Blacklisted 411

The Official Hackers Magazine

Hack The System...

WWW.BLACKLISTED411.NET

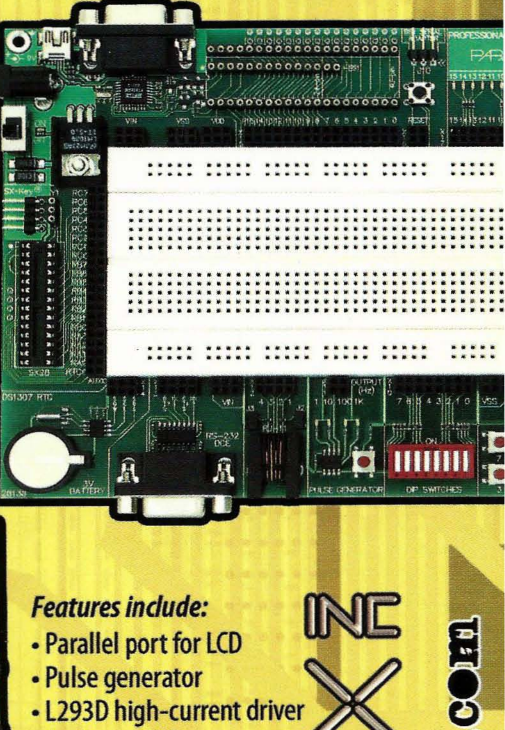
Current News

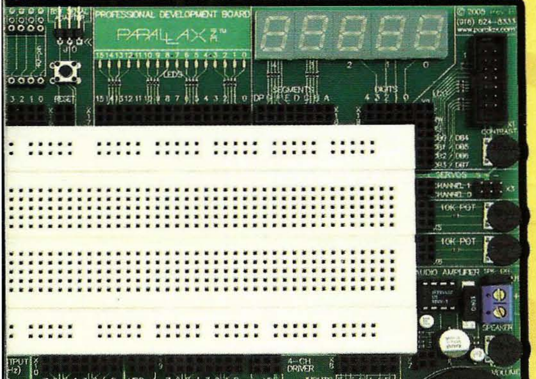
.NET Edition 4 Released
New SWAG for 2006 Now Available
Blacklisted Membership Cards Released

Inside This Edition

The Art of Electronic Deduction
Swinging for Fun and Profit
Port Knocking Simplified

VOLUME 8 ISSUE 1 WINTER 2005-2006





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

Web Admin
Ustler

Writers
Ustler, Israel Torres, Unicoder,
Dr. Fibes, Jeremy Martin,
The Goldfinger, dual_parallel,
MobbyG, Cactus Jack, ML Shannon,
Grandpa Hackman, Electra-Solve

Inside this issue

Additional information

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

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

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**

ISSN 1082-2216

All opinions and views expressed in Blacklisted! 411 Magazine are those of the writers of the articles, and do not necessarily reflect the views or opinions of any Syntel Vista, Inc. staff members or it's editors.

9035768ABBAJBVJB-0025

DBBL 01,07,32,41,52

PRINTED IN THE UNITED STATES OF AMERICA

Icons used on the front cover are from Dropline Neu! created by Silvestre Herrera and are released under the GNU General Public License (GPL). A full copy of the license and icons can be located at http://www.silvestre.com.ar/or available on request as required.

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. They were all deeply interested in their Atari, Apple and Commodore computers, electronics, sciences, arcade games, etc. They built projects, hacked into various things, made their own programs, 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 (at the time) without all the cool toys we take for granted today. There was no internet to utilize and nobody had printers which could print anything other than plain text (and didn't even do that well). With a disk based system, text files, primitive graphics/pictures, and utilities were fairly easy to distribute and it could be copied by anyone who had a compatible computer. At our peak, at least 150 disk copies <per month> of the disk magazine were sent into the public, though there is no way to know how many were copied by others.

Eventually modems caught on and the magazine was distributed through crude BBS systems. Using the power of a Commodore 64, a *Blacklisted! 411* info site, which anyone could log into without handle or password, was created and operated. It was a completely open message center. Using X-modem or Punter file transfer protocols, one 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". There was only one message center, no email capability & only 1 phone line. Primitive, indeed. Effective, however.

Around 1984, the purchase of a 9 pin dot matrix printer that could <gasp> print basic graphics was entered into the mix. Printing out copies of the *Blacklisted 411 monthly* and copying them at the media center at the high school became the new "experiment". The media center staff graciously allowed the production of these copies free of charge which was very cool at the time. The copies were passed 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). Piles of the magazine were left anywhere and everywhere people could see them. One popular location was next to the Atari Gauntlet and Gauntlet II arcade games strategically located at 7-11's all over the place. It's been a longtime myth that people photocopied those original 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 they were left, they were taken - and taken quickly! The feedback was awesome in that people wanted more. The interest was very high, but the inability to meet this growing demand was completely overlooked. The plug was officially pulled on the printout experiment and distribution through diskettes remained the norm. It was really the easiest way to go at the time. 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 disks were still being released at this time.

June of 1987 marked the end of *Blacklisted! 411, the hackers monthly*. The last disk based magazine (# 46) was distributed that month. Since all of the original crew were finally 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, it was assumed that this was the end and *Blacklisted! 411* would never be resurrected in any form.

In the summer of 1993, one member (and the original editor-in-chief), Zachary 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 and he was alone. 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, the will to make it happen, 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. Regardless, the related user meets were packed! The interest in the magazine was great. After a year passed, it was decided to try a quarterly format in an effort to increase distribution. During that year Zachary managed to get in contact with many of the old group members, most of whom which are active staff members even today.

In 1999, what was to be the last issue of *Blacklisted! 411* (Volume 5, Issue 4) was published. It was unknown at the time, but many pitfalls would ultimately cause the demise of the magazine. Officially, it was dead as a doornail. After 4 years of regrouping and planning, *Blacklisted! 411* magazine was resurrected yet again..

To date, Blacklisted! 411 is 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. Hanging onto the very same hacker mentality and code of ethics from the 80's, Blacklisted! 411 stands apart from the rest. Their ideal is that hackers are not thieves - they're curious people who are the makers and shakers of the technology sector. They're not elitist hackers by any means and believe that no question is ever a "stupid" question. Old school hackers and newbie hackers alike, Blacklisted! 411 caters to you.

What' about now...

Community

The last two years have been an exciting time for the staff and crew over here. We have become extremely active in the hacker community. As we are based in the Los Angeles area, we have built relationships with the local Hacker groups such as LA2600, SD2600, twentythreedotorg, Irvine Underground and many others. We have been attending and sponsoring Hacker Conventions and Conferences such as the Layer One Convention and the ever popular Defcon. You can find us attending these conventions regularly. We usually run a vendor booth at these events and we make available our wares - subscriptions, back issues, t-shirts, hats, stickers and other SWAG. We also provide several "convention only" promotions such as the Apple IPOD give-away we held at DefCon 13. Our give-away was a big hit. We're planning on attending DefCon 14 this year and we'll be holding our own private catered reception for subscribers and supporters. Additionally, we'll be handing out membership cards with all new subscriptions this year. Whatever you do, be sure to check out our booth first, you'll be glad you did!

Magazine Development
A major effort has been made to increase our exposure to the hacking and information security community. Our distribution goals for the magazine was to break 100K copies distributed each quarter sometime in 2004 and we far surpassed our goal within our timeframe.. To date, Blacklisted! 411 has a circulation over 200,000 copies per issue. Based on orders from distributors and sell through, we're doing excellent in the marketplace. Additionally, we have been seeking and hiring freelance writers, techs, photographers, and editors to increase the quality and scope of the magazine. We've also been promoting the magazine outside of our community to bring in cross-over readers.

Merchandising / SWAG
We now have a whole series of *Blacklisted! 411* themed swag and merchandise. This currently includes stickers and apparel, but will soon include posters, a new DVD, gadgets and technology.....whatever our creative minds can come up with. Ideas and suggestions on this subject will be accepted and appreciated.

Charities
People generally believe that hackers are awful scum-sucking low life degenerates not fit to inhale the air they breathe. This idea has been pounded into the heads of people repeatedly by the mainstream media. Not necessarily because they're evil-doers, but more likely due to the fact that they simply have no idea what hackers are or what we're all about.

They think we're an uncaring bunch of thieves. They couldn't be any further from the truth. Hackers do care. In fact, they probably care more about the things that really matter than your average Joe does.

Blacklisted! 411 is owned and operated by real people who care about things aside from hacking. No, really. In the spirit of helping people and organizations outside of our community by offering real support, not only have we done a good deed, but we've demonstrated our philosophy at it's core level. We want to help. As such, *Blacklisted! 411* Magazine has officially donated to several local charities in an effort to achieve this goal.

