won't break your wallet to stock up on some parts for immediate resale....or collecting.

I'm officially out of the chip/equipment collecting/buying/selling business and since this highly secretive information no longer serves my needs, I'm going to spill the beans once and for all which will allow a whole new generation of collectors and entrepreneurs to access the massive opportunities us old-timers have had all to ourselves for decades. Are you ready? Be sure to check out each and every single one of these places and BUY, BUY, BUY as much as you can -- stock up and resell until you're blue in the face. Don't forget where you got this information, either -- a simple letter to Blacklisted! 411 telling them about the great deals you've found for yourself will do. I'm going to be listing salvage yards, obscure retail locations and swapmeet sources. These are all worth the time to visit and explore.

**ACP (Advanced Computer Products)**
**1310 E. Edinger Avenue**
**Santa Ana, CA 92705**
TEL (714)619-3487
Email: dfreeman@acpsuperstore.com
URL: http://www.acpsuperstore.com

Type: Retail/Surplus/Excess Inventory
Contact: Dave Freeman

This is probably one of the first electronic stores I ever visited as a child. It was 1975 or 1976 and I was thrilled to see this place for the first time. It was by far, the biggest computer/electronics store I had ever visited at the time. Yeah, back in those days the retail store was much larger than it is today. They've downsized so many times, I lost count. Each time they did, I was witness to the auction/sale/whatever when on when they got rid of the excess. I walked away with excellent deals and stocked up my own personal warehouse with great parts for so-much-less-than-wholesale-prices. Like clockwork, I used to visit this place almost weekly to see what other great deal I could find. I missed one downsizing but I was there for the aftermath. The leftovers included massive amounts of rapid rack shelving, the wood for the shelving, cardboard parts bins and lots of hardware—screws, nuts, spacers, etc. I had to fil my truck up three times to get everything—and it was FREE!

A few downsizing's back, a few days before the downsizing actually happened, I was in the retail store looking around. I was interested in buying a lot that day because they had an incredible amount of connectors available. I talked to a guy named Jeff (I believe—he's no longer there) and I asked him out of curiosity how much he wanted for the entire surplus area in the store. He said, "give me $700 and it's yours." I know my mouth dropped open when he said this. I quickly closed my mouth, thought for a second and asked him, "$700??" He confirmed what I thought I had heard and said, "Ok, so you want it?" Naturally, I agreed to take everything on the spot. I couldn't give him the money fast enough. He and a helper started boxing everything up for me and helped me load up my truck. It took four trips to get everything. When it was all said and done, I had scored one of the biggest parts purchases to date.

So, they've downsized and downsized so many times over the years, the retail store has shrunk down to an itty bitty place. Keep in mind that they still have a good amount of surplus available, so give 'em a visit.

Ok, so what about now? First, most of their good surplus isn't located in the main retail area any longer. A few months back, they had a couple isles of surplus on the floor and a wall of component cabinets stocked up with common and uncommon chips. It was still fairly impressive, though nothing like the early days. Anyhow, the surplus is now located in the back warehouse and the HUGE warehouse they maintain across the street (Edinger). Many people have no idea that ACP has the large warehouse directly across from their retail store.

When you visit the retail, you must ask to either look at the surplus in the back or try to arrange a time to visit the surplus across the street. The stock in the warehouse is impressive. Not only do they store the bulk of their surplus, but they maintain the *biggest* stash of I.C.'s that I've ever seen in one place! Apparently this is their bread and butter business (ACP Components). They have great prices and a wonderful selection. Don't let the retail space fool you because there's a lot more to them than meets the eye. Armed with the little bit of information I've given you, there's no reason you can't go there right now and pick up yourself a great deal on some excellent surplus parts. Go visit them today!

**Mark Capps (AKA Big Dog)**
**1842 Chrysler Dr**
**Atlanta, GA 30345**
Email: catfishh@bellsouth.net

Type: Scavenger/Broker-Online
Contact: Mark Capps

This guy posts his parts list on the usenet all the time. He appears to cater to the arcade groups, but his list of parts is somewhat impressive—a lot of hard to find parts and good prices. When you have a second, check out a Google search for: "Mark Capps" The guy can be slow from time to time because he seems to go on trips often, but he is a good supplier. There's no phone number available for him, so you're going to have to email him. If you can't email him, find someone who can email him for you.

**eBargain Electronics**
**2720 S. Harbor Blvd #G**
**Santa Ana, CA 92704**
TEL: (714)444-4934
FAX: (714)444-4936
URL: http://www.ebargainelectronics.com

Type: Retail/Surplus/Salvage
Contact: Hamid

This is an interesting place. I never heard of it until a few years back while I was driving from another surplus place. Nestled in your standard business complex, this small place packs a lot of good junk. Set up like a retail store, you walk into this place and immediately realize it's a salvage/surplus store with shelving all the way up to the ceiling. If you like old tech, go to this place. The prices vary from excellent to OH-MY-GOD-YOU-WANT-HOW-MUCH for that old 2400baud modem? If you run a production company and need time sensitive computer/electronics props, this place is for you. Neatly organized, the shelving has just about anything you could want—modems, KVM's, wall warts, o-scopes, eprom programmers, eprom erasers, lab kits and what have you. I've picked up so many good deals at this place in such a short time, I really have only good things to say about them. It would be easy to grab up some equipment at this place and quickly turn it around on ebay or your own website. I know, I've done it. This place is worth the visit, people.

**R-Vac Electronics**
**23684 El Toro Rd. #O**
**Lake Forest, CA 92630**
TEL: (949)586-1210

Type: Retail/Surplus
Contact: None

I've been to this place a few times and usually find a good deal each time I visit. I don't have too much information on this place, but I'll give you want I have. When you walk into this place, the first thing you'll notice is how incredibly stuffed and disorganized the place is. It used to be a normal retail electronics store some time ago, but with all the closing of the other electronic stores from the 80's on up, this place managed to get ahold of more stock than they can effectively display in an organized fashion. So, they have heaps of junk everywhere! If you dig, you can find a lot of good stuff here. I picked up several small piles of goodies for a few bucks each time. Disregard the notice in the front that says more or less, "No Deals". They'll deal just fine.

**Marvac Electronics**
**2001 Harbor Blvd**
**Costa Mesa, CA 92627**
TEL: (949)650-2001

Type: Full Retail/Surplus
Contact: Gene

There are maybe 6 of these stores left in the chain. This particular one happens to be the one I've visited the most. Ok, so this place is one of my old stomping grounds. They always have a lot of surplus goodies in the back "surplus" section, they have a table on the other end near the parts counter which has piles of stuff that used to be on the shelves—marked down to MOVE. Further, they have little grab boxes all the time, anywhere from $2.99-$6.99 (buy more of them, get price break) which are stocked up with vast amounts of surplus parts that used to be part of their retail stock. The best part of those grab boxes is that they usually contain at least one or two items worth 10 times the price of the whole box. I always pick up a few of these because it reminds me of the grab boxes Radio Shack used to sell way back in the 70's when they actually catered to electronics hobbyists—anyone remember that? Anyhow, I've picked up tools, chips, displays, switches, lights and more all for great prices. The cool part is that they maintain a HUGE warehouse of parts that nobody knows about or has ever been to. However, the dad who owns the chain just passed the biz on to his kids, so things are changing. If you want access to great untouched stock, go to this store, talk to Gene and tell him that you want to visit the warehouse and he'll hook you up.

**California Electronics & Industrial Supply**
**221 N Johnson Avenue**
**El Cajon, CA 92020**
TEL: (619)588-5599
TEL: (866)225-3532
FAX: (619)588-0371

Type: Retail/Surplus
Contact: None

I found this place while search on ebay for some parts one day. I ended up bidding on and winning a massive amount of chips at a typical price of $0.99 per auction. After I won everything, I decided to go to this place in person and check it out thoroughly. I spent a whole day at this place. Why? It's HUGE inside and they have a lot of surplus. The first thing I did was go to the bookshelf and gathered up roughly 150 books—databooks, manuals, etc. Really good stuff! After this, I hit up the back area of the place and spent most of my time digging through everything. They have an incredible amount of surplus—everything from heat sinks and ribbon cable to connectors and OLD non-pc keyboards. Even though I'm out of the business, I plan to go to this place many more times just to see what else I can find. Anyhow, after closing time, I was still there for another 30 minutes and they let me look around since they knew I was going to be spending money….. You see, most electronics stores aren't doing well like they did back in the 80's (the height of electronic hobbyists) so money is KING now at these places. After it was all said and done, I filled up my truck with piles and piles of obsolete (read: expensive) components, books, eprom programmers, S-100 buss cards, arcade parts, connectors, keyboards and other surplus parts for only a hundred bucks! Now that was a deal. Visit this place as fast as you can!

**THE SWAPMEET LIST**

I had to include this because quite a few of the sellers mentioned in the series I have written sell at one or more of these swapmeets and you'll usually find a selection of parts that you wouldn't otherwise be able to find from them.

**ACP SWAPMEET**
When: Last Sunday of each ODD month (Janurary, March, May, July, September, November)
Where: ACP parking lot. 1310 East Edinger Avenue, Santa Ana, CA 92705
Time: 7:00AM - 12:00PM
Cost: FREE

This is one of the oldest if not the oldest computer/electronic swapmeets available. While it's toned down over the years, it's still a cool swapmeet. Run by the same people that brought Advanced Computer Products and the ACP Superstore, there's a decent selection of old vintage electronic equipment, computers and NEW computer equipment here. I always buy something at this one.....usually a truckload worth. Many of the salvage places sell here.

**TRW SWAPMEET**
When: Last Saturday of every month.
Where: TRW parking lot at intersection of Aviation BLVD and Marine Avenue in El Segundo, CA
Time: 7:30AM - 11:30AM
Cost: FREE

Excellent swapmeet with lots of old electronics - parts, equipment, tools, etc. I found a great deal there every single time I have been there. This happens to still be my favorite swapmeet of them all. It's really geared toward ham radio enthusiast and electronics guys. If you look, you'll find great deals on electronic parts and components here. Many of the salvage places sell here.

**CAL POLY POMONA COMPUTER SWAPMEET**
When: Third Saturday of every month.
Where: Cal Poly Pomona Parking Lot F. 3801 West Temple Avenue, Pomona, CA 91768
Time: 8:00AM - 11:30AM
Cost: FREE

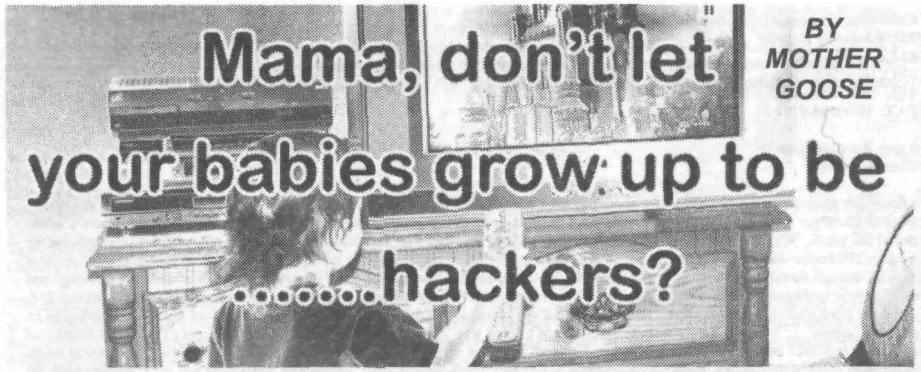
Small electronics swapmeet but worth the trip most of the time. They have a lot of people with older vintage parts and equipment. Found a good deal there every time I've been. This swapmeet has always been somewhat small and it tends to move around the parking lot a lot. In fact, the swapmeet has been slowing down over the years and I don't know how much longer it's going to last, so visit before it's too late.

**ARC SWAPMEET (Inland Empire)**
When: Second Saturday of every month.
Where: AB Miller High School. 6821 Oleander, Fontana, CA 92335
Time: 7:30AM - 11:30AM
Cost: FREE

Another small swapmeet, but a good one. It's been about a 50/50 deal here, but when I find a deal, it's excellent!