First and foremost is the local chapter of the Ronald McDonald House. Many people have never even heard of this place, but nevertheless, they're a wonderful bunch of people who offer an amazing service to those less fortunate families who have a child in the hospital....they offer a place to stay and a hot meal - for FREE (or a very small donation if you can afford it). We've donated many items to help their cause because we really believe in it. One of our favorite donations was the 200 some odd small children costumes we supplied them with to give to the children around Halloween. If you have children of your own, maybe you can appreciate this place a little better. *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. The festival they operate is much like a small carnival with rides, food, drinks, and entertainment. They also run a huge raffle which is right up our alley as far as lending a helping hand goes. We've been able to supply them with some unique and stunning prizes for the children who attend the festival. Prizes you wouldn't expect to win for a cheap raffle ticket.

Our hope is that we were able to brighten up the day for some children, maybe even a family or two....and help our community at the same time.

Of course, we also donate to EFF and other hacker-friendly groups. That really goes without saying, right?

Closing thoughts
Let's start our closing thoughts by mentioning that we're your friendly neighborhood hacker magazine. We're one of the team players and happy to help people. Please don't feel that you cannot approach us.

So, if you have questions, comments, articles, ideas, suggestions, have a business proposition or wish to offer support in some way, please contact us and let's see what we can come up with. Thanks for your support, hackers!

BL411

Important notes of interest:

SWAG NOW AVAILABLE
That's right! We have SWAG now. We have some cool "Hack the System" T-shirts and baseball caps, plus a wide variety of bumper stickers available at our online store. We'll soon have some additional SWAG and technology available as well. Keep watching. www.blacklisted411.net

DEADLINES
For some reason, people seem to miss our deadline mention in the magazine and online, so be sure to read this. The DEADLINE for articles, letters, artwork and ads for Volume 8, Issue 2 is April 1st, 2006. Got that? APR 01 2006

ADVERTISING
People often email us asking if classifieds are free. We keep telling everyone YES. Classifieds are free. If you have a classified you want us to run and it's topic related to the magazine, send it in and we'll consider it. Ads are limited to space constraints per issue. First come, first served. Naturally, we reserve the right to reject advertising for any reason.

ARTICLES
Do we really need to mention this one? We're a magazine and we NEED articles. If you're a writer and want us to consider your work, send something to us. Don't waste any time. We're a PAYING MARKET. What does that mean? It means that we pay for articles which we use...but only if you want the $. We can donate your payment to your favorite charity if you'd like. Our rates are generally $75-$100 a page, depending on size, quality & use of photos.

ONLINE CONTENT
If you haven't noticed it yet, we have a website (www.blacklisted411.net) and we like to fill our pages with interesting, topic related content. If you'd like to write articles/reviews for use on our website, send them in.

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

By now, I'm certain you've noticed the changes made to our cover. That seems to be the theme around here lately. Change. We've been making sweeping changes to everything from the office we work out of and the products we offer to the cover of our magazine and the look of our website.

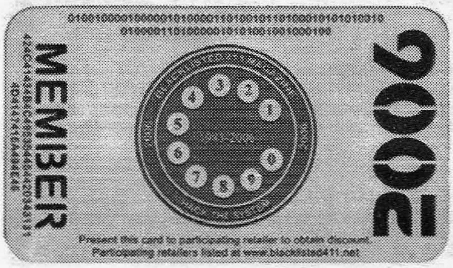
We recently made a move to a new location which has had its ups and downs. Needless to say, the move has given us an opportunity to clean up and make some most required changes to the way we operate.

Have you ever taken on the task of an office relocation? It's not a pretty proposition, at least for us anyway. It's quite amazing just how much "stuff" a group of hardware hackers can accumulate over a few years. I've come to realize that the whole bunch of use over here are nothing less than packrats….and not you're every day variety, either.

During our initial packing, the most unbelievable pieces of techno-history were unearthed. I found a nice stack of ancient SBC's (Single Board Computers) lodged behind my desk of all places! Packed away in one of our technology stashes, we found some of the very-early hardware hacking projects I personally headed up back in the early to mid 80's, my favorite being the 128MB RAM "cube" (named for the shape of the finished contraption) which was a solid state RAM drive for the Commodore 64/128 series. It may not seem like much now, but in 1983, 128MB was nearly unheard of, especially for home computer users. In all it's glory, this multi-board, wire-wrapped behemoth has become a very effective dust collector. Many other items of similar interest were located during the move. I'll write more about them later.

Since we're almost settled in at our new digs, we've had some time to put on our thinking caps and come up with several new ideas and plans for 2006. Honestly, I think 2006 is going to be one hell of a year for the magazine and our readers. I'll tell you about a few of the more interesting projects we have going on and you can be the judge.

Something new over here is our membership card program. You're probably wondering, "membership card? What? Why??" I'll tell you what it is, why we're doing it and why it'll be good for you. First, the What. The card is a small card about the size of a standard business card And get this, it's made from stainless steel. Yeah, it's metal! Some graphic details are etched, others are punched completely through. The card looks like this:


MEMBER
3
2
1
4
5
6
0
7
8
9
2006
Present this card to participating retailer to obtain discount.
Participating retailers listed at www.blacklisted411.net

Please note that the "black" parts of the card are punched through, the "gray' parts are etched. The end result is a pretty cool looking card.

Now, the why. First reason, because it's just cool and nobody else is doing it. Second, to give our subscribers something special they can enjoy. Last reason, networking. No, not computer networking. We've started the process of networking with a crapload of "hacker friendly" retailers who will give discounts to anyone presenting them with this card. Ok, now that's a great idea. So far, we have maybe a dozen local retailers on-board. Our goal is to get ALL of the conventions and the convention vendors to offer discounts to our members. I know it's a tall order, but we have a habit of setting very high goals, most of which I'd like to add that we meet and/or surpass. Toot toot.

The first fear people have with an idea such as our membership program is the security and integrity of our customers information. With that in mind, let me be very clear on this topic. YOUR information is not in any way embedded into, attached or correlated to these cards. That means that nobody can "get" ANY of your personal information, including your name, address, phone, email, etc. Nothing. Nor will your buying habits be tracked in any way. Simply by possessing this card, you are entitled to all the benefits and extras which it's designed for.

How can you get yourself one of these fancy little cards? If you want one of these, that's the easy part. Simply purchase a subscription and we'll include one with your first issue. If you already have a subscription, expect your card to be enclosed along with this very issue. If you subscribe for multiple years or opt for our "lifetime" subscription, you will get a new membership card every year of your subscription, throughout the lifetime of this program. Our plan is to create a new design each year, possibly making this card a collectable item. Who knows.

Our fourth issue of Blacklisted 411 .NET was just released and the fifth issue just around the corner - probably by the time you get this issue in your hands. Our .NET online magazine is doing very well. In case you've been living in a cave for the last few months, the new .NET edition is available on our website for FREE. It's been receiving good reviews and everyone seems to appreciate it, so we might be onto something here.

One last mention is our plans for the conventions this year. We're expecting to host our own private catered receptions (parties) and if you're a subscriber, expect a personal invite in the form of a special "party pass" which will get your foot in the door with any special event we host.

This is just the beginning of what we have going on over here, guys. I wish I could tell you about everything else, but not only am I running out of room for my editorial, but we're still working on the ideas and I don't want to spill the beans just yet. All I can say is that you should keep your eyes open and in our direction. 2006 is going to be a kick ass year for all of us. HACK THE SYSTEM.

- Editor

Letters and comments from our readers…..

I have a Dell Latitude C400 notebook that's about 4 yrs. old and have always had hardware problems with the external CD drive.

For some time I've been having more system problems because I haven't been able to back-up my files due to the external CD drive's inability to copy data (all other functions are OK (reads data, photos, plays CDs, etc. with some intermittent difficulty uploading programs and reading disks)

After much trouble-shooting with Dell and my own research/ trouble-shooting, it appears there is a problem with Dell's initial operating software regarding writing data files. Some system corruption has occurred, particularly since I can't yet load MS service pack 2. I've been using Foxfire online browser instead of MS almost all the time.

I bought a Belkin USB flash drive (128MB) to use for file backup so I can delete and reload the necessary program (computer needs a lot of clean-up anyway), but need to find out if I have a zip drive (required for XP professional)

To make things worse, my girlfriend forgot to put the optimum online modem on standby for several hours. I tried to run the Norton Anti-virus (don't know if it helped) and then today got an error message from MS Internet Explorer, asking me to let them send an error report to fix a significant processing error (MS online crash analysis dcp20 MS internet explorer) which could potentially identify some info from open files/programs and other identifying info (condition of IE, OS version, hdwr in use, dig. Product ID, which could be used to ID my license and IN protocol address), but it would be done on a secure website to a limited access db & not for marketing)

I'm concerned cause they say any person ID info won't be used at present to determine my ID, but only used to fix problem & they'll tell me if more info available when I send report in conjunction with their privacy policy.

Technical info about the report:
ERROR SIGNATURE: AppName:iexplore.exe, AppVersion: 6.0.2800.1106, ModVer: 0.0.0.0, ModName: unknown, offset:0003868

FILES INCLUDED IN ERROR REPORT: C:\DOCUME~1 \SusanP\LOCALS~1\Temp\WER4.tmp.dir00\appcompat.txt

INFORMATION ABOUT YOUR PROCESS: A bunch of data regarding Modules 1 through 95 (won't let me copy the specific info)

I did copy their data collection policy on an MS Word file.

I didn't send the error report and they closed down. I'm really concerned about the current state of security of my computer, whether to let MS Internet Explorer fix the error. As far as I can tell, you people have been the most knowledgeable by far and willing to share your expertise to help "know-nothings" like me learn to protect myself and my hardware (I'd never have found out about you if I hadn't found one of your magazines in my floor's recycling bin and was blown away by it)

If I ruin my hard drive I won't have the $ to fix it or get any other computer and I really need one cause I'm disabled.

Any help would be so very much appreciated. Regards,

Eddie L

Wow, Eddie. That's a mouthful of information. If I were in your position, I would install a fresh copy of XP Pro on the laptop, then install SP2 and move forward., specifically looking for any flash upgrades for the laptop. Essentially, start from zero and rebuilt the OS. Windows has always been known to be an unreliable POS of an OS, especially when it's been running on the same machine for a few years. They call it "OS Rot" - which I always considered a humorous term. Anyhow, don't bother using the "report error" because it won't help your situation. My official answer is going to have to be: fresh start, clean installs and go from there.

WEP cracking usually takes hours. Lots of hours, depending on the amount of traffic on the access point. A few months ago, two FBI agents demonstrated how they were able to crack a WEP enabled access point within a couple of minutes. 3 minutes to be exact. This is unbelievable when compared to, say 3 days of work. Here is how they did it, and how you can do it. You may need to know your way with each and every of these tools to get this done. You can ask Google for that. Anyway, if you are familiar with them, just do as follows :

1. Run Kismet to find your target network. Get the SSID and the channel.
2. Run Airodump and start capturing data.
3. With Aireplay, start replaying a packet on the target network. (You can find a 'good packet' by looking at the BSSID MAC on Kismet and comparing it to the captured packet's BSSID MAC).
4. Watch as Airodump goes crazy with new IVs. Thanks to Aireplay.
5. Stop Airodump when you have about 1,000 IVs.
6. Run Aircrack on the captured file.
7. You should see the WEP key in front of you now.

The software runs on Linux . I do not know any Windows alternatives. And finally, I think you should always use a combination of 2 or more security features. As for what you need, get Aircrack (Includes Airodump, Aireplay, Aircrack and optional Airdecap for decrypting WEP/WPA capture files) and get Kismet.

Another thing I might add is, always use a firewall when mingling with unfamiliar networks and use SSL to connect to the internet.

Dewayne S.

Thanks for the input Dewayne.

First of all I just wanted to tell you how much I have enjoyed your mag... OK My wife & I Currently reside in a condo just outside NYC and we have a Remote Meter owned & operated by QUAD LOGIC Our remote meter has been showing us the same digital reading for 3 years and they claim we are wrong and on their end everything is fine. And Our Electric Bills Are Thru The Roof! When many of our neighbors monthly bills are only $40- $90 a month! Our average is around $250 -$300. And Dig This, we left for 3 months and I shut off the main (curiosity) Guess what? our highest bill to date- $400 -$500 a month. How is that possible? Well needless to say we refused to pay until we were threatened w/a shut-off. Tired of fight'n THE MAN but SOMTHING IS REAL WRONG and I suspect - especially after that 3 month bill- that suspect, no I know I am getting the shaft. I would really appreciate any knowledge you could give me on Quad Logic themselves and how I can find out and catch someone who might be tapping into our line. Middle Aged Newbe

Eddie L.

Hi Eddie. We don't have any experience with Quad Logic to date, but your situation isn't an isolated one. If your meter is reading one thing and the power company is charging you something else, you should be able to determine the difference by looking at your bill (it should show meter *readings and when they were taken). If your meter says, for instance 123456 but when you get the bill it says that the last meter reading was 243165, something is obviously wrong. Maybe they're looking at the wrong meter... maybe you are. Contest the bill and take it to the PUC (public utilities commission) in your state.*

On the other hand, if your meter reading and theirs conincide but you're still paying outrageously high bills you don't believe you are responsible for, someone could be tapping your power. We've seen it all. If this is infact the case, the most likely suspects are your closest neighbors. If in a condo or apartment building, it should be rather easy to determine who's sapping your power. Once you figure it out, call the cops on them and file a police report. The contact your PUC and power company and lodge a formal complaint with them and give them the police report number. It should be somewhat painless, though time consuming, to get your money back. Good luck!!

Hello, I am unsure as to who to contact about my comment on this ad. I was reading volume 7 issue 4, and I noticed a site with content for hackers with macs. I just visited the site today and the current site (www.undergroundmac.com) is just a 4 page info site on the history of apple, though on the page they give this message (If you are looking for previous Underground Mac content, please visit) and then a link to http://machacking.net. This may or may not be useful, but i just thought to point it out anyway. Thanks for your time

P.S . I really enjoyed reading this issue, I really liked the first part, explaining the history of blacklisted 411, from being distributed by disks to having an entirely separate zine online. Keep up the good work, I look forward to reading the next issue.

Aaron F.

Unfortunately, UndergroundMac was recently the recipient of an attack to their site. It left the site, all of it's contents and the desire for the sysadmin to repair it in disarray. It's our hope that they site will be restored to it's previous state sometime soon. If not, it would be a shame as it was the best macintosh focused hacking site I've ever seen. They had the most complete forum packed with tons of information. It was a two thumbs up in my book! Anyhow, we continue to run the ad for them until which time we determine that there's no hope left for them.

I'm glad to hear that you enjoyed our recent issue. The magazine we have today is the product of many people and many years of hard work. It's always nice to see someone taking the time to comment on it. Anyhow, stay tuned because our Winter edition will be on the shelves fairly soon. 2006 will be a great year for us and our readers because we're going to be implementing many new member programs and offer additional products to the community.

My son who began his hacking on a Commodore in the mid-eighties and is now a Goon at Defcon brought back a copy of your magazine for me because it has an article on Aminet. I admit I have had to go to reading glasses as I have gotten older and my always slightly far-sighted eyes have gotten less flexible for focusing on small close things but I can read the magazine easily if I wear a loupe magnifier that I usually need only for the close up soldering jobs.

My question is has anyone had articles in your magazine about hacking the latest Commodores the DTV of last year and the Hummer DTV of this year? I lurk on the cbm-hackers mailing list cbm-hackers@ling.gu.se and Homestead digest

Ray B.

Hello Ray. Thank you for contacting us. We appreciate the interest. With regard to your comment on the text size. This is a topic which has been under debate for some time now. In the latest (Fall 2005) edition, we actually attempt to alleviate this issue by bringing up the font size a notch. I'm not sure it will be enough for everyone, but we're trying to concede that most of our old school hackers are aging and their eyes are not as good as they once were. Myself, I still have my 20/20, even as an aged hacker, so I don't completely empathize with those who comment about the small text. However, I take heed and have tried to institute changes so everyone can enjoy our magazine a little more.

As for your question on the DTV and Hummer DTV, we've got a pile of these in our lab and they've been yanked apart, hacked, rehacked, put back together and turned into new devices. We'll be offering some articles on the subject sometime soon. To date, I don't believe anyone has submitted any material on the subject which is curious. Myself, I started the better part of my hacking career on the Commodore 64 and have a warm place in my heart for the little machine.

Anyhow, stay tuned for an upcoming article on the subject. I have a personal interest in this subject, so I'll push to get something churned out.

I'm writing to say thanks for posting my article/solution for the online edition #2 crypto. I'll be trying to crack this next one when I have some free time at work.

On that note, I purchased the fall issue of Blacklisted at our local Barnes and Noble in Victorville CA the same weekend I returned from Iraq. I bring it to work so I can help spread the word. I know of a couple people in my platoon who went out and purchased your magazine as well.

I made a few desktop backgrounds with the Blacklisted 411! title on it, and keep it on my computer as a way to promote the discussion about hackers. I'll upload them and send you the address if your interested. Thanks again!

Brian D.

Thanks for the support Brian. Send over the link and we'll share it with our readers.

Hey Guys -- Was reading the letters and comments in Vol 7 #4, and saw the questions and your responses about using the Amiga and Commodore computers. I just wanted to send a note letting everyone know that there is still quite an active Amiga / Commodore scene, including a lot of hardware hacking. There are still a few active users' groups around, such as LUCKI, TPUG, and the one I belong to, SWRAP. Each year, we hold multiple Expos in various locations (Toronto, Chicago, Las Vegas) to support our Commodore 8 bits and Amiga computers, share the latest news, tips, products, etc. In fact, the Las Vegas Expo last year was the same weekend as DefCon, and will most likely be the same weekend again this year. Many of the members of these groups (including me) got their starts hacking with these machines, and continue to be interested in older hardware and hacking in general.