**SANTEE SWAPMEET**
When: First and Third Saturday of every month.
Where: Santee Drive-In Theater. 10990 Woodside Avenue (off highway 67)
Time: 7:30AM - 11:30AM
Cost: FREE

So-so swapmeet. Not the best, but still worth mentioning. I've found more than my fair share of excellent deals at this place. Made some big $$ off of them, as well.



# Mama, don't let your babies grow up to be .....hackers?

BY MOTHER GOOSE

Aren't kids lucky these days? They get to grow up in a world of computers and the internet, satellite and cable tv, gameboys, dvd players, cell phone, etc, etc, etc. Boy, we must have had it pretty bad in the dark ages to have to deal with lame things such as Atari, Commodore 64's, tape and record players, and rotary dial phones. How on earth could we have lived like that?? The truth of the matter is, kids, every generation has better, more technically advanced "stuff", and it's all thanks to the hacker generation before them. I think most people need to realize that, as it seems that a lot of people don't.

I am not a hacker, the best I can do on a computer is find Gymboree's website, and charge a hefty sum on the cutest kids clothes I can find. I am also not a professional writer. What I am is a hacker advocate, simply sitting here writing down my thoughts. I am a proud wife of a hacker, and mother of three small children ages 6 and under who I'm hoping will grow up to be hackers. I did not say that I want my kids to grow up to be criminals, I said hackers. Just as you would not call a banker who stole money out of his till simply a "banker", you would call him a thief, aka criminal. You should not call a hacker that does something illegal simply a "hacker", he is a criminal that also happens to be a hacker. There are criminals in every profession. There are also good people in every profession. Hackers are responsible for many things that keep "criminal hackers" from doing harm. What does a company do to protect their company from criminal hackers? They hire hackers, and they pay them a lot of money to do it. We tend to think of hackers as people who can't get enough of computers. Maybe that's because anyone with a hackers mindset loves a good challenge, and the computer has so many possibilities that have yet to be explored. But hackers are not just computer geeks, hackers love all technology. Any sort of electronics they can get their hands on is good. They make things that make the world a better place. Yes, I want my kids to grow up to be hackers.

I love the idea of my kids being the next inventors of some great technology we haven't even thought of and can't even imagine yet. A fresh generation of minds to take what my husbands generation of hackers have come up with and practice, take apart, manipulate, and hack these things to do whatever it is that they can think of to make them do. I for one encourage my kids to explore and "hack" a technology they find interesting.

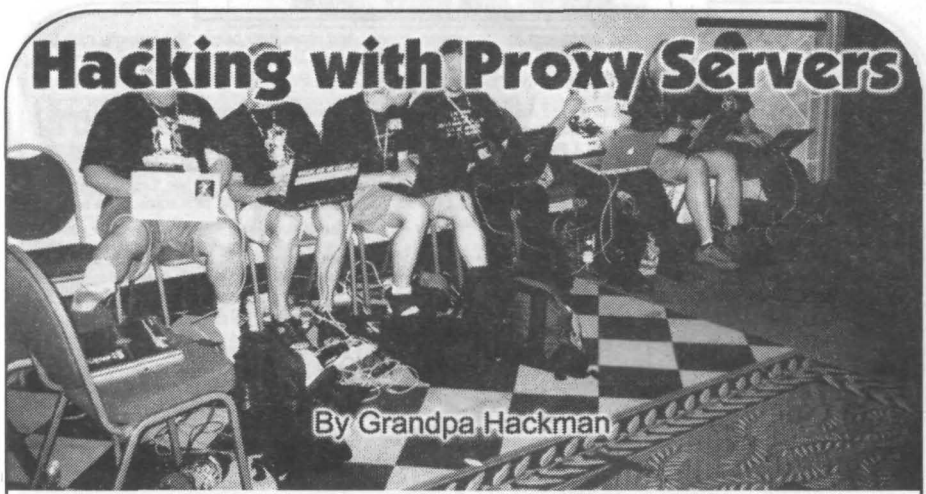
However, it took some persuasion from my first child to allow me to understand the scope of it. My daughter, at the time three years old, had a huge interest in our satellite box and how it worked.. My husband the "hacker" of the family, and I were very reserved about the idea of her having the remote control and doing with it as she pleased. He preferred the remote to be put up high and out of her reach. Now just to show you that we are born curious, thus actually we are born hackers, what do you think a three year old would normally do? That's right a three year old certainly would not sit there and take that, they would do what they could to reach that darn remote and play with it until their heart was content. Well, being that this was my first child, I did not realize this. My daughter not only from being simply three years old, but also presumably having a hackers mentality would some how climb up something and get that remote without any evidence to condemn her. Apparently she would do this when my husband and I were in the next room having a conversation, and she would keep an ear on what we were saying. I am assuming that when she would here our conversation come to a close, she would quickly and without proof put the remote back where she found it. This must have gone on for a while because for the longest time we'd find cartoons and kids programming recorded and we just couldn't figure out why that darn satellite receiver keep recording these frigen things! We didn't even imagine that our little three year old would be able to record them, I mean gee, the remotes were always put up.

My sweet little three year old would honestly think that my ears were going to fall off when she would rattle on and on, so much so that she'd have to stop in mid sentence to push my hair back and check that my ears were still there. So, how on earth could such an innocent three year old understand how and covertly record the show she was watching? Well, she did. She must not have been paying attention one day, because I walked in to find her in front of the TV with the remote in hand. She was startled, she jumped, and then she started to cry for fear that she was going to be in trouble. I know it sounds mean, but I couldn't help but chuckle at the discovery, and I had to call my husband in to see for himself. There she was with her little bottom lip sticking out, tears down her face, remote in hand, Blues Clues on the TV and the record button lit red on the receiver. It was cute, it was humorous, it was a revelation, and it was also a little sad. It was sad because she had to hide her thirst and desire to understand and learn. It was sad because she felt afraid of a consequence for wanting to educate herself. This was a revelation for my husband and I. We decided that if she wanted to learn how something worked, then she was free to explore. Naturally with many things, we would, or rather my husband would need to be there for technical support.

Aren't we always telling our children to study up. Don't we try to send them to the finest pre-schools we can find to give them the best head start on learning that we can? Yet, we still stifle their naturally curiosity. Who knows how many people out there today would have already invented a flying car had they been allowed to tinker with things more as a kid. Yeah, I know I'm reaching with that example, but it gives you the idea. Let's try to encourage our children to have a thirst for knowledge from a young age. Why not buy a newspaper, look in the freebies section and find an old TV to take apart together? Why not let your teenager stay up late on a Friday or Saturday night messing around on his computer and sleeping in late the following day? Who knows, that teenager of yours might be on the verge of a breakthrough on a new computer program that will make him millions and make life easier for billions of people including you..

In the sense that scientist invent cures to make the world a better place for human kind, hackers on a different level, give human kind new technology to make the world a better place. We should thank them. We should encourage them to learn, tinker, and explore. Mama's, please let your babies grow up to be hackers. I would hate to miss out on what good things they could have contributed.

# Hacking with Proxy Servers



By Grandpa Hackman

Most folks have never utilized a proxy server because, well, why should they? It's usually only done by folks whose ISP requires them to use one. It's slower and more hassle to deal with. So why on Earth would you want use one? Well, have you ever been in a location with web access that is censored? Maybe you want to check out that www.playboy.com (for the articles), but the school district's "NetNanny" shuts you down. Or maybe you're a hacker, just looking for some innocent (?) info (like a mailbox bomb), and up pops the thought police, No, no, no, no. Maybe you've got a slow dog phone line connection at home, but you'd sure like to download that 25 Meg file on the workplace's T-1 to burn to CD and take home instead of tying up your phone line for hours and hours. But you can't, because it had a metatag that your administrator considers dangerous. I find that oftentimes it's not even the intent to limit access on a particular subject, just some wording somewhere on the page that trips the "censor" erroneously.

Or maybe it's a web location that you don't trust altogether, and you don't want them to be able to see your IP address. For me, warez/virii sites fall in this category.

While there is no "one size fits all" solution, you may find that a proxy server will do the job. There are also html to email portals that will email "forbidden" web locations to you through your email server. This will always get through. And, done properly, the location being accessed will not be able to view your IP address, they will instead see only the IP address of the proxy server. Of course, law enforcement will be able to track you, so don't send that threatening letter to the president. But even they will have quite a time of hunting you down if you do it right. For example, I used to use a proxy server that was in a far off country, and not one of the friendliest of nations to the U.S. I think I would have to do something very serious for them to agree to play ball with the Feds.

How does one go about using a proxy server? Well, first you have to find a proxy server. Now, they are really not all that happy about you doing this, because this server is maintained to serve a certain number of customers, and if you start using it, you just become one more straw on the camels back. So they just don't freely advertise that they can be used in this way. Actually, a few do, I've never used those.

But, as I said, many ISP's require their customers to use a proxy server. And bless their hearts; they usually maintain web pages that explain in great detail how to set the browser up with the proxy. This is so that they don't have to hold their customer's hand on the voice phone explaining this information. The trick is to find these web pages.

I hate to give this info out, because it has served me well over the years. But there are so many proxy servers I guess it really doesn't matter. Go to your favorite search engine and look for "Internet Explorer" "proxy", something like that. "Configure" is another good search word. I like using "internet explorer" no matter which browser you prefer to use, because 90 + some percent of the ISP's out there "recommend" the Bloated One to their users. I know from experience that this search will give you all the hits you need to complete your task. You'll get thousands of hits, I recommend not using the ones on the first page your search engine finds, but rather, go several pages in and pick some. That way the ones on the first page aren't being used by 95% of the "spoofers."

It isn't really necessary for me to tell you the rest because the found web pages will explain to you in great detail how to set up "Internet Explorer". If you're using another browser, I'm sure you'll be able to figure it out quite easily. Basically, in IE, you go to Tools > Options > Connections > Lan Settings, click on the checkbox that says "Use a proxy server for your LAN", and enter the proxy server's URL. Be sure and type a full URL, don't skip the http:// stuff!

You'll probably find that you need to try several to find the one that works best for you. Some are just _too darn slow, some just don't work at all (who wants to waste time figuring out why, just get another one), others will censor material on you (the Arab sites don't like anything that has the word sex, for example). But if you are perseverant, you'll find several you can use.

How does it all work? When your local browser sends out a request for a web page, it no longer sends it directly to the site (after DNS lookup). Now the request is sent to the remote proxy server. The proxy server then sends the request to the site retrieves the data stream and then sends it back to you. It's like a middleman.

I used to work at a school and the administrator there was very diligent about limiting access to certain sites. But this technique slipped through every time, because it didn't see something like www.playboy.com as a request, instead it saw <proxy address>:www.playboy.com, etc. Something like that, I don't recall the exact syntax. Frankly, I didn't care about the above mentioned site at all; I was just interested in the challenge. Er, and I was reading the articles.

After you've configured your browser to use the proxy and you're curious about just how invisible you are, check out one of the many "IP testers" on the web. Here's the URL of one, there are many:

http://all-nettools.com/toolbox

You'll find that if you did your proxy configuration correctly, and you have a good proxy, your local IP address will be invisible to the site (You can view your local IP address by starting a command prompt and typing IPconfig). Congratulations, you now have a low-grade IP spoofer. Remember though, the date/time, requested site, and your real IP address is logged by the proxy server, so there IS a track record. Although, if it's in say, China, the track record might as well be non-existent.

It's not really "IP spoofing" because that involves changing the outbound packets to reflect an IP other than your own. That is much more difficult, and for the most part, not necessary to become relatively invisible on the web. The huge number of proxy servers available makes this the hands-down easiest approach for most purposes. Those that would require real IP spoofing are advised to investigate the subject further on the web; it is beyond the scope of this article.

Now, you may occasionally find this doesn't do the trick for you, for various reasons. For example, maybe you like that Arab proxy, but when you go looking for, ah, somewhat clandestine information, the sites with that information are loaded heavily with porn banner ads. As I said, to the best of their ability, the Arabs try to censor that. Even though you had no interest in those ads (right?), the server is going to refuse access. Now what can you do? Well, you can use a web to email gateway. These way-cool servers just sit and wait for you to write them an email, really! You write them an email with the URL you're having trouble getting, and voila! In a few minutes, the web page is sent to you via email. In text or html format -with pictures even. What could be cooler than that?