Some websites of note: http://www.dtvhacking.info, http://www.quantum-link.org, http://www.luckyclub.net, http://www.tpug.ca, http://videocam.net.au/fcug/, and of course, my group: http://www.swrap.org.

I'd love to help contribute Commodore/Amiga articles in the future, if you need more people to cover it.

TW

Hey TW, thanks for the heads up. The Commodore 64 was possibly the best computer ever made. But, then again, looks who's talking... me... Mr.-Started-a-hacker-magazine-with-a-Commodore64... So, needless to say, I'm won over.

OpenWRT

By Ustler

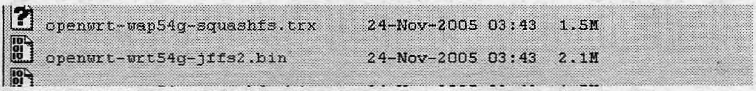
Introduction: In this article, we are going to look at OpenWRT, a small and expandable Linux replacement to the Linksys WRT54G/S firmware. Unlike other variations from Sveasoft and DD-WRT, OpenWRT has very limited built in features but gives us the ability to completely customize the firmware to our specifications. The obvious advantage is the increased space provided by not including unnecessary packages. For example, DD-WRT offers everything from Xbox Kiad to a web interface. Although these features are welcome by most users, their implementations drastically reduce the space available for any customized packages. Furthermore, since the root file system is not writable, customization becomes very hard for a standard user. In order to remedy this, OpenWRT comes in two flavors, full JFFS2 file system and a SquashFS file system with an accompanying JFFS2 filesystem.

Choosing the proper firmware:

As we mentioned before, there are two types of firmware, JFFS2 and SquashFS. To the normal user, the advantages are probably not readily apparent, so we will cover the differences briefly. Unlike JFFS2, SquashFS is a read only file system. In other words, you are unable to change a lot of the configuration files without removing the symlink and copying the file to the JFFS2 partition first. During the boot process of the SquashFS firmware, the system checks to see whether or not the JFFS2 partition exists. If it does exist, the firmware will boot from it rather than the SquashFS file system. The advantage over a full JFFS2 partition is for recovery purposes. If the JFFS2 partition is accidentally wiped, or a configuration file is messed up and prevents openwrt from booting, the user can reset to the SquashFS filesystem. The disadvantage is that valuable space is wasted since you actually have two copies of every file you need modified. Depending on your knowledge of Linux, I would suggest you choose the firmware that you are most comfortable with. For this article, I will be using the JFFS2 firmware simply because I am confident that even if I break my root partition, I will still be able to fix the device using other means.

Downloading the firmware:

Obviously, the first step is to download the firmware. To do this, we first go to openwrt.org and click on the download link under navigations on the right hand side. Next we choose whiterussian (The name of the current firmware release). In order to get the newest version, select newest, then default and select the correct firmware for your device. Notice that the format is <Name>-<Device>-<Filesystem Type>.bin. So if you have a WRT54G and want to use the SquashFS firmware, you would use *openwrt-wrt54g-squashfs.bin.* After selecting and downloading the correct firmware its time to move on to the installation.

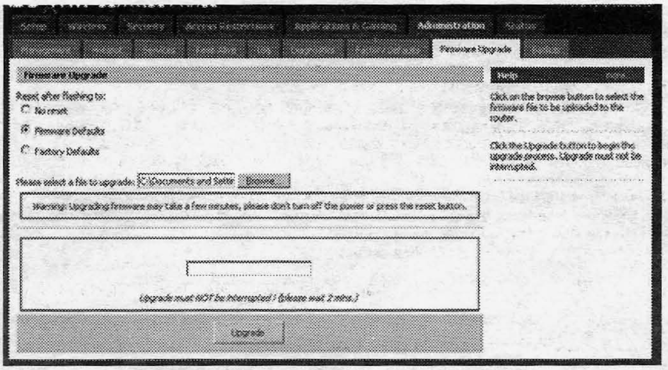


```
openwrt-wap54g-squashfs.trx      24-Nov-2005 03:43   1.5M
openwrt-wrt54g-jffs2.bin         24-Nov-2005 03:43   2.1M
```

We suggest you use default, but a few distributions exist. These are micro, pptp, and default. Micro contains no unnecessary packages, pptp contains packages required for having the OpenWRT act as a PPTP client, and default contains a few extra packages such as the web interface, dropbear and others.

Installing the firmware:

The installation is pretty straight forward. Once you obtain the firmware, you use the web interface to install it. In the following example we will be installing OpenWRT on a WRT54G containing DD-WRT.



Firmware Upgrade

Reset after flashing to:
○ No reset
● Firmware Defaults
○ Factory Defaults

Please select a file to upgrade: C:\Documents and Settir

Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

Upgrade must NOT be interrupted ! (please wait 2 mins.)

Click on the browse button to select the firmware file to be uploaded to the router.

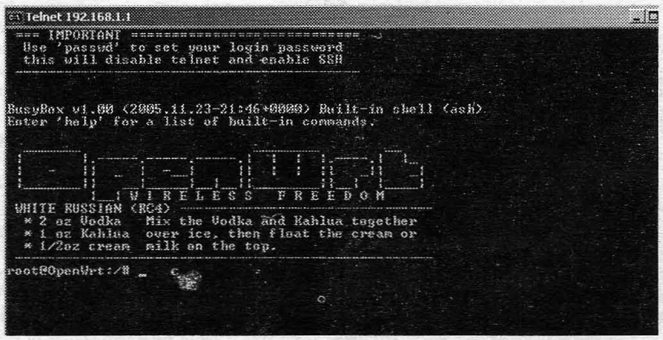
Click the Upgrade button to begin the upgrade process. Upgrade must not be interrupted.

After clicking upgrade, wait till it has finished. The router should reboot and your network settings will be reset to 192.168.1.0.

Logging onto OpenWRT is rather simple. In order to login, use telnet. In this case we use

telnet 192.168.1.1

This gives us root access to the device.



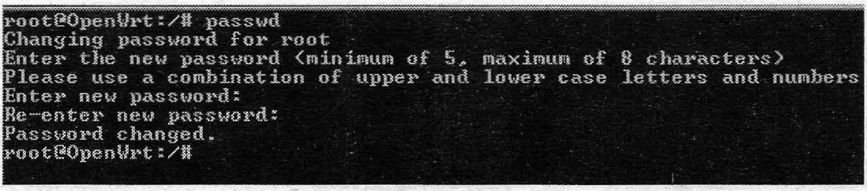
```
=== IMPORTANT ============================
 Use 'passwd' to set your login password
 this will disable telnet and enable SSH
------------------------------------------


BusyBox v1.00 (2005.11.23-21:46+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 WHITE RUSSIAN (RC4) -------------------------------
  * 2 oz Vodka   Mix the Vodka and Kahlua together
  * 1 oz Kahlua  over ice, then float the cream or
  * 1/2oz cream  milk on the top.
 ---------------------------------------------------
root@OpenWrt:/# _
```

We highly suggest you erase nvram in order to remove any unnecessary variables. After erasing nvram and rebooting, OpenWRT will initialize the variables with predefined settings. This ensures that you don't have unnecessary variables that may have been left over from the previous firmware. In order to do this, use the following command

mtd nvram erase && reboot

Changing the root password:

You probably already noticed that there is no root password present. In order to secure the router, we need to specify a root password to prevent tampering. To do this, we use passwd. For example, if we want to change the root password to blacklisted, we would do:



```
root@OpenWrt:/# passwd
Changing password for root
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers
Enter new password:
Re-enter new password:
Password changed.
root@OpenWrt:/#
```

Installing software

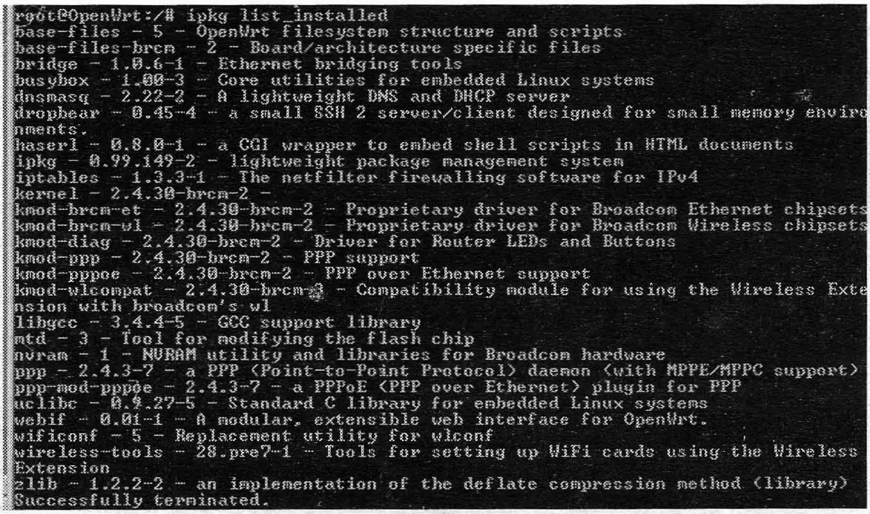
One important feature of OpenWRT is its ability to install additional software. To do this, we use IPKG, a lightweight package management utility. In order to retrieve an updated list of available packages, we use the following command:

ipkg update

This downloads a list of available packages from downloads.openwrt.org. Luckily, for us, we have descriptions of each package available for download. Another useful trick is to use "ipkg list_installed" to show the installed packages.