The following URL has much information on the subject, including a list of several servers:

http://www.bellanet.org/email.htm

You can find many more servers, just type "web to email" in your favorite search device. There are a multitude of uses for these servers. In addition to the "forbidden" URL workaround mentioned, you may sometimes find that you are occasionally reduced to surfing in a very limited bandwidth situation. Maybe at the hotel, or connected through your cellular, etc. Actually, that is really the reason these servers were created. While most of us have become spoiled and cannot stomach the time it would take to go from web page to web page in such an instance, you can request several web pages at once, wait a few minutes for them to arrive in your email, and then view them in rapid succession after downloading your mail. Or write an email with your favorite sites that you hit daily, send it off to one of these servers in the morning, and have your favorite news sources, etc. on tap, updated daily without the wait. At least not the maddening "human assisted" waiting between each page. And if you ARE in a censored environment, these emailed web pages will come through without a hitch, no matter what their content.

Do use these resources responsibly though, abuse could put a serious hitch in the availability of these handy sites. Most are free, maintained by volunteers.

Repeat after me, the hacker mantra, "There's always a way."

Although off-topic, while we're on the email subject, have you ever been in a remote location and wanted to view your pop email (not web-based) on another computer? While most pop servers have a web-based interface just for this purpose nowadays, not all do. And some can be quite the hassle to access if you can't recall the exact URL. You have to go to your ISP's general information page and fish through links, and many don't do a very good job of making this as easy as it could be.

www.mail2web.com is the answer. Here's what they say about themselves: "From any computer, anywhere in the world. No need to register!" That pretty much tells the whole story. Just put in the name of your email server, your username and password, they can retrieve your email on the spot as though it were web-based.

While some might argue that there is no need for such security measures ("what are you trying to hide?") others would argue that in a society with an ever increasing intrusion into personal daily affairs, such techniques are more than necessary. They are mandatory.

The founding fathers took great pains to protect us from the very intrusions that many of our peers consider "normal" today. They knew what they were doing, for they had experience with a very intrusive government themselves. That is why they CLEARLY stated that the right to pursue liberty and happiness were inalienable rights "endowed by the Creator." Not some permission granted to you by powerful men, mind you, but rights that you were given when you were born, by the Creator. Inalienable, they cannot be separated from you.

May we always remember to question those that would chip away at our rights, that it is their job to demonstrate by what right they attempt to do such a thing, when it is a power higher than them that gave us these rights in the very first place. The only other option is to scrap the entire concept of the United States as having been founded on erroneous concepts in the first place. I doubt you'd find any support for that (thank goodness!).

At this point you may have deduced that the author has degenerated into a drifting ramble, but there is a point to be made. There is no freedom, except for that which we make for ourselves. There is much information available on the web regarding security; I recommend that all readers become familiar with at least some of it. PGP is still Pretty Good encryption (won't stop the Feds though, it is rumored). Remailers are a very powerful and useful tool. These remailers will allow you, when used properly, to send TRULY anonymous email messages. You can also "chain" the remailers, making any attempt to track the source a nightmare without end. Who knows when and if such a thing might become more than an exercise in security measures; it's conceivable that it could become necessary at some point. One thing you can be sure of, if that time were to come, it would be too late to find the remailers and learn how to use them. The same thing is true of many of the security measures mentioned in this article.

Browser-based anonymous FTP is possible using the proxy server techniques spoken of earlier. You'll note that in the IE options menu for the proxy there is an "Advanced" button. Clicking on this, you'll see how you can do the same thing spoken of earlier for your browser for browser-based FTP access. Usually the web browser proxies use port 8080, and the FTP proxies use port 21. These are the standard default values for these functions. They are not written in stone however, note the ports that the proxy server mentions if they are not the default values.

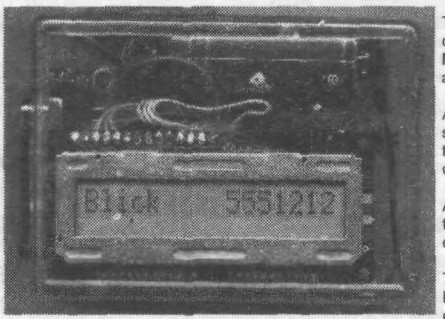
The techniques mentioned in this article are easy to implement, you'll be a pro in no time. You'll have another feather in your hacker headband, and you'll have the knowledge that you can become invisible on the web on whim. You can laugh at any attempt to censor your interests. And, if need be, you can get information out to others, without sacrificing yourself as a martyr. Heck, you'll be needed for your other talents.

Onwards and upwards!

# DTMF TONE DECODER PROJECT

***By Bob Blick***

***Additional excepts by Kingpin***
***Editing by Zachary Blackstone***




These plans explain in detail how to construct a project which displays telephone numbers decoded from DTMF (Dual-Tone-Multi-Frequency) tones, or touch tones. This is a useful tool for any hacker to keep handy.

A microphone picks up the tones, a preamplifier boosts the signals, an SSI-202 DTMF chip decode all 16 of the DTMF tones (1-9, A-D), a Basic Stamp acts as an interface to an LCD display and also provides "RS-232" serial output.

Alternatively, the DTMF decoder can be directly connected to a telephone, scanner, or a tape recorder using an optional circuit described in this article.

The tone decoder can be used for many things. Anytime you hear a DTMF tone, and want to know what it is, just hook up the decoder. When it is hooked up to a phone line, any tones sent over the line can be decoded immediately. It is great for services like credit card verification, voice mail systems, answering machines, COCOTS, etc. DTMF signaling is so widespread, there is no doubt that you will discover many useful applications with the decoder.

Speaking of DTMF, the 16 tones that this circuit decodes are as follows:

| | 1209 Hz | 1336 Hz | 1477 Hz | 1633 Hz |
|---|---|---|---|---|
| 697 Hz | *1* | ABC *2* | DEF *3* | *A* |
| 770 Hz | GHI *4* | JKL *5* | MNO *6* | *B* |
| 852 Hz | PRS *7* | TUV *8* | WXY *9* | *C* |
| 941 Hz | * | oper *0* | # | *D* |

A PCBoard has not been designed for this project, thus you must use a breadboard or design your own PCBoard before you build the project. On a scale of 1-10, this is about a 6 as far as difficulty is concerned. In order to build this circuit, you will need quite a bit of electronics knowledge. Therefore, if you have never built anything involving electronics before, we suggest that you seek help from someone with intermediate electronics experience when trying to complete this project. A schematic of the circuit is provided to guide you but, again, a PC Board layout is not included at this time.

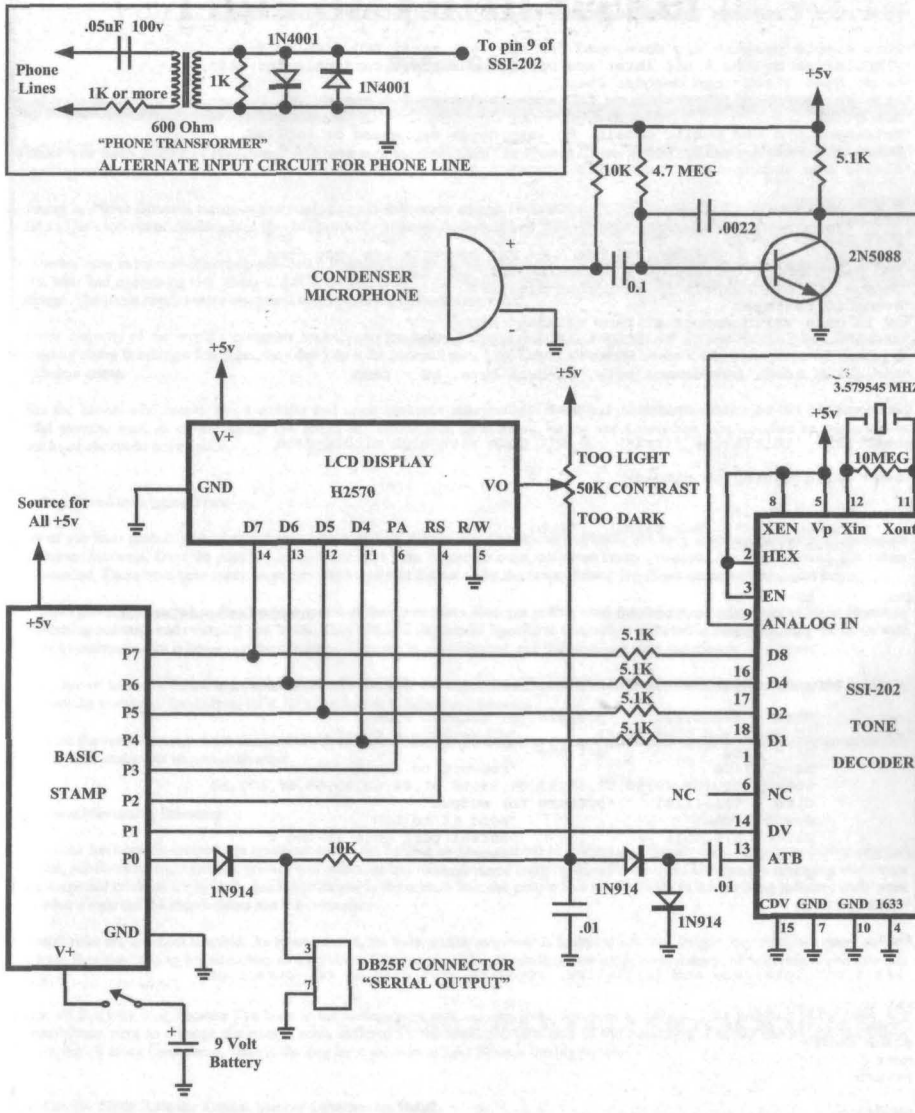
You might have trouble finding the SSI-202 chip, even though Radio Shack used to sell them. In the United States, the best place to buy them in small quantities is B.G. Micro, www.bgmicro.com. They have the SSI-202 chip for $6.95 (part number ICSSSI202). In addition, B.G. Micro also supplies a SSI-202 datasheet at $0.50 for those who are interested (part number ACS1023). *Editors note: At time of publication, the SSI-202 is also available from ACP components www.acpcomponents.com - price unknown.*

If you have access to Mitel 8870 DTMF chips, you could use it in this circuit if you change the pins to match the corresponding functions. I have not done it, so I can't help you. Silicon Systems, maker of the SSI-202 chip, has been dissolved by Texas Instruments.

Concerning the schematic diagram of this project. I have not included a parts list, but I've tried to make the diagram self-explanatory. If you can understand it, you can probably build it. Due to popular demand, I have included a modification that allows direct connection to the phone lines. I must say, however, that I have not tried the modification (I have been told it does work) and it's probably against the laws of certain countries, states, provinces, townships, and telephone companies to connect home-made devices to the phone lines.

*Editors note: We've supplied a parts list and have suggested locations to purchase these components. The Basic Stamp can be purchased from Jameco (www.jameco.com). Support for the Basic Stamp can be found at Parallax (www.parallax.com). About the LCD - it's a Hitachi H2570 1x16 matrix LCD. We have them available at $10 each. However, you may substitute any number of LCD panels in the place of this one if you have difficulty locating this one. The following LCD's are suitable replacements: Hitachi H2572, Sharp LM016L, Sharp LM018L, Sharp LM038L, Sharp LM1615A, Vikay VK2116L or the Philips LTN211F-10.*

## *DTMF TONE DECODER PROJECT - SCHEMATIC DIAGRAM*




### PARTS LIST FOR THE DTMF TONE DECODER

IC1 SSI-202 TONE DECODER
IC2 BASIC STAMP
LCD1 HITACHI H2570 LCD
Q1 2N5088 Transistor
X1 3.579545 Mhz Crystal
B1 9 Volt Battery
C1, C2 .01 uF Capacitor
C3 0.1 uF Capacitor
C4 .0022 uF Capacitor
C5 .05 uF 100v Cap. (for use with alternate input circuit)
D1, D2, D3 1N914 Diode
D4, D5 1N4001 Diode (for use with alternate input circuit)
R1, R2 10K Resistor
R3, R4, R5, R6, R7 5.1K Resistor
R8 4.7 Meg Resistor
R9 10 Meg Resistor
R10 1K Resistor (for use with alternate input circuit)
R11 1K or higher Resistor (for use with alternate input circuit)
P1 50K Potentiometer
T1 600 Ohm 1:1 Phone Transformer
CD1 Condenser Microphone
CN1 DB25 Female Connector

## *DTMF TONE DECODER PROJECT - BASIC STAMP CODE*

```
'TONE DETECT PROGRAM FOR BASIC STAMP/HD44100 LCD DISPLAY/RS-232 OUTPUT

'This simple program was developed for the 16x1 ascii LCD display from
'TIMELINE using the 4 bit interface option, stamp set currently for 2400
'baud. Uses SI202 tone decoder chip.
'Written by Bob Blick with some LCD code thanks to Jim Remington.
'Bob Blick 1996
'Released into the public domain. No warranties expressed or implied.
'Bob Blick February 18, 2002
'Please see accompanying schematic "tonesch.gif"

'CONNECTIONS
'lcd pin            14  13  12  11   6   4            5    2    1
'port pin on stamp   7   6   5   4   3   2   1   0   gnd   +5  gnd
'function         db7 db6 db5 db4   e  rs  DV rs232 r/w  vcc  gnd
'LCD pin numbers correspond to TIMELINE 16x1 LCD display.
'Change LCD pin numbers to suit your display.
'e=enable rs=reset
'DV is data valid output of tone decoder chip
'Stamp supplies 5 volts to LCD, tone decoder, preamplifier.

'variables used: b0=command byte, b1=data byte, b2 = temp

dirs = %11111101   '7 output, 1 input bits

gosub init 'initialize display - 4 bit mode with high nibble=data

'send hello string to display

for   b2 = 0 to 15
      lookup b2,("   Bob Blick    "),b1
      gosub lcdout
      next

for       b2 = 0 to 1
          lookup b2,(0,112),b0                          'scroll mode selected
          gosub send
          next

'main loop, no check for line length. Plenty space for such options!

loop:     dirs = %00001101    'prepare for decoded tone
test1:    if pin1 = 0 then test1        'do we have a tone?
          b1 = pins           'got one
          b1 = b1/16                    'convert to ascii
          lookup b1,(68,49,50,51,52,53,54,55,56,57,48,42,35,65,66,67),b1
          dirs = %11111101    'prepare for output
          gosub lcdout                  'send it to LCD
          serout 0,4,(b1)               'serial port gets it too
test2:    if pin1 = 1 then test2        'same tone?
          goto loop           'ready for new tone

'SUBROUTINES

init:

'set 4 bit interface and initialize, standard plus display on, cursor off

for b2 = 0 to 13
lookup b2,(48,48,48,32,32,0,0,128,0,16,0,96,0,192),b0
gosub send
next
return

send:
'output command byte b0 to port, pulse e. Note: assumes bit 2 is clear
pins = b0|8 : low 3
return

lcdout:
'send character in b1 to display, first top nibble then bottom
b0=b1&240+4    : gosub send  'bit 2 = 4 sets data mode
b0=16*b1&240+4 : gosub send
return
```

The software for this project. It is only a bare-bones program. The smart people that build this circuit will surely write some better programs and send them to me to include in this page. This program works fine, it's just very basic. You must rename it with a .bas extension before loading it into a Basic Stamp. *Editors note: This source code is available for download on Bob's website at the following URL: http://www.bobblick.com/techref/projects/tonedec/tonedec.txt Additionally, this code will be made available on the Blacklisted! 411 website in the magazine forums > project discussion area.*

# Thief or Thrill seeker?

**By Erik Giles**

I wonder how many readers of Blacklisted! 411 have seen the film called *The Thomas Crown Affair?* For those of you who haven't, let me quickly summarize it for you.

Portrayed by Pierce Brosnan, the main character is a multi-billionaire named Thomas Crown. He's reached to the pinnacle of the business world and he's run out of challenges in life. Billion-dollar business deals bore him. Crown crashes expensive sailboats for spite.

Mr. Crown, now in his mid-life crisis, concocts a diabolical criminal masterpiece and steals a priceless painting from a museum. Why did a man who had everything risk going to jail? He didn't need the money. It was never about the money for him. He did it for the challenge. The game itself is more important to him than the rewards ever were.

The vast majority of the world's computer hackers are the same. They break into systems just for the challenge. While they aren't necessarily above breaking a few rules, they don't do it for personal gain. Like Crown viewed his art theft, they view computer hacking as a victimless crime.

Unlike the hacker who breaks into a website and steals customer information, Crown had the luxury of returning the painting to the rightful owners. Sure, an ethical hacker can return any information he acquired, but no one knows how many copies he made and to whom he or she might have sent it.

**Growing Trend is Eroding Trust**

Many of you have probably heard of the recent hack of BJ's Wholesale. Announced in March, this hack involves hundreds of thousands of customer accounts. Over the past few years there have been numerous other notorious hacks. Amazon, Axcion, Egghead and others come to mind. There have been many more, smaller hacks that did not make the news. I think it will get worse before it gets better.

Merchants generally react when they become aware of their customers accounts getting used fraudulently. Banks react to these situations by cancelling accounts and reissuing new cards. They can also implement aggressive transaction monitoring strategies. But the down side of these countermeasures is impact on the customer. They are inconvenienced, and they can lose time and money.

In the wake of these incidents, merchants and banks can also turn against each other. A few banks are already pursuing the matter in court, looking to recover losses from BJ's. BJ's has vowed to fight these lawsuits.

But I think the worst damage is not financial. Faith in the banking system begins to erode. Customers become less willing to spend money and merchants and banks turn on each other.

**Banks and Merchants Dilemma**

Once a hack has been discovered, the merchant and/or the banks now has a number of choices. Leadership has to weigh a number of risks, financial, public relations, consumer privacy and others against each other and come to the right decision. Despite the emerging stereotype of the corporate criminal whose only guiding principal is the bottom line, the people I've worked with in the banking industry truly want to do what's right for the shareholders and the consumer.

Financial risks are the most tangible. As losses mount, the bank and/or merchant is forced to act. The longer they wait, the more money they lose. However, taking action carries its own costs. Closing accounts and sending new cards costs money. Monitoring accounts costs money.

I know all this very well, because I've been in the management side, helping make decisions to safeguard the interests of the bank. My responsibilities were to manage the overall costs suffered by the bank and take care of the customers. I could reduce the short-term impacts, but all along I wondered, what is the long term solution to this? What is the big picture?

**How Can (or SHOULD) the Ethical Hacker Community Help?**

Okay, the *Thomas Crown Affair* was just a movie. Pure fiction. But I imagine that a real world Thomas Crown Affair would motivate the management of the art museum to re-evaluate and upgrade their security. Crown's actions allowed them to gain valuable information about security gaps that would enable them to prevent similar losses in the future.

At the end of the day, the art museum learned of their vulnerabilities and did not lose the painting. From this point of view, one could rationally argue that Crown did them a favor. But this does not make Crown's actions legal or morally right?

Looking at it from the strictly economic point of view of the insurance company, the theft was a good thing. Sure, they had to pay the investigator, played by Rene Russo, her finders fee. But her fee was insignificant compared to the loss of the painting. The security vulnerabilities could be addressed, or theinsurance company could revoke the museum's policy.

In the real world, a hack of customer information works out much the same way. The victim, in this case the merchant who got hacked, becomes aware of their security loopholes after the information and the money is gone.

Where do the 'White Hat' hackers enter here? Of course I cannot suggest or condone this kind of activity, but I wonder, what if an ethical hacker, rather than a criminal, found the next major exploitable gap in a large merchant? If he reported the vulnerability, would the victim even bother to respond? Or would wait for real losses in order to get them to react?

What if an ethical hacker had identified the breach at BJ's wholesale and informed the right people before any dollars were lost? Would anybody have acted?

We all hear about the mass compromises where there are losses associated with it. But how many more occur, where the hacker is a Thomas Crown, not intent on stealing the cash, but just beating the system?

Would the merchant or bank work to close the loophole then? Somehow, I don't think so. Sure, the card associations such as Visa, MasterCard and Discover have strict rules regarding storage and protection of customer information, but they can't possibly enforce these rules in every database in the world. In our current climate, like the tree that didn't really fall because no one hears, loopholes are not truly loopholes until money is lost.

**Hacker Wargames: Radical Idea For A Solution**

If you want to safeguard trust, you've got to prevent the hack from happening in the first place. But I don't think that it's possible to close every potential loophole in every data system, so it's futile to even try.

But there is a large, untapped resource out there that the business community could harness. And I don't think it would cost nearly as much money as they are currently losing to these hacks.

I suggest that the banks, merchants and credit card associations get together with the ethical hacker community and run large scale hacker wargames. Certain businesses could declare their systems as legal targets within certain timeframes, offering bounties and amnesty to the hackers who find the most exploitable gaps. I believe that most of the worst vulnerabilties would be discovered before a criminal hacker is able to.

Everybody wins. The ethical hackers would relish in beating the system, the security issues could be fixed with no customer impact, and these threats to trust and consumer privacy could be greatly reduced. I think the hardest part would be figuring out how to get the risk-taking, free-thinking hacker types and business leaders to work together.

Enjoy yourself, Mr. Crown. Try to beat the system again. Steal the paintings and give them back, but be sure to tell us how you did it.

**Links**

http://www.usatoday.com/tech/news/computersecurity/2004-08-10-database-culture_x.htm

http://business.bostonherald.com/businessNews/view.bg?articleid=40303

http://www.eweek.com/article2/0%2C1759%2C1597974%2C00.asp

***About the author: Erik Giles has worked for three of Americas top ten banks, specializing in fraud prevention. His first novel, Terror Cell, features a computer hacker as the main character. See www.terrorcellbook.com for more information.***

# CALLER ID SPOOFING PRIMER

***BY THE CRYPT PHREAKER***

So, you've heard of caller ID spoofing as it's a fairly hot topic. You want to know what it's all about? No problem. We'll give you a real quick lesson on the subject and hit you with a detailed article in the next issue.

In a nutshell, Caller ID spoofing is pretty much exactly what it sounds like. It's a method by which the caller ID of the calling party is "spoofed" to indicate a different (user selectable) caller ID on the receiving end of a phone call. Why would anyone want to do this? For any number of reasons, all of which are to hide or conceal the true identifying number of the calling party by replacing it with a false number. It's an extremely useful tool for the phreaker, private investigator and bill collector. Yes, even bill collectors use this. See www.star38.com for more information.

How does it work? Without going into heavy detail on the subject, I'll give you a couple examples. Each of these examples require the use of a third party service of some sort.

#1 The most popular method is the use of the Telus service which was first discovered by Lucky225. The caller places a call to Telus (800)646-0000 with an ANI fail (using AT&T op divert), gives the operator the number they're dialing from (fake #) and completes the call. The called party receives the call with caller ID indicating the fake number originally provided to the Telus operator. As of this writing, the AT&T op divert was working only some of the time. This method still works, depending on which AT&T call center you reach. Varying reports are coming in on this subject, so YMMV.

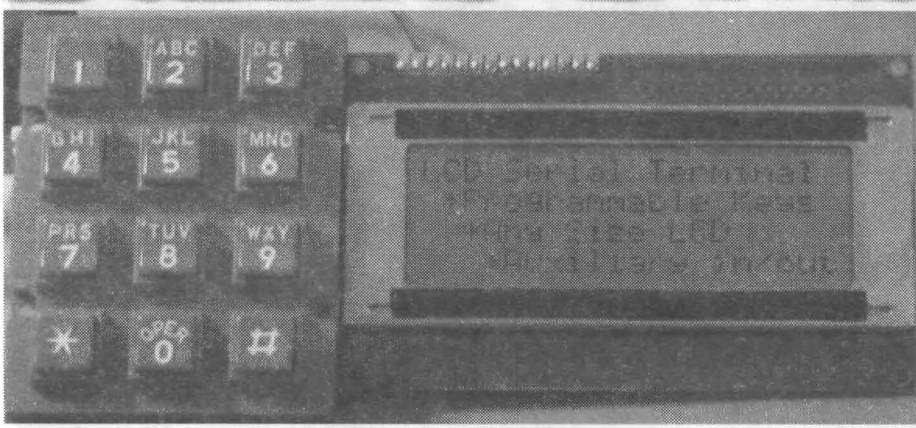
#2 Method two involves the use of Voicepulse voice over IP (VOIP) service (www.voicepulse.com). The caller sets up their Voicepulse account to forward to the number of the person they wish to call. They then call their own Voicepulse number with their caller ID blocked. They are prompted to enter the calling number (fake # inserted here) and the call goes through.