In order to view the available packages, we need to use "ipkg list". The list is rather long, so in order to make it easier to read, we need to pipe the command to more. To do this we use "ipkg list | more". Notice that the list will pause when data has filled the terminal. To continue viewing the packages, simply press any button.

If you look carefully, you will see a variety of tools including tcpdump, dsniff and others.

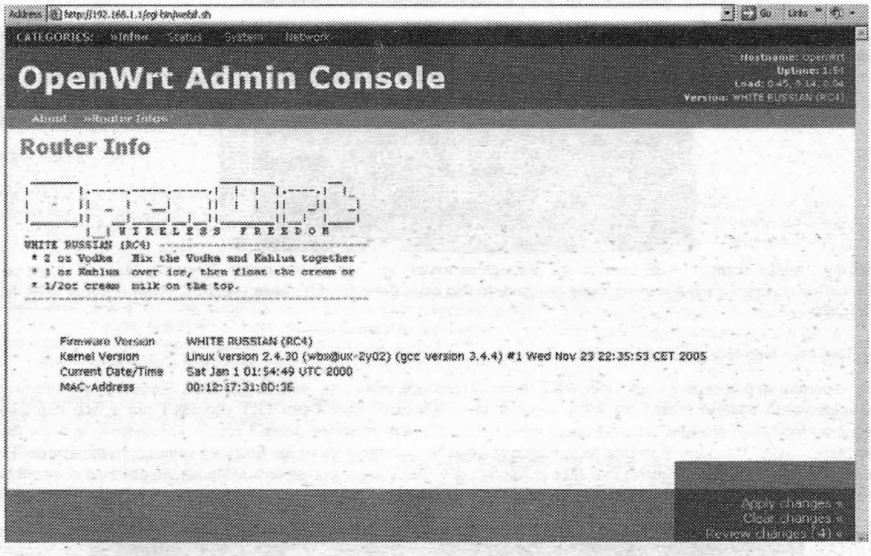


```
root@OpenWrt:/# ipkg list_installed
base-files - 5 - OpenWrt filesystem structure and scripts
base-files-brcm - 2 - Board/architecture specific files
bridge - 1.0.6-1 - Ethernet bridging tools
busybox - 1.00-3 - Core utilities for embedded Linux systems
dnsmasq - 2.22-2 - A lightweight DNS and DHCP server
dropbear - 0.45-4 - a small SSH 2 server/client designed for small memory enviro
nments.
haserl - 0.8.0-1 - a CGI wrapper to embed shell scripts in HTML documents
ipkg - 0.99.149-2 - lightweight package management system
iptables - 1.3.3-1 - The netfilter firewalling software for IPv4
kernel - 2.4.30-brcm-2 -
kmod-brcm-et - 2.4.30-brcm-2 - Proprietary driver for Broadcom Ethernet chipsets
kmod-brcm-wl - 2.4.30-brcm-2 - Proprietary driver for Broadcom Wireless chipsets
kmod-diag - 2.4.30-brcm-2 - Driver for Router LEDs and Buttons
kmod-ppp - 2.4.30-brcm-2 - PPP support
kmod-pppoe - 2.4.30-brcm-2 - PPP over Ethernet support
kmod-wlcompat - 2.4.30-brcm-2 - Compatibility module for using the Wireless Exte
nsion with broadcom's wl
libgcc - 3.4.4-5 - GCC support library
mtd - 3 - Tool for modifying the flash chip
nvram - 1 - NVRAM utility and libraries for Broadcom hardware
ppp - 2.4.3-7 - a PPP (Point-to-Point Protocol) daemon (with MPPE/MPPC support)
ppp-mod-pppoe - 2.4.3-7 - a PPPoE (PPP over Ethernet) plugin for PPP
uclibc - 0.9.27-5 - Standard C library for embedded Linux systems
webif - 0.01-1 - A modular, extensible web interface for OpenWrt.
wificonf - 5 - Replacement utility for wlconf
wireless-tools - 28.pre7-1 - Tools for setting up WiFi cards using the Wireless
Extension
zlib - 1.2.2-2 - an implementation of the deflate compression method (library)
Successfully terminated.
```

The web interface:

If you selected the default firmware for OpenWRT, you have the ability to use a web interface. This interface gives you a graphical control over network settings, wireless settings, package installation, and the ability to upgrade firmware. To show you how to properly apply changes, we are going to disable wireless functionality in the following example.

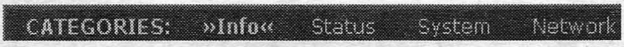
First open up a browser and type in http://192.168.1.1. You should then see a summary page similar to this:
To navigate, look towards the top and notice the categories. Choose Network.


Address http://192.168.1.1/cgi-bin/webif.sh
CATEGORIES: »Info« Status System Network
OpenWrt Admin Console
About »Router Info«
Router Info

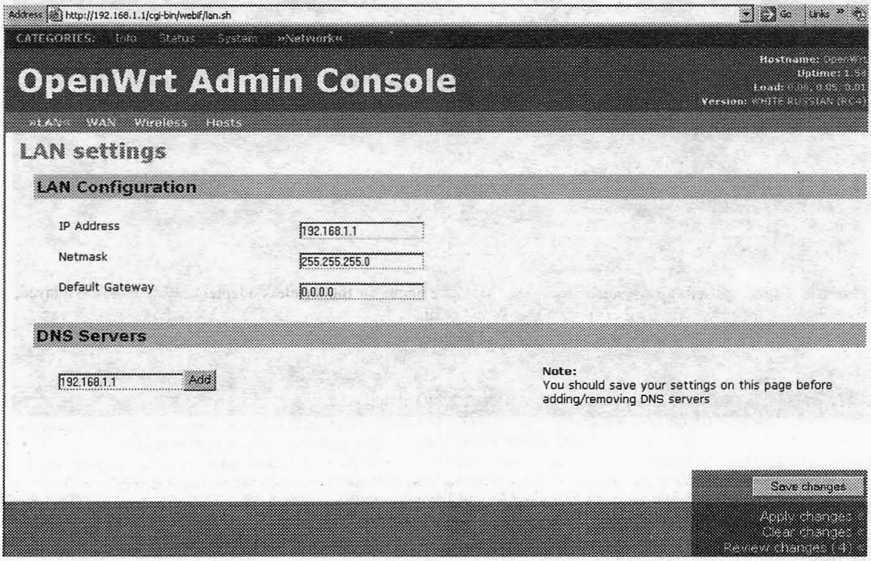
```
      W I R E L E S S   F R E E D O M
WHITE RUSSIAN (RC4) ---------------------------
 * 2 oz Vodka   Mix the Vodka and Kahlua together
 * 1 oz Kahlua  over ice, then float the cream or
 * 1/2oz cream  milk on the top.
-----------------------------------------------
```

Firmware Version   WHITE RUSSIAN (RC4)
Kernel Version   Linux version 2.4.30 (wbx@ux-2y02) (gcc version 3.4.4) #1 Wed Nov 23 22:35:53 CET 2005
Current Date/Time   Sat Jan 1 01:54:49 UTC 2000
MAC-Address   00:12:17:31:0D:3E

To navigate, look towards the top and notice the categories. Choose Network.



You will then be prompted for a username and password (Assuming you changed your password using passwd before). The username will be root and the password, in this case, will be blacklisted. After typing in the correct username and password, we are presented with this:



Hostname: OpenWrt
Uptime: 1:5
Load: 0.00, 0.05, 0.01
Version: WHITE RUSSIAN (RC4)

LAN settings

LAN Configuration

IP Address: 192.168.1.1
Netmask: 255.255.255.0
Default Gateway: 0.0.0.0

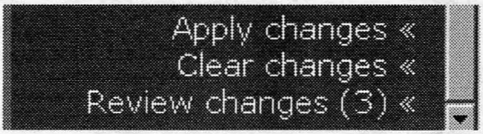
DNS Servers

192.168.1.1

Note:
You should save your settings on this page before adding/removing DNS servers

Notice the sub menu under the title.