Ok, that's it for now. Sound interesting? Stay tuned for the full article in the next issue of Blacklisted! 411.

# LCD SERIAL TERMINAL PROJECT

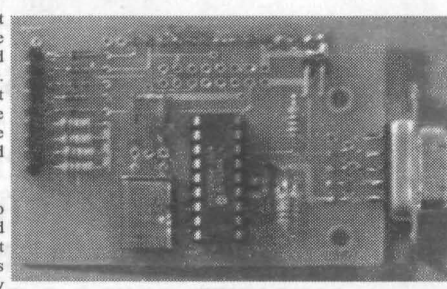
*By Bob Blick*

*Additional excepts by Rogue*
*Editing by Zachary Blackstone*




**Introduction:**
In the 1980s a serial terminal was a big thing with a picture tube and keyboard. You used it to communicate with a computer by RS-232 cable or with a modem. In this century, we still sometimes have need for a serial terminal, and we'll typically use a personal computer running a terminal program (Hyperterminal, bundled with Windows, is a terminal program). This project is a self-contained serial terminal using a PIC16F84 microcontroller chip, an inexpensive LCD character display, a keypad, and very little else. It is full-duplex, meaning keypresses cause RS-232 output, and RS-232 input makes characters appear on the LCD. If you connect the RS-232 output to the input you can see the keys as you press them, without connecting to anything else (that's called "looping back").

**Project Description:**
The picture above doesn't show the electronics, just a keypad and LCD display. The electronics is on a small board behind the LCD. This LCD is a 4 line by 20 character intelligent LCD display. Displays from 1x8 to 4x20 or 2x40 and pretty much anything in between are compatible. I paid less than US$10 for this display from All Electronics (http://www.allelectronics.com) (*editors note: All Electronics still has a backlit Samtron UC20402 TLAT5-H 20x4 LCD available at the time of publication, part number LCD-89 at a cost of $24.80. The spec sheet is available in PDF format at http://www.allelectronics.com/spec/LCD-89.pdf*). The keyboard you use should be a matrixed keyboard or keypad with up to 5 rows and 4 columns (20 keys maximum).

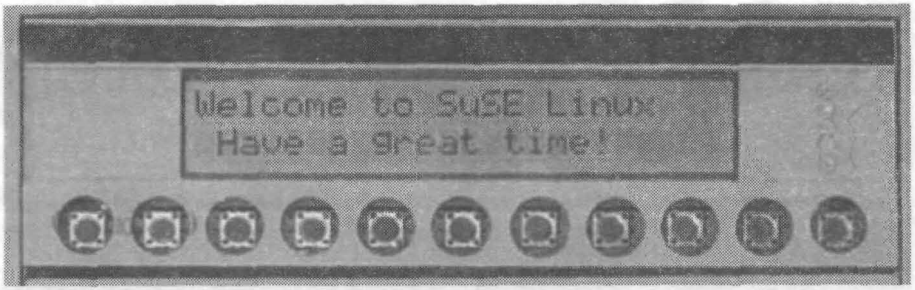


This small PC board is the terminal itself. Someday I will document a PC board design, but currently I am only making available the schematic diagram, source code for the PIC16F84, and compiled hex code for a typical configuration so you can quickly test it out. The source code is in C and very easily configured for different baud rates, LCD and keypad configurations. The program should be compiled with Hi-Tech PICC (http://www.htsoft.com/). A free version supporting the PIC16F84 called "PICLITE" is available and works fine.

The mapping of the keys is fully configurable, and each key can also be configured for one of four different modes. Each key is allowed to have a primary code and a secondary code. Depending on what mode is chosen, the secondary code might be sent when the key is released, or when the key is held more than one second, etc. Key repeat is also programmable, and each key can have a different mode.

Many cursor movement features are implemented, all the standard ones (backspace, carriage return etc.) and if you tell the program your LCD format, text will flow from line to line.

Every pin of the PIC16F84 is used, and some pins are used for 4 functions, through multiplexing the LCD, keyboard drive, and auxiliary input and output, using a feature I call "supermultiplexing". I intended the auxiliary outputs to drive LEDs. The picture on the top of the opposite page shows a terminal mounted in a computer's drive bay, see the five LEDs on the right side. The LEDs are time-sliced, so the pins are not dedicated all the time, so the LEDs will show a faint glimmer when off. Nonetheless, it's a useful feature. Auxiliary inputs should be connected through a 10K resistor and will read high if left floating. One PIC pin is completely free




and is configured as an output. The source code is easily modified if you need more pins and can sacrifice keypad columns.

**Technical Notes:**
Baud rates are chosen in the program before compiling. If you use a 4 MHz crystal the maximum baud rate is about 2400 baud. Actually you can get 2400 baud with a 3.58 MHz crystal. If you need 9600 baud you can use a 14.318 or 16 MHz crystal, even though the PIC16F84 is only rated for 10 MHz(or use a PIC16F84A). "Funny" baud rates are possible, within limits any baud rate can be used. It is not possible to have split (different baud rate for send and receive) rates. The PIC16F84 does not have a hardware UART (serial port) so each bit must be done in software using a method called "bit-bashing". I used the timer-based interrupt to manage the timing. This limited the maximum baud rate, but the code is less messy using the timer interrupt.

The circuit requires a 5 volt DC power supply at a few milliamps. Although the PIC16F84 can run from 4 to 6 volts, the LCD contrast varies wildly with voltage. In the schematic I have shown LCD pin 3, the contrast pin, grounded. This might give you too dark a display. Connect it to ground through a 470 Ohm or 1K ohm resistor to lighten the display.

RS-232 is supposed to have +12 and -12 volts. This circuit does neither. Driving long, noisy lines could be troublesome. The receive pin is a Schmitt Trigger so it should reject most sources of noise, but if you have problems you could terminate it with a 4.7K resistor to ground at the board.

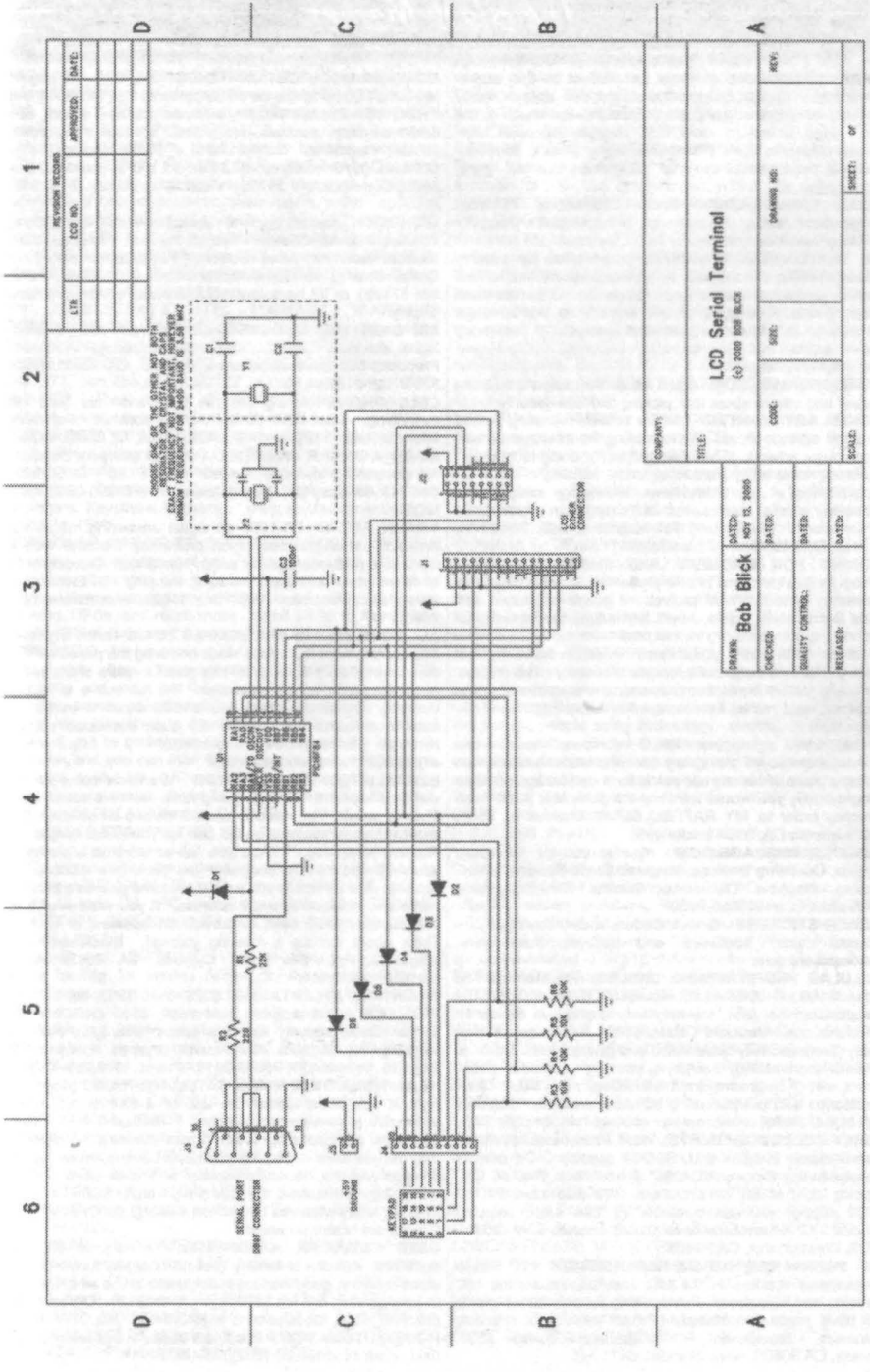
Supermultiplexing is not shown on the schematic. It is available on 5 pins (RB3-7). For output, connect LEDs through resistors (minimum 220 Ohms). The are commanded with control-P followed by the binary pattern you wish to output. The upper 5 bits of the byte you send will be output, and the lowest bit is sent out RB0. The other two bits are ignored. For input, hook to pins RB3 through RB7 through 10K resistors. You can use switches to ground, sense logic levels, or even sense 12 volt logic in an automotive application. Read the pins with control-N. A byte will be sent out showing the state of PORTB. The bottom 3 bits are not cleared so you should ignore them.

The source code is heavily commented so you should consult it before asking questions!

Timing is based on the crystal. You may substitute a ceramic resonator instead of a crystal, the accuracy of a resonator is adequate. Although a PIC can use an RC oscillator, it should not be used in this circuit, your baud rate would not be accurate. Use a crystal or resonator.

*Editors note: The C source code for the PIC16F84 is about 23K in length, so we decided NOT to include it in print form. It's available on Bob's website at the following URL: http://www.bobblick.com/techref/projects/lcdterm/lcdterm6.c Additionally, this code will be made available on the Blacklisted! 411 website in the magazine forums > project discussion area.*

## LCD SERIAL TERMINAL PROJECT - SCHEMATIC DIAGRAM



# The Black Market

**LARGE SELECTION** of items of interest to the hacker community. Surplus, stun guns, pepper spray, hobby supplies, electronics, survivalist, spyware, too much to list here. Huge selection of FREE ebooks, Succeed With Women, Guerilla Web Promotion, many others, some for purchase, the cream of the crop. Come check us out! www.hacksupplies.com

**URBAN EXPLORATION!** Phone obsessions! Pointless conversation! And a slight chance of hacking! It's Doug TV baby http://www.dougtv.org

**THE WORLDWIDE WARDRIVE** is an effort by security professionals and hobbyists to generate awareness of the need by individual users and companies to secure their access points. The goal of the WorldWide WarDrive (or WWWD) is to provide a statistical analysis of the many access points that are currently deployed. http://www.worldwidewardrive.org/

**LOCKPICKING101.COM** Open forum discussion to educate yourself and others about lock picking and lock security.

**HACKER ART WANTED!** We're actively recruiting people to submit artwork to us. We're looking for freehand as well as computer artwork of technology, people using technology, events, devices, utility personnel, utility vehicles in action (or doing nothing at all), tradeshows, technology swap meets and hacker meets, comics, etc. If it's related in any way, we want artwork!! Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**LOOKING FOR HACKERS AND PHREAKERS!** We're looking for hackers and phone phreakers to work on a new community based WWW project. If you're interested and would like to know more, email keynet@spoonybard.org or visit http://spoonybard.org/keynet.html

**INFOSEC NEWS** is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles will come from newspapers, magazines, online resources, and more. For more information: http://www.c4i.org/isn.html

**I'M RAFFLING** my original APPLE-1 computer I have no use for it anymore so im giving any one who wants a chance on owning a piece of history all I ask is for a one paragraph letter telling me why you would want my computer,and $2.00 cash or money order to: MY RAFFEL, 567 W. channel Isl. Blvd., Port Hueneme CA, 91341 suite 416

**HACKERSHOMEPAGE.COM** - Your source for Keyboard Loggers, Gambling Devices, Magnetic Stripe Reader/Writers, Vending Machine Defeaters, Satellite TV Equipment, Lockpicks, etc...(407)650-2830

**HACKER STICKERS** Geeks, Coders and Hackers get your stickers, shirts, hardware and caffeine from www.hackerstickers.com

**CELLULAR PROGRAMMING CABLES:** For Motorola Flip Series $100, 8000/Brick Series $150, Mobile/Bag: $100 (includes handset jack, the only way to program Series 1). Panasonic and Mitsubishi Cables $100. All cables are high quality, professionally assembled and guaranteed. Guide to Cellular Programming, everything you ever wanted to know, correct wiring diagrams, troubleshooting, etc.: $45. Other accessories and programming software available. Inquiries to: (714)643-8426, orders only to: (800)457-4556. C.G.C.

**HIGHLY COLLECTIBLE INTEL 4004** Processors. We have these available in NEW OLD STOCK condition. Ceramic as well as plastic. Ceramic "D4004" $70. Plastic "P4004" $40. Shipping cost of $6 not included. We also have P4001/P4002 support devices available @ $26 each, shipping included. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**GET YOUR FREE AD 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. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**SCANNER MODIFICATION HANDBOOK.** Big! 160 pages! More than 20 performance enhancements for PRO-2004 and PRO-2005. Restore cellular, increase scanning speed, add 6,400 memory channels, etc. Step by step instructions, photos, diagrams. Only $17.95, + $3.50 hipping ($4.50 Canada). (NYS residents add $1.38 tax.) CRB research, Box 56BL, Commack, NY 11725. Visa/MC welcome. (516) 543-9169.

**HIGH-TECH** security/survival books/manuals: Computers, Internet, Phones, Energy, Physical Survival, Financial, Law, Medical/Radionics, Mind Control, Weird/Paranormal. Free Online Catalog at: Consumertronics.net (PO 23097, ABQ, NM 87192), or $3 hardcopy (USA/Canada, $7 foreign). See display.

**SIX DIGIT LED CLOCKS** (with seconds); AC powered, highly accurate. Several models. Free catalog! Whiterock Products, 309 South Brookshire, Ventura, CA 93003. (805) 339-0702.-9169.

**CELL PHONE** cloning for the guy who has (two of) everything. Must have current service contract. For more info, call Keith (512)259-4770. 6426, Yuma, AZ 85366-6426.

**BUILD A RADAR JAMMER** out of your old radar detector. No electronic knowledge needed. Only $9.95 + $2.50 S&H Call 24fr. for easy step-by-step plans. 1-800-295-0953 Visa/MC/Dis.

**BOGEN FRIDAY FR-1000** all digital answering machines. An excellent all-purpose digital answering machine with 8 mailboxes (4 announcement only). Has a total recording time of 18 minutes. $52 each including shipping. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**ALL YOUR 802.11B ARE BELONG TO US** Unlike any other database system that exists since or during the period of "the collective" (2002), none other has given a return of the entire collective back to the submitter. The collective is not a mapping database system. It is a mechanism to exchange data in a cumulative fashion for such interested parties through anonymous assimilation. http://www.allyour80211barebelongtous.org/

**BLACKLISTED! 411 MEETINGS** We know some of the diehards kept the meetings going while we were out of print. Thanks guys!! You need to contact us and let us know the details of your meetings so we can list you in the magazine. For everyone else. Would you like to start up a meeting, yourself? It's fun, it's easy and you get a free subscription out of it. Tell us where you want it held and give us a contact name and number or email address. If you want your free subscription, you'll need to provide an address, of course. Think about starting a meeting yourself. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**SCIENTIFIC ATLANTA** 8580 $225, 8570 $250, 8550 $150, 8500 $120. Will program your 8550, 8500 EAROMS for $7.50. Cable security key gets past collars $25. Add $5 shipping. No TX sales. Send money order to: K. Perry, PO Box 816, Leander, TX 78646-0816. Phone: (512)259-4770.

**HEAR NON-COMMERCIAL SATELLITE RADIO** programs right in your area without the use of a dish or any other expensive receiving equipment. Thousands of these programs are operating today across America. Programs may include talks shows, weather, sport events, news feeds, financial reports, music programs and data ports. This technology is received through a high tech. SCSRT1 card. Find out today what you have been missing! (800) 944-0630. Credit card orders accepted.

**USED CELLULAR HANDHELDS:** Panasonic EB3500 portables, includes a battery (but no charger) forty number alpha memory, good working order, available as an extension to your existing line for $279, or as is for $129. Orders only: (800)457-4556, Inquiries to: (714)643-8426. C.G.C.

**HOME AUTOMATION.** Become a dealer in this fast growing field. Free information. (800)838-4051.

**TIRED OF SA TEST KITS** with marginal or inconsistent performance? 21st Century Electronics and Repair guarantees peak performance with 40-pin processor kits. New, more flexible program with additional features puts others to shame. Price $49 each or 5 for $233. 1st time offered. (404)448-1396

**FEDERAL FREQUENCY DIRECTORY!** Kneitel's "Top Secret" registry of government frequencies, New 8th edition. 268 pages! FBI, DEA, Customs, Secret Service, BATF, Immigration, Border Patrol, IRS, FCC, State Dept., Treasury, CIA, etc. & surveillance, bugs, bumper beepers, worldwide US military, 225 to 400 Mhz UHF aero band, Canadian listings, & more! Ultimate "insider's" directory! Standard reference of law enforcement, news media, private security, communications industry & scanner owners. $21.95 + $4.00 shipping ($5.00 to Canada). NY State residents add $2.21 tax. CRB Research Books, Box 56BL, Commack, NY 11725. Visa/MC welcome. Phone orders (516) 543-9169 weekdays (except Wednesday) 10 to 2 Eastern.

**TV CABLE/SATELLITE ("GRAY" MARKET) DESCRAMBLER EXPOSE,** 160pp, illustrated, with vendor lists for chips, parts. Law, countermeasures, much more! $23.95 + $3 S/H. Check/MO. INDEX, 3368 Governor Dr., Ste. 273, San Diego, CA 92122. Credit cards only: (800) 546-6707. Free catalog of "insider" books on scanners, cellular, credit, eavesdropping, much more.

**TOP SECRET SPY DEVICES** Home of the Worlds' Smallest Digital Voice Recorders and Spy Cameras. We stock many items including: Transmitters, Bug Detectors, Audio Jammers, Telephone Recorders, Lock Picks, Voice Changers, Keystroke Loggers. www.spydevicecentral.com (305)418-7510

**EUROZINES AND OTHER CULTURAL HACKER ZINES!** A one-stop, cutting-edge mail-order source for over 1,000 titles. Beautifully illustrated 128-page catalog includes: alternative/ fringe science, conspiracy, Forteana, sexuality, computer hacking, UFOs, and much more. Send $3.00 to Xines, Box 26LB, 1226-A Calle de Comercio, Santa Fe, NM 87505.

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

**FM STEREO TRANSMITTER KIT.** Transmitter broadcasts any audio signal from a CD player, VCR, or cassette player to FM stereo radios throughout your home and yard. Uses the unique BA1404 IC. Tunable across the FM band, runs on 1.5 to 12 volts CD. PC board/components, $24. Visa/MC. TENTRONIX, 3605 Broken Arrow, Coeur d'Alene, ID 83814. (208)664-2312.

**CALLING ALL WRITERS!** We want YOU to write for us. We're looking for articles related to the hacker "scene", technology reviews, opinions on issues, etc. If you submit an article for print and we use it, we'll pay you $25-$600, depending on length, content and the use of additional material such as (diagrams, photos, pictorials, schematics, etc). We require all photos to be 3.0megapixel or greater. JPG format is acceptable. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**TRUE TAMPER-PROOF** Security Screw Removal Bits. The super torx kit includes: T-10, T-15, T-20 & T-25. Complete set for $19.60. TOCOM 5503 bit $8.95. TOCOM 5507 bit $19.95. Zenith PM/PZ-1 bit $10.95. Jerrold Starcom bit $19.95. Pioneer (oval) bit $23.95. Oak Sigma (oval) bit $23.95. Security Screws available. Tamper-Bit Supply Co. (310)866-7125.

**CELLULAR RESTORATION** on your 800 Mhz scanner performed expertly for $40 including return shipping. Guaranteed. Offer expires soon. Keith Perry, 607 Osage Dr., PO Box 816, Leander, TX 78641. (512) 259-4770.

**6.500 MHZ CRYSTALS** $4 a piece, 50 for $115, 100 for $200. Add $3.00 for shipping. Send checks to C. Wilson, P. O. Box 54348 Philadelphia, PA 19105-4348

**SPECIAL SALE** amd 2400+ system with 256mb ram, 40gig hdd, 64meg int video w/agp slot and extremely portable case w/handle $450.00 + shipping handling. for details send email to xteraco@yahoo.com w/ subject special sale??

**OBSOLETE COMPONENTS** Are you looking for an old IC you can't seem to find anymore? We have a very wide variety of hard to find and obsolete components available. Check us out. Odds are, we have the part you need or can find it for you. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**COIN-OP VIDEO ARCADE GAMES.** Parts, boards, and empty cabinets available for your projects. Cabinets available for $75. C.J. Stafford, (301)419-3189.

**WANTED: FEATURE FILM JUNKIE** who can access up-to-date FAX numbers for hot agents and/or producers & directors. My objective: to bring to their attention my action-thriller script. Can pay by the hour. (909)275-9101

**THE BLACK BAG TRIVIA QUIZ: On MSDOS** disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes catalogs of selected (no junk) shareware and restricted books. Send $1.00 for S.25 disk, $1.50 for 3.5, plus two stamps, to: MENTOR PUBLICATIONS, Box 1549-W, Asbury Park NJ 07712

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

**ANARCHY ONLINE** A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers and phone phreaks. Scheduled hacker chat meetings. Encrypted E-mail/file exchange. WWW: hhtp://anarchy-online.com Telnet: anarchy-online.com Modem: 214-289-8328

**WAR DRIVING IS NOT A CRIME** The benign act of locating and logging wireless access points while in motion - Wardriving is NOT a crime, being stupid should be. http:// www.wardrivingisnotacrime.com/

**ARE YOU A PHOTOGRAPHER?** With the increasing number of high resolution digital cameras in the hands of our readers, we're actively recruiting people to submit photos to us. We're looking for 3.0megapixel or better digital photo's of technology, people using technology, events, devices, utility personnel, utility vehicles in action (or doing nothing at all), tradeshows, technology swap meets and hacker meets. If it's related to hacking in any way, we want photographs!! Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**HACK THE PLANET** A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. Hand-scanned 99XX exchanges in 516 AC. Included may be data kit modem numbers, WFA/FA, SSCU, TSAC(SCC), CO#'s, etc. Send $2.00 check or money order payable to CASH and specify exchange. "MCI-Style" Phone Patrol hats are now available! Just $18 check or money order payable to CASH. 2447 5th Ave, East Meadow, NY 11554.