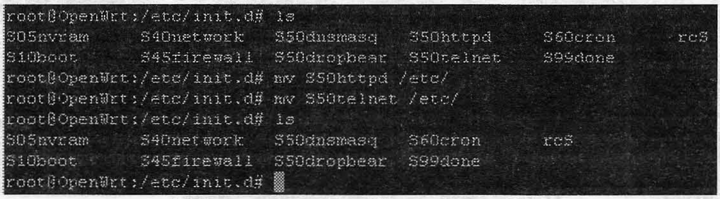
Clicking on wireless gives us a configuration page. In order to disable the wireless adapter, we need to choose disable under the Power settings. After we have selected this, scroll down to the bottom and select "Save Changes". Of course, one would assume that the changes made have already been applied, but this is not the case with webif. To apply the changes, you need to look near the bottom right hand corner for this



Clicking "Apply changes" will commit the settings to nvram and reboot the router. "Review changes" gives us information on exactly what is going to be changed. In this case, the main difference is that wl_radio is going to be set to 0 (Off).

Disabling the web interface and telnet:

One important step in securing our OpenWRT router is disabling telnet and the web interface. Since the web interface and telnet don't encrypt traffic, we must consider them insecure. Also, OpenWRT shouldn't run a web interface unless configuration changes are necessary. We see that the web interface doesn't require a password to view the information page. This page may leak information to unauthorized users about the firmware running on the device. To do this, we simply need to remove two files in /etc/init.d/ . These are S50httpd and S50telnet. In order to ensure that we can use these later, move them out of the init.d folder into /etc/.



```
root@OpenWrt:/etc/init.d# ls
S05nvram     S40network   S50dnsmasq   S50httpd     S60cron      rcS
S10boot      S45firewall  S50dropbear  S50telnet    S99done
root@OpenWrt:/etc/init.d# mv S50httpd /etc/
root@OpenWrt:/etc/init.d# mv S50telnet /etc/
root@OpenWrt:/etc/init.d# ls
S05nvram     S40network   S50dnsmasq   S60cron      rcS
S10boot      S45firewall  S50dropbear  S99done
root@OpenWrt:/etc/init.d# 
```

After moving the files, reboot and telnet and httpd will be disabled. Before doing this, ensure that you have dropbear installed or another means of remote access.

Nvram basics:

Non-volatile ram is used for storing settings such as the SSID, channel, vlan membership and others. Nvram can be modified via the command line using the command nvram. In this article, we are going to demonstrate a few practical examples on how to modify nvram values. Just in case you didn't notice the suggestion above, we suggest you wipe nvram and force OpenWRT to re-initialize if you had previous firmware running on the device. Nothing is worse than trying to sort through nvram keys that have no purpose.

Example - Wireless settings
In this example we will change the SSID, channel, and wireless encryption settings. Our first objective is to modify the SSID of the router. In order to do this, first run

```
nvram show | grep wl0
```

This will display all settings associated with the wl0 (The name for the wireless adapter). After this is displayed, you should notice the value wl0_ssid is set to "OpenWRT". This is the value we want to change. To do this we use

```
nvram set wl0_ssid= OurName
```

After we set this, we must commit the changes to nvram by running

```
nvram commit
```

This will save our changes to nvram and once we reboot, they will be applied. Just a quick note, the name of the value is case sensitive, so Wl0_ssid will not be the same as wl0_ssid. If you make a mistake when using the set command, this value will still be present but won't do anything. In order to remove it, we must use (The name of the variable can be substituted for anything you need to remove)

```
nvram unset Wl0_ssid
```

You may have noticed, no apparent settings are present for changing the channel. This is because a default value is assumed when no value is present. In this case, the default value is 0 (Meaning auto select channel). To set the channel variable, we first need to know what it is. In order to do this, a complete list is available in the OpenWRT Wiki (http://wiki.openwrt.org/OpenWrtDocs/Configuration). Viewing section three of the configuration page gives us the layout for the wireless nvram settings that can be applied. Since we are wanting to change the channel, we see that wl0_channel is the value we want to change. To do this, we use

```
nvram set wl0_channel= 6 && nvram commit && reboot
```

Notice, we are actually using three commands. One to set the variable wl0_channel=6, the other to commit changes to nvram (Or write) and the last one is used to reboot.

Firewall settings

In the following section, we will be looking at configuring iptable settings. This section covers the basics of understanding iptables. Topics such as port forwarding and advanced filtering are also covered. Iptables in openwrt allow you to control what is sent, received and forwarded. Since, as you may have noticed, OpenWRT doesn't have GUI support for firewall rules, most of our configurations will be done via the command line. After getting the basics of iptables down, modifying and creating your own custom rules should not be a problem. The first thing we are going to do is look at the current firewall rules. To do this, we use

```
iptables –L
```

which will list out our current settings. Adding –v will give us a more detailed look into the current settings (-v standing for verbose). At first glance, this may not make much sense, but in reality, it is rather simple. In iptables, we have specific chains for INPUT, OUTPUT and FORWARD. While many would assume that OUTPUT would be the traffic being sent from clients, this is not the case in this situation. OUTPUT in openwrt is the traffic sent from the actual device itself. The FORWARD chain is the one used by hosts on the LAN and Wireless interfaces. This is because the system is simply forwarding traffic out of the WAN port. Now you may be wondering, why are there three extra chains? These chains are called from one of the three main chains we referred to early. For example, forwarding_rule is listed as the target for the forth rule in the FORWARD chain. So as the packet moves down the chain, it will eventually process the rules in the forwarding_rule chain. Rules are processed in order, so ordering your rules will increase performance. In the following example we will examine the INPUT chain and its default rules.

Default INPUT chain rules:

```
Chain INPUT (policy DROP)
target     prot opt source       destination
DROP       all  --  anywhere     anywhere            state INVALID
ACCEPT     all  --  anywhere     anywhere            state RELATED,ESTABLISHED
DROP       tcp  --  anywhere     anywhere            tcp option=!2 flags:SYN/SYN
input_rule all  --  anywhere     anywhere
ACCEPT     all  --  anywhere     anywhere
ACCEPT     icmp --  anywhere     anywhere
ACCEPT     gre  --  anywhere     anywhere
REJECT     tcp  --  anywhere     anywhere            reject-with tcp-reset
REJECT     all  --  anywhere     anywhere            reject-with icmp-port-
unreachable
```

The first rules test the state of a connection and if its invalid, it will drop (Ignore) it. The second rule tells us to look at the state to see if its already been established, or is related to an already established connection. The next rule we will ignore. After that rule, we pass the traffic to input_rule. If it doesn't match any of the rules in the input_rule chain, it will return and continue down the chain. The next rule is somewhat confusing unless we add the –v option to the iptables –L command. If we run it with –v we get this result

```
target     prot opt in      out     source          destination
ACCEPT     all  --  !vlan1 any     anywhere        anywhere
```

This rule says to accept any traffic that is not coming from vlan1 (Our WAN interface). This will allow the clients to communicate with the router via SSH etc.

The next rule is somewhat of a security concern. It accepts all ICMP traffic, which can be used to identify that a network device is present. After that, we have a rule that accepts all gre traffic (Which is used for routing). The last two rules are also somewhat of a security concern since they respond to connection attempts with a tcp-reset or port-unreachable instead of simply ignoring it.

Making note of the rules we considered a security concern, the next task at hand is to fix them. To do this, we need to modify the startup script /etc/init.d/S45firewall. The first rule we need to remove is on line 39 and states

```
iptables -A INPUT -p icmp     -j ACCEPT       # allow ICMP
```

This rule can simply be removed since we don't care if our router responds to pings. Also note, we can still ping from the LAN side since the ACCEPT anything that is not on vlan1 applies.

The last two rules we talked about responded to request on unopened ports with a port-unreachable or tcp-reset. We can simply remove these since the default policy is to DROP all connections that don't match a rule. This default policy applies to all packets that have reached the end of the chain. We know that the default action is DROP because we can see it by using "iptables –L" at the end of the chain name "(policy DROP)".

```
iptables -t nat -A prerouting_rule -i $WAN -p tcp --dport 22 -j DNAT --to 192.168.1.2
iptables        -A forwarding_rule -i $WAN -p tcp --dport 22 -d 192.168.1.2 -j ACCEPT
```

This was copied from firewall.user in /etc/ . Firewall.user is executed after the initial S45firewall script is near the end. It is here that we can add our forwarding rules. First we add a rule to the prerouting_rule chain that takes traffic from the LAN interface (-i $WAN) that is tcp (-p tcp) with a destination port of 22 (--dport 22) and forwards it to the DNAT chain with the instruction to rewrite the destination address to 192.168.1.2 (--to 192.168.1.2).

The next rule tells the firewall to accept any packets that are from the WAN interface, tcp, port 22 and destined to 192.168.1.2. Since we already changed the destination address, this rule will match and the port will be forwarded to 192.168.1.2.

Advanced filtering

The last topic I will cover is advanced filtering. This filtering is what we call pattern filtering and applies to the actual data being sent. To be specific, this is layer 7 filtering. The disadvantage to this is the time that it takes to process the rules will slow down network performance slightly. Generally speaking, the performance slow down should barely be noticeable. I personally been running multiple filtering rules using layer7 (the module that we will use to filter) for a good month or two and have noticed no bandwidth reductions (Network consists of 12 computers 4 active clients average and a maximum of 12 consecutive active clients.) The filtering module and rules first need to be installed and can be done using ipkg. To install the package, we use

```
ipkg install iptables-mod-filter
```

After this has finished installing we should have a new folder in /etc called l7-protocols. This is where the definitions for matching data in packets is contained. A quick glimpse shows us a variety of protocols. Most notably are the P2P and instant messaging ones. In order to implement these, we need to add a rule to the FORWARD chain. But before we can do this, we must force the layer7 module to load. To do this use

```
insmod ipt_layer7
```

Next we will add our custom rule which will block AIM from being used on our network. To make the rule easier to understand, we will first show the command we will use to insert the rule, then explain what each part does. The command is

```
iptables –I FORWARD –m layer7 --l7proto aim –j DROP
```

Now you may wonder why the FORWARD chain instead of the forwarding_rule chain?? Well, if you may have noticed, the rule doesn't work after the initial sign in attempt. This is because "Established, Related" now applies and bypasses the rule in the forwarding_rule chain. Actually, I would probably end up creating a separate chain for l7 filters and have it listed at the top if implementing multiple rules. A quick rundown of the rule is rather simple

Command
iptables –I FORWARD –m layer7 --l7proto aim –j drop

Interpretation
iptables insert into FORWARD using module "layer7" matching layer7 protocol "aim" send to drop.

Conclusion

Of course this is not everything you can do with OpenWRT, this is only an introduction. I could ramble on about OpenWRT for hours, but due to time restraints and other projects im working on, this article will have to be limited to basic ideas. Since I tend to write in a manner that can be interpretated by any skill level, explaining advance techniques often becomes extremely lengthy and time consuming. If there is a demand for more information or if you want a specific topic covered, let me know and I would be more than willing to cover it in the next printed edition.

SECURITY:
A STATE OF MIND + LESS + NESS

Security: A State of Mind + Less + Ness

By Israel Torres <israel@israeltorres.org>

This article is not for the faint of heart and the situations explained herein are real. Names have not been changed to protect the innocent. Facts have not been obscured in any way.

When it comes to security there isn't a second of the day where I am not thinking about how to make things better. Some may perceive *better* as in being "more secure", but I will leave that to your imagination. Humans make great subjects when it comes to studying the state of things as they are now. Therefore I study humans in their natural habitat to see how they are adapting to a world of evolving humans versus humans that could care less. This particular example is one that is known to be pretty common as the "in-between" of these extremes – the overall average.

I went to a local shopping center to observe people and to eat lunch. All seemed well until something caught my eye. A few feet away a semi-attractive woman and her companion shouted out a brisk curse almost in symphony. She stood with her hands on her hips staring through her driver side window while her companion had her hands cupped looking through the passenger side window. *Ah, yes that familiar feeling eh*? She the driver left her keys inserted in ignition mounted on her steering wheel. Her vehicle obviously wasn't the kind that does not lock the passenger door if the keys are left inside by mistake. *Hint: Time to upgrade.* So there they stood for about 5 minutes staring at something so close yet so far. They had set their shopping bags full of post-holiday merchandise near the rear of the vehicle as a small breeze swam by. The woman dug through her purse and pulled out a small shiny container, opened it and pulled out a long slender cigarette. Her companion came over and took one for herself. Together they lit up and took long deep drags as they pondered what exactly their next step would be.

I wondered to myself if I should walk over and assist them. I was long done with my lunch but figured I just sit tight and watch the show. After they were done with their smokes they starting to hurriedly try each door handle. *Yeah these girls were real sharp.* So now they started to look around in the distance maybe there was a locksmith nearby or a hero. Not finding anything more than a few feet away the driver asked her companion to call someone since she left her cell in the car, her companion opened her purse and asked for the number – without discretion she practically shouted the number for being only a few feet away. At first I figured she was going to The Automobile Club (AAA) to have someone come and jimmy the lock for her. But instead she called dad. As she listened her eyes got wide and she smiled. She shouted to her companion that there was an extra key hidden under the wheel well. They both smiled at each other like they were now once again pimps of the day. While still on the cellphone she walked over slightly bent over (pink thong) and started to reach her hand inside coming out with nothing. She didn't seem to have knowledge of where exactly the key was hidden. Her companion went over and started to do the same on the other wheel wells (white w/purple thong). Now they started to look like two monkeys looking for ants in a rock. Apparently they were panicking and their voices were getting louder. I could have sworn I heard the male voice on her cellphone say "IT IS THERE – KEEP LOOKING!"

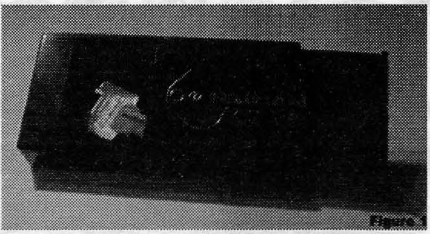


Figure 1

"Here it is!" the driver finally said. She thanked her dad on the cellphone flapped it shut and pumped her elbow to depict success. She unfolded her hand and there was a small black box with an outline of a key etched on it (*see figure 1*). Ah yes the old "Hide-A-Key" trick. She slid open the lid and there it was. She and her companion ran over to the driver side door and inserted the key and the door clicked open. They were both smiling more than before. They gave each other a hug. The driver reached and took out her keys to make sure she wouldn't lock them again. She remembered the extra key in her hand and put it back into the little black box then put it back under the wheel well where she found it. She popped the trunk and together they put their goods away. They looked around and lit up another set of cigarettes while they laughed at each other over this panicked incident. After giving each other a high five they took their purses and walked back into the shopping center to spend more money.

In there moment of happiness I had jotted their license plate, plate frame, color, make, and model of vehicle, and even where the box was hidden. I also wrote down the phone number she shouted earlier. I quickly looked around the parking lot and even though it was a high traffic area there weren't any visible surveillance that you would expect or normally see in little orbs or white and beige cameras. There wasn't a high rise building where someone could be sitting with a pair of binoculars nearby. Nothing obvious for now… (I always like to check just because) I have a t-mobile account so I decided to see what I could do with this information. What do you know there was a Starbucks about a block away from my position. I powered up the built in card, logged into my account and brought up google. I used to have a reverse number lookup database on my laptop, but I had just finished playing with the latest WMF 0-day last night and had to format the system after cursing google desktop – so I was still in a state of rebuilding my windows laptop and had not a chance to load all my favorite tools.. That's ok that is why wireless is so handy (as long as you are using an authorized account of course). Google came up and I typed in the 10 digit phone number that was captured earlier. Immediately there were promising results. The number was local and appeared to match the name of a local party that fit the initial description of a male. I pulled up Microsoft Streets and Trips 2006 and typed in the address and came up with the precise visual location which was about 5 miles away from this shopping center taking streets and only 3 taking the freeway. Since I was still online I decided to cross reference this map with google maps (http://maps.google.com/) and they matched, I clicked on the satellite button to get an overview of what this residence looked like and the result was a standard suburban tract housing unit. I wanted to get a closer look to see if it was gated or guarded but google didn't offer a feature to get even closer so I brought up the old reliable globe explorer site: (http://www.globexplorer.com/) where I am able to zoom pretty close in. I pan around zoomed in the closest it will take me and see that this residence is completely unguarded and does not have a gated entry system. I stare closer at the exact area of the address and see a tiny vehicle parked in the driveway and lo and behold it matches the color of the vehicle parked in front of me. Yes we all know the dates of these maps could range into the years, but as I mentioned earlier this vehicle has been around the block so the image capture seemed believably accurate. There was no doubt in my mind that this woman still lived at home with her parents (at least her father).

This had all happened rather quickly so I decided to put his name into the callsign database for HAM radio operators (http://www.qrz.com/i/names.html) and query a name search just to see if he was by chance an operator. What do you know… he is an operator and belongs to a radio club. I cross referenced his known address and it matched. He also has a picture on a site with him standing by his daughter and his wife. I *didn't* know the daughter's (the woman driver) name but I sure do now. So I typed her name on google and to my ***unsurprise*** she has a myspace account. Looking through her profile I notice one of the accounts in the friend's space (and one that is commenting the most) is the companion she is with. I now know her name *too*. I also know where they are going to college and they live a few houses down from one another, I even know their favorite drinks and bars they hang out in. I download each photo – I love personal photos because you can really tell a lot about person from the objects behind them sometimes reflections and more information than they think they are showing. I quickly read their blogs and find out her friend has bad breath – at least she gets teased about it a lot. I also get to view a few not so safe for work pictures of her at a party someone posted (beer + vodka + inexperience = regret). One of her recent blog entries mentions she got an Xbox-360 premium package as a Christmas gift from her loving dad. He bought her all the games (no doubt so he could also use it) for the unit. *How sweet.*

In the latest blog entry the woman driver wrote mention that her family and her friend are going to go

shopping for a trip they are going to up north for New Year's and won't be back until the next weekend in case they don't hear from her (*she isn't sure her aunt has a computer that can get online*). She proves to be really informational.