**ATTENTION HACKERS & PHREAKERS.** For a catalog of plans, kits & assembled electronic "TOOLS" including the RED BOX, RADAR JAMMER, SURVEILLANCE, COUNTER SURVEILLANCE, CABLE DESCRAMBLERS & many other HARD-TO-FIND equipment at LOW PRICES. Send $1.00 to M. Smith-02, P.O. Box 371, Cedar Grove, NJ 07009

**PRIVACY ACT AND SOCIAL SECURITY NUMBER LIMITATIONS**, How anyone can win $10K fine for this simple violation of your rights. Open a bank account without a SSN $5 plus 3 F/C stamps. Obtain a major credit card without a SSN (making it impossible for a bank or any institution to check your credit history or records) $25 plus 5 F/C stamps. For info send $1 and LSASE to: Know Your Rights, c/o R. Owens, 1403 Sherwood Dr., Bowling Green, KY 42103. NO CHECKS PLEASE. M/O or FRN's only.

**HARD TO FIND 6502 6800 68000** Microprocessors. We have a wide array of very hard to find microprocessors and micro support devices available. If you need it, we probably have it. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**VOICE CHANGING ACCESSORY.** Digital voice changing: male to female, female to male, adult to child, child to adult. Use with any modular phone. 16 levels of voice masking. Connects between handset and phone. STOP THOSE ANNOYING TELEPHONE CALLS! Sound older and tougher when you want to. Not a kit. Fully assembled. Use with single or multi-line phones. 30-day refund policy. Ask for free catalog of our products. VISA/MC ok. Xandi Electronics. 1270 E. Broadway, Tempe AZ 85282-5140. Toll Free order line: (800)336-7389. Technical Support: (602) 894-0992

**MAGENCODERS.COM** Manufacturer of the World's Smallest Portable Magnetic Card Reader & Point of Sale Data Loggers. We also have Magnetic Stripe Reader/ Writers, Smart Card Loaders & Copiers, etc... (407)540-9470

**UNDETECTABLE VIRUSES.** Full source for five viruses which can automatically knock down DOS & windows (3.1) operating systems at the victim's command. Easily loaded, recurrently destructive and undetectable via all virus detection and cleaning programs with which I am familiar. Well-tested, relatively simple and designed with stealth and victim behavior in mind. Well-written documentation and live antidote programs are included. Priced for sharing, not for making a ridiculous profit. $10.00 (complete) on six 1.44MB, 3.5" floppy discs. Money orders and checks accepted. No live viruses provided! Do NOT ask. Satisfaction guaranteed or you have a bad attitude! The Omega Man. 8102 Furness Cove, Austin, TX 78753

**NO SOUND ON PREMIUM CHANNELS?** It will happen sooner or later on your Jerrold DPBB-7 Impulse. Ask Manhatten! Soundboard brings the sound back. Best sound fix on the market. Easy to install soundboard $24.95. Easy to build soundboard schematic, parts list and common chip number $34.95. Send us your unit and we will install the soundboard for $59.95. SOUNDMAN, 132 North Jardin St., Shenandoah, PA 17976. (717) 462-1134.

**BAD CREDIT? WANT/NEED A VISA CARD?** If so, send us $19.95 (cash/check/MO) and we will send you a very useful list of addresses and phone numbers of banks and financial institutions that *WILL* work with you. Most will give you a VISA credit card regardless of your credit rating. We even include a few banks that will require a deposit, just to "round out" the list a bit. For an additional $10 we will include a small "how-to" program showing you step-by-step how to improve your credit rating and dealing with creditors. You might think that your bad credit doesn't mean anything right now.. Wait until you need to buy a house or a car, then you'll see how much you REALLY need to have GOOD CREDIT. So, get back on track. Buy our list and the how-to program and start your way back into a good credit status. Cash or money order. TCE Information Systems. P.O. Box 5142, Los Alamitos, CA 90721.

**SINGLE DUPLICATION OF CD-ROMS** Send your CD and $25 and you will receive your CD and an exact copy. Want more than one copy? Send a additional $15 for each duplicate. Make checks or money orders Payable to/Mail to: Knoggin, 582 Merket Street Suite 616, San Francisco, CA 94114

**LOOKING FOR A BLACKLISTED! 411 MEETING IN YOUR AREA?** Why not host one yourself? It's easy. Tell us where you want it held and give us a contact name and number or email address. If you want your free subscription, you'll need to provide an address, of course. Think about starting a meeting yourself.

**FIND PIRATE SOFTWARE** Learn how to find pirate software on the Internet. Get thousands of dollar's worth of programs for free such as Office97 and more games than you can play. Complete guide includes background, tools, techniques, locations, and shell scripts that will find software for you! Send $5.00 money order or CASH (no checks) to The Knoggin Group, P.O. Box 420943, San Fransisco, CA 94121-0943, USA.

**RAM DRAM SRAM GALORE** We have many hard to find memory devices available. If your project requires old RAM not available any longer, check us out. We have a very wide selection of RAM to choose from. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**CB RADIO HACKERS GUIDE!** New! Big 150 pages; pictorials, diagrams, text. Peaking, tweaking and modifying 200 AM and SSB CB radios. Improved performance, extra capabilities! Which screws to turn, which wires to cut, what components to add: Cobra, Courier, GE, Midland, Realistic, SBE, Sears, Uniden/President. $18.95 + $4 S&H ($5 Canada.) NY State residents add $1.96 tax. CRB research, Box 56BL, Commack, NY 11725. Visa/MC accepted. Phone order M-Tu-Th-F, 10 to 2 Eastern time. (516) 543-9169.

**S-100 BUSS CARDS** for sale. I have piles & piles of S-100 cards I'd like to sell off at $15 each. Vector, Corvus, SpaceByte, Cromemco, Heath, etc. Please contact me for a complete list of available items. techgathering@comcast.net

**AUCTIONS!** You hear about them all the time, but you've never been to one? You gotta GO to one. You can buy just about anything for pennies on the dollar! Cars, trucks, boats, houses, electronic equipment, furniture, etc. Forget that "cars for $100" crap. That's a load! But, you can get some pretty awesome deals for small amounts of cash.. Our favorite auctions (and many of the BL411 staff) include the arcade auctions and the car auctions. Remember those arcade games you played as a kid in the 80's? Man, you can get some bitchen deals on those! This is only the tip of the iceberg. There's SO MANY things you can get for a small fraction of their worth. Send $5 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! So send $5 right NOW: TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721.

**WE WANT WRITERS!** That's right! We want YOU to write for us. The people at Blacklisted! 411 are currently seeking freelance writers to increase the quality and scope of the magazine. We're looking for quality articles related to the hacker "scene", events, technology reviews, opinions on issues, etc. If you submit an article for print and we use it, we'll pay you $25-$600, depending on length, content and the use of additional material such as (diagrams, photos, pictorials, schematics, etc). We require all photos to be 3.0megapixel or better. JPG format is acceptable. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**NULL MODEMS** - Download laptop: or upload to your pc the easy way! w/ direct connect, or (DOS 6.1) Customized setup, no bulky adapters, MAC or IBM compatibles. Send $18.95 for 6ft cable, specify 25 or 9db ends, custom ok. Instructions included. P.O. Box 431 Pleasanton, CA 94566 (510)485-1589

**NEW BOOK FOR CABLE HACKING.** All about the industry and how to install test chips in nearly every model of decoder. Test chips available, Etc. (408)581-2380

**SECURITY SCREWDRIVER BIT SET** Our best selling 30 piece screwdriver bit set is now available for $40 including shipping to anywhere in the U.S. The set includes 9 security Torx bits from TT7 through TT40, 7 security Hex bits from 5/64" through 1/4", 4 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 you'll wonder how you ever did without! TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

**DON'T BUY A MODIFIED CABLE CONVERTER!** I'll show you what to do. Where to get parts, everything. Call 24hr.. 1-800-295-0953 Only $9.95 + $2.20 S&H Visa/MC/Dis.

**SPEECH CHIPS - WE GOT 'EM** Yes, we have hard to find speech chips. We have General Instruments SPO250, SPO256, Votrax SC-01, Harris HC-55532, Texas Instruments TMS5220NL, TMS5220CNL and more. Come and check us out. We have a wide selection to choose from. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**HACKERS '95 THE VIDEO** by Phon-E & R.F. Burns: See what you missed at Defcon III and Summercon 95! Plus, our trip to Area 51 and coverage of the "CyberSnare" Secret Service BUSTS. Elec Cntr Measures, HERF, crypto, and more! Interviews with Eric BlookAxe, Emmanuel, and others. VHS 90 min. Only $25 - distributed by Custom Video 908-842-6378.

**HACKERS SCREWDRIVER BIT SET** Brand new for 2004! Our newest selling 60 piece security screwdriver bit set is now available for $55 including shipping to anywhere in the U.S. The set includes 3 Spline bits M5 through M8, 4 scrulox (square) bits S0 through S3, 3 torq-set bits 6 through 8, 12 security torx T-5 through T-40, 13 security hex bits 2mm through 5/32", 5 tri-wing bits 1 through 5, 3 posidrive bits PZ0 through PZ2, two flat bits 1/8" and 3/16", 3 phillips bits 0 through 2, 5 spanner bits 4 through 12, 3 bowtie bits C1 through C3, triangle bit 2mmx2mmx2mm, wing nut driver, 1/4" x 60mm bits holder, bit holder socket, socket adaptor, ratchet screwdriver and a covered plastic case. This is an extremely handy toolset no hacker should be without! TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

**SPEECH CHIPS - WE GOT 'EM** Yes, we have hard to find speech chips. We have General Instruments SPO250, SPO256, Votrax SC-01, Harris HC-55532, Texas Instruments TMS5200NL, TMS5220NL, TMS5220CNL and more. Come and check us out. We have a wide selection to choose from. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**A TO Z OF CELLULAR PROGRAMMING.** Programming instructions on over 300 phones in a software database. Also back door and test mode access instructions for all the popular models; manufacturer's contacts, system select, lock/unlock info. Just $59.95. Orders only: (800)457-4556, inquiries: (714)643-8426. C.G.C.

**WE NEED ARTISTS!** We're actively recruiting people to submit artwork to us. We're looking for freehand as well as computer artwork of technology, people using technology, events, devices, utility personnel, utility vehicles in action (or doing nothing at all), tradeshows, technology swap meets and hacker meets, comics, etc. If it's related in any way, we want artwork!! Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**GAMBLING MACHINE JACKPOTTERS** We offer a complete range of gambling products designed to cheat gambling machines as well as other games. Our products are designed to demonstrate to gambling machine owners the vulnerabilities of their machines. Our product line consists of Gambling Machine Jackpotters, Emptiers, Credit Adding Devices, Bill Acceptor Defeats and Black Jack Card Counting Devices. Please visit www.jackpotters.com

**ADVERTISE IN BLACKLISTED! 411** Classifieds are now FREE for everyone. 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. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**KEYSTROKEGRABBERS.COM** Manufacturer of discreet keyboard logging hardware. Our devices capture ALL keystrokes on a computer including user name and password. PARENTS---Monitor your child's internet, e-mail, instant messaging and chat room activity. EMPLOYERS---Monitor employee computer usage compliance. Employees will spend less time browsing the internet and sending e-mails if they are being monitored. EXECUTIVES & SYSTEM ADMINS---detect any unauthorized access of your PC. If someone uses your computer after hours, you will know. (305)418-7510

**ADAPTEC SCSI CARDS** for sale. We have AHA-2940, AHA2940UW, AHA-2944, etc. $20-$30 each. We also have brand new 3' and 6' SCSI cables $2-$4 each. DB25-to-SCSI, SCSI-to-SCSI II, etc. We also have brand new Belkin 15' IEEE printer cables $3 each. Shipping extra. We have a wide selection of SCSI products to choose from at low, low prices. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**INTEL SDK-85 SYSTEM DESIGN KITS** available here. I've been collecting this stuff for years. They're in GREAT condition. $100 each plus shipping. If you're interested, please contact me ASAP. techgathering@comcast.net

**MAKE MONEY NOW, HACKERS!** Have an interesting story to share? Write for us and make some money. Have some cool photo's of something nobody has seen? Send it to us and get PAID! Doodle on paper all the time and wish you could catch a break...along with a paycheck? Draw for us and make $$$! Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

**ZINE PUBLISHER RESOURCE BOOK** If you're thinking about publishing or already started publishing a zine, you need this resource booklet. Discover who you can distribute your zine through and make more money. Send $14.95, cash or money order only. TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

**CELLULAR EXTENSIONS, SEND US YOUR PHONE** or buy a new or used phone from us! Proof of line ownership required. We have phones from $129. Call for a list of available models, we program many different brands including all Motorola, same day service. Orders only: (800) 457-4556, inquiries to: (714)643-8426. C.G.C.

**WANTED: OLD COMPUTERS** for my collection. Looking for Commodore, Atari, Amiga computers, accessories, books, cables, software. If you have something like this that you no longer want, please contact me ASAP. techgathering@comcast.net

**NEW BOOK ON HACKING** We're going to put together a hard cover book full of interesting stories from hackers, crackers and phreakers. If you have a story to share, please send it to us along with some contact information (ie: name, address, email, phone number - we won't publish this information), your handle/alias/pen-name for print. The longer the story, the better. We'd like factual stories, but we'll consider fictional stories as well. If you have any suggestions on the topic of this book, we'll consider your ideas. Once the book is complete, each person who submitted material we use will get a FREE copy of the book. Please send your material to: Blacklisted! 411 Book Project, P.O. Box 2506, Cypress, CA 90630.

**ATARI/BALLY/WILLIAMS ARCADE PARTS** We stock hard to find parts for your arcade games. We have custom ROMs, PROMs, custom sound and speech chips (AY-3-8910, AY-3-8912, AY-3-8913, HC-55532, TMS5200, TMS5220, SC-01, SPO250, SPO256, LM379, etc), custom video chips (TMS9928), custom Atari chips (AVG, SLAG, SLAPSTIC, POKEY, etc), custom Namco chips, custom Williams "Special Chip 1", D-to-A and A-to-D converter chips (AD561JD, AM6012, AD7533, ADC0804, ADC0809, etc), Atari LED buttons, Keltron brand Cinematronics flyback transformers, trackball roller repair kits, 6500, 6800 and Z80 series CPU's and support chips. We even carry manuals and schematics. We have a wide selection of arcade parts to choose from. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

**CHIP COLLECTOR / SALVAGE SOURCEBOOK** Have you ever looked online for some collectable components or vintage electronic equipment, only to find out that it's cost is way too high? This sourcebook will provide you with the ability to locate the same items at only a small fraction of the bloated online cost. Buy collectable gold chips (Intel, Motorola, Zilog, National Semiconductor, etc) for $20-$40/lb. Do you have any idea how many chips are in a single pound? More than enough to make this sourcebook worth a peek! Find that Intel C4004 you've been looking for and pay pennies, not hundreds of dollars. Grab a few thousand EPROMs and pay a few bucks a pound, not a few bucks per EPROM!! Find older high end EPROM programmers for $20-$30, not $200-$300! The deals are many, the price is minimal. You'll be glad you got yourself a copy of this sourcebook and wonder how you ever did without! Send $19.95, cash or money order only. TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

**BUILD YOUR OWN REPLICA APPLE I** 8-bit computer! The replica 1 is a functional clone of the first Apple computer. Prices start at $129. See www.vintagecomputer.tk for more details.

**Marketplace classified advertising is currently FREE to anyone. It's a first come, first served offer, limited only by space constraints within each issue. If you'd like an ad placed within Blacklisted! 411, you should send it in as soon as possible. We accept both commercial as well as personal ads. We may decide not to publish any ads which are inappropriate or have no connection with the hacker community.**

***CONTACT US AT: www.blacklisted411.net***

# MONTHLY MEETINGS

Interested in meeting up with some of the Blacklisted! 411 readers? We will list all hacker meeting information that is provided to us. We will list "Blacklisted! 411" only meetings as well as "independent" meetings open to all.

## California

*(949 Area Code) - Irvine*

iHop - By Airport (Upstairs Room), 18542 MacArthur, Irvine, CA. 92714 - Meeting is not Blacklisted! 411 specific. The meeting date may change from month to month. For specifics, check here: www.irvineunderground.org

***Hosted by: Freaky***

## New Mexico

*(505 Area Code) - Albuquerque*

Winrock Mall - Louisiana at I40, food court, east side doors under the security camera dome.

First Friday of the month, 5:30pm—9:00pm

***Hosted by: Mr. Menning***

*(505 Area Code) - Albuquerque*

The computer room in the Grand Reserve Apts. at Maitland Park

Last Friday of the month, 12:00pm—1:30pm

***Hosted by: Whisper***

## YOUR MEETING HERE

**Want to set one up? Contact us and give us your information in a similar format to the meeting info. listed here.**

---

**We removed all of the hacker meetings we could not confirm were still in existence. If you're still running a meeting, contact us right away and we'll get you listed here on this page.**

**If you are interested in organizing a new meeting in your area, please contact us, advising us of your interest, where you're located, where you would like to hold the meetings, etc. (Be sure to include your contact name, area code, city, state, day of month and time as well as a description of meeting location). Also include contact information for our use such as: *name, phone number, address, email, etc.***

# G.I. ELECTRONICS

**YOUR BEST SOURCE FOR HARD TO FIND AND OBSOLETE COMPONENTS**
**WWW.GIELECTRONICS.COM**

## DRAM/SRAM

| | |
|---|---|
| 1101 | $15.00 |
| 1103 | $15.00 |
| 2016 | $5.00 |
| 2101 | $8.00 |
| 2102 | $10.00 |
| 2104 | $8.00 |
| 2107 | $15.00 |
| 2114 | $5.00 |
| 2115 | $15.00 |
| 2117 | $12.00 |
| 2128 | $6.50 |
| 2147 | $7.00 |
| 2148 | $8.00 |
| 2149 | $9.00 |
| X2212 | $35.00 |
| 27S03 | $5.00 |
| 4016 | $6.50 |
| 4027 | $4.00 |
| 4116 | $4.00 |
| 4118 | $10.00 |
| 4164 | $4.00 |
| 4416 | $5.00 |
| 4801 | $10.00 |
| 5101 | $10.00 |
| 5114 | $25.00 |
| 6116 | $6.00 |
| 6264 | $7.00 |
| 9101 | $8.00 |
| 9128 | $6.50 |
| 74S89 | $5.00 |
| 93415 | $15.00 |
| 93419 | $10.00 |
| 93422 | $15.00 |
| 82S09 | $15.00 |

## SOUND/SPEECH

| | |
|---|---|
| AY-3-8910 | $15.00 |
| AY-3-8912 | $15.00 |
| AY-3-8913 | $15.00 |
| CO12294B | $15.00 |
| LM379S | $25.00 |
| MB3730 | $35.00 |
| SC-01 | $45.00 |
| SPO250 | $35.00 |
| SPO256 | $35.00 |
| TDA1004 | $25.00 |
| TDA2002 | $15.00 |
| TMS5200NA | $25.00 |
| TMS5220NA | $25.00 |
| TMS5220NL | $25.00 |
| TMS5220CNL | $30.00 |
| HI55532 | $55.00 |

## Z80

| | |
|---|---|
| Z80 | $2.00 |
| Z80A | $4.00 |
| Z80B | $6.00 |
| Z80-CTC | $2.50 |
| Z80A-CTC | $4.50 |
| Z80B-CTC | $6.50 |
| Z80-PIO | $3.00 |
| Z80A-PIO | $3.50 |
| Z80B-DART | $3.00 |
| Z80A-DART | $3.00 |
| Z80-SIO/0 | $4.00 |
| Z80A-SIO/0 | $4.00 |
| Z80B-SIO/0 | $4.00 |
| Z80-SIO/2 | $4.00 |
| Z80A-SIO/2 | $4.50 |
| Z84C00-4 | $8.00 |
| Z8530 SCC | $6.00 |
| Z8603RS | $20.00 |
| Z8613RS | $25.00 |

## 6500

| | |
|---|---|
| 6502 | $5.00 |
| 6502A | $6.50 |
| 6502B | $8.00 |
| 65C02 | $8.00 |
| 6504A | $8.00 |
| 6507 | $8.00 |
| 6510 | $8.00 |
| 6512 | $8.00 |
| 6520 | $8.00 |
| 6522 | $6.00 |
| 65C22 | $8.00 |
| 6525 | $8.00 |
| 6526 | $7.00 |
| 6529 | $7.00 |
| 6532 | $8.50 |
| 6551 | $6.00 |
| 6551A | $6.00 |
| 65C51 | $6.00 |

## PROM

| | |
|---|---|
| 82S23 | $15.00 |
| 82S123 | $8.00 |
| 82S126 | $8.00 |
| 82S129 | $8.00 |
| 82S130 | $9.00 |
| 82S131 | $8.00 |
| 82S137 | $9.00 |
| 82S140 | $16.00 |
| 82S141 | $16.00 |
| 82S147 | $20.00 |
| 82S153 | $25.00 |
| 82S180 | $12.00 |

## 6800/68000

| | |
|---|---|
| 6800 | $4.00 |
| 6802 | $10.00 |
| 6803 | $9.00 |
| 6808 | $12.99 |
| 6809 | $8.00 |
| 6809E | $8.00 |
| 6810P | $2.99 |
| 6810 | $9.99 |
| 6821 | $5.00 |
| 68B21 | $5.00 |
| 6840 | $6.00 |
| 6850 | $4.00 |
| 68000P8 | $4.99 |
| 68000P10 | $5.99 |
| 68000P12 | $6.99 |
| 68000L8 | $14.99 |
| 68000L10 | $16.99 |
| 68000L12 | $17.99 |
| 68008 | $10.00 |

## EPROM/EEPROM

| | |
|---|---|
| 2516 | $10.00 |
| 2532 | $16.00 |
| 2564 | $15.00 |
| 2708 | $15.00 |
| 2716 | $10.00 |
| 27C16 | $8.00 |
| 2732 | $12.00 |
| 2732A | $10.00 |
| 27C32 | $8.00 |
| TMS2732 | $11.00 |
| TMS2732A | $11.00 |
| 2764 | $4.50 |
| 2764A | $4.50 |
| 27C64 | $2.00 |
| 27128 | $3.50 |
| 27128A | $3.50 |
| 27C128 | $2.50 |
| 27256 | $4.50 |
| 27C256 | $2.00 |
| 27512 | $5.50 |
| 27C512 | $2.50 |
| 27C010 | $5.00 |
| 27C010A | $5.00 |
| 27C020 | $8.00 |
| 27C040 | $9.00 |
| 27C080 | $9.00 |
| 27C1024 | $6.00 |
| 27C2048 | $8.00 |
| 27C4096 | $10.00 |
| NC7055 | $35.00 |
| ER2055 | $35.00 |

## SPECIAL SERIES

| | |
|---|---|
| MC1495 | $8.00 |
| AM2901 | $8.00 |
| AM2903 | $20.00 |
| AM2907 | $8.00 |
| AM2909 | $8.00 |
| AM2910 | $8.00 |
| AM2911 | $8.00 |
| AM2914 | $15.00 |
| AM2960 | $15.00 |
| AM2964 | $14.00 |
| AM29116 | $20.00 |
| AM29516 | $20.00 |
| AM29701 | $8.00 |
| TMS9927 | $35.00 |
| TMS9928 | $45.00 |
| DG201 | $4.50 |
| LF13201 | $4.50 |
| LF13331 | $9.95 |
| CD4016 | $1.50 |
| CD4066 | $2.00 |
| LM324 | $6.50 |
| LM3900 | $6.50 |
| TL081 | $3.50 |
| TL082 | $3.50 |
| TL084 | $4.00 |
| WD1010 | $15.00 |
| WD1014 | $15.00 |
| 1771 | $15.00 |
| 1791 | $15.00 |
| 1793 | $15.00 |
| 1795 | $15.00 |
| 1797 | $15.00 |
| 2793 | $21.00 |
| 2797 | $21.00 |
| DSP32010 | $15.00 |
| TMS32020 | $15.00 |
| TMS38010 | $15.00 |
| TMS4500A | $15.00 |
| TMS5501NL | $45.00 |
| TMS5502NL | $45.00 |
| 8X300 | $15.00 |
| 8X305 | $15.00 |
| G171S-35C | $10.00 |
| N3002I | $35.00 |
| NS32201 | $10.00 |
| NS32203 | $10.00 |
| P4004 | $40.00 |
| D4004 | $70.00 |
| INS4004 | $60.00 |
| P4001 | $20.00 |
| P4002-1 | $20.00 |

**WWW.GIELECTRONICS.COM**

GI ELECTRONICS, P.O. BOX 11029, WESTMINSTER, CA 92685