In my research for this article I picked up one of these plastic magnetic cases that I have to thank for all this great information. The original models I recall were made of a thin metal – this particular model (Hillman #701327 / 9300-12) is larger and made of plastic (probably to hold the larger SUV keys out there). I frankly didn't know they were still around because they were so obvious. Take a look on the back of the package for instructions (*see figure 2*).

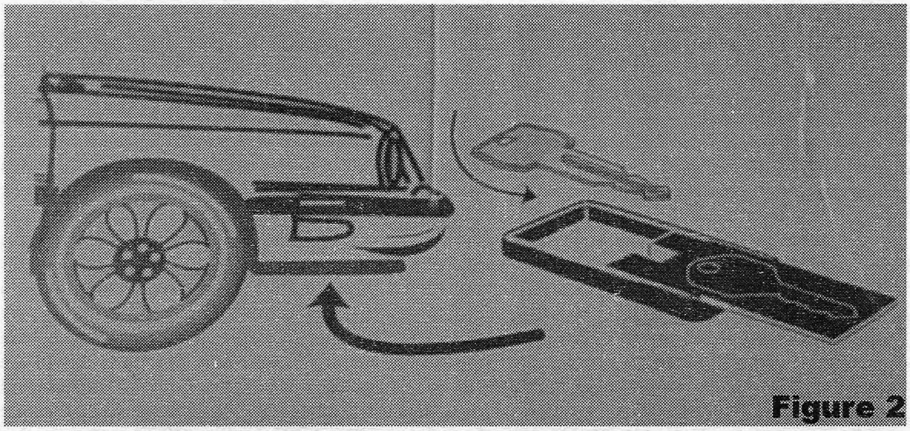


Figure 2

It looks like most people take this visual set of "instructions" a little too literally. I guess it is difficult to expect that people would think for themselves and figure out that if everyone kept their keys hidden in the pictured area that the key isn't **HIDDEN**. *Instead it is expected to be there.* Look at it this way, at least they weren't using a magnetic rock to *hide* they key in… and at least they are bothering to lock their doors unlike more than a significant percentage of people that don't even bother to do that – or even bother too look in their back seats before getting into their vehicle. To me it seems that people may want to be secure but in a way that allows convenience to be the majority ruler. I think they are just fooling themselves.

So far we've learned how **not** to use this Magnetic Key Case. Now I'm going to explain better uses for this device as a low tech solution.

If you are familiar with the historical version of the Cold War you may recall that there was a lot of spying and espionage going on (*don't think it isn't happening today*). There would be agents and double agents trying to contact their handlers to pass vital and often critical information to the other side without having their cover blown. Some agents didn't even know what their handlers looked like and vice-versa. (Often it was better than the less anyone knew the better in regards to a handler-agent relationship) Yet they regularly needed to give each other intelligence such as rolls of microfilm and further instructions. There wasn't anything like e-mail or FTP to get things from one point to another so they had to rely on physically going somewhere and leaving the information in hidden objects to be picked up later after they have left. There was a lot of paranoia and it was always best to assume you were being watched so you never wanted to be seen together or give away where the drop off point was. Thus drop points were articulated and visited round robin and the hidden objects were to vary such as from hollowed out bolts on a telephone pole to fake bricks in a fireplace. The objects had to be easily accessible so someone watching a suspect wouldn't figure out when or how they were dropping the information. They had to be hidden in plain sight. For example one agent would be taking a morning jog along one of their regular routes and would usually drink from a water fountain but observers took a long time to figure out the handle of the water fountain was hollowed out so that while the agent was taking a drink of water they would quickly slip "the package" into the handle and then replace the handle without being noticed. Since this drinking fountain was at a park a lot of people usually joggers came to visit it so keeping track of people coming and going was more than a task – especially with technology as it was (nothing like facial recognition software that we have today).

Taking from this idea I tried stuffing objects into Hillman's Plastic Magnetic Key case and found that quite a few useful items could fit in here (see figure 3).

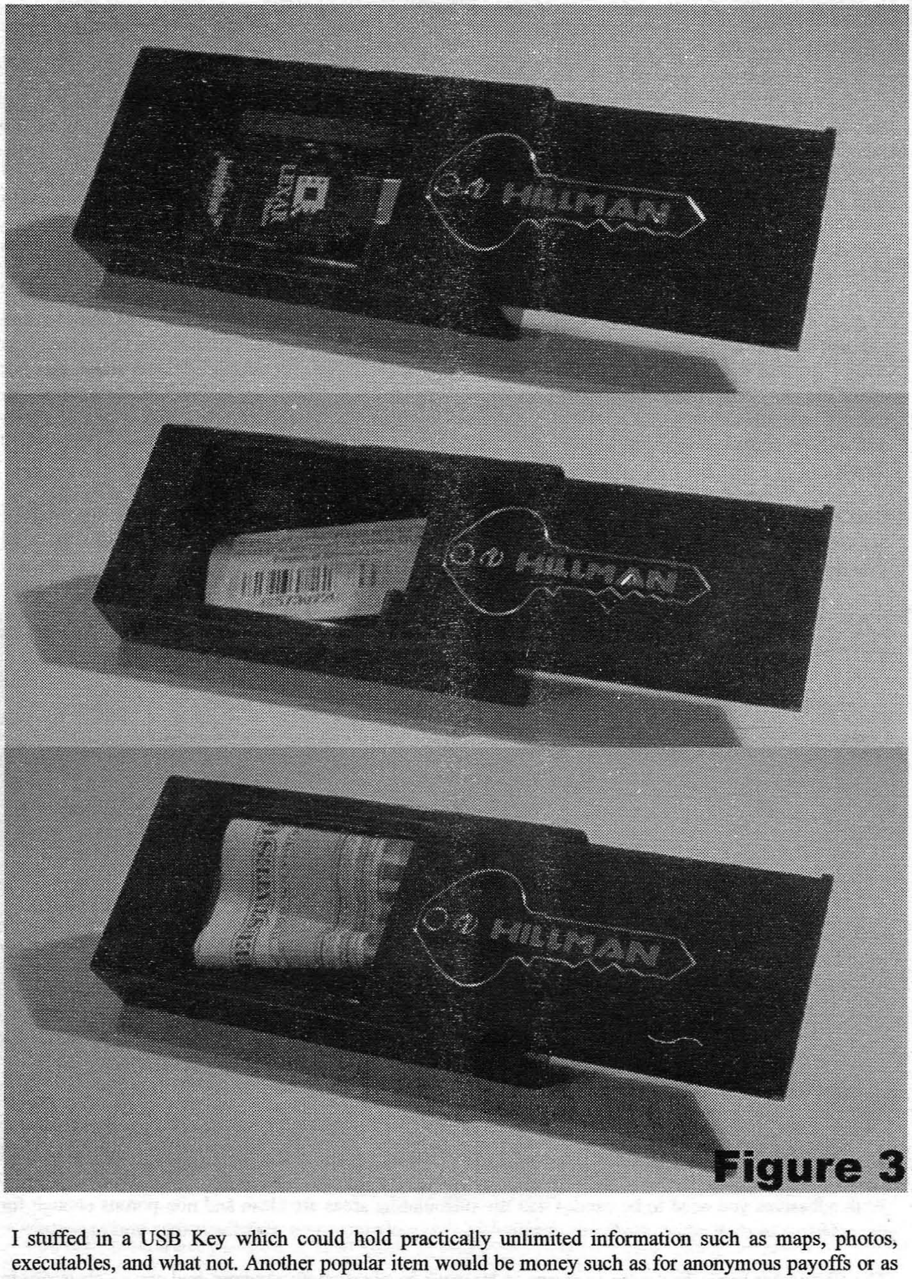


Figure 3

I stuffed in a USB Key which could hold practically unlimited information such as maps, photos, executables, and what not. Another popular item would be money such as for anonymous payoffs or as hidden money. That's right you don't have to exclusively use this to transfer information or data to other people you can use it for yourself in the future. It is always good to have backups in remote places away from your common domicile. This is one practical way how.

Do you remember in the movie ***hackers*** (I know… I already hear you groaning) where Phreak and Acid Burn were in this discussion? :

> *"Yeah! You better figure out what's on that disk, cause we're being framed.* ***It's in that place where I put that thing that time.***"

… and Acid Burn knew exactly where to go for the pick up, at the same time anyone monitoring the call did not? That's the type of forward thinking you want if the day ever comes where you are on the run. Other examples include storing a key to a locker somewhere else with your passport and bankroll. These magnetic plastic enclosures could then be placed practically anywhere – usually somewhere up high where things don't change too much and someone won't accidentally run into it. Also you want to account for the weather and whether the items being hidden will have trouble with things like rain – these cases aren't waterproof but you can put your items in latex (like in the finger or a latex or plastic glove and tying the end in a tight knot)

A great dynamic drop off scenario could involve sticking this device somewhere in a parking lot and you can call up the other party and tell them the license and color of car to look for and where it is stuck. You can then monitor them without letting them know you are watching. Now relax, I'm not advocating anything except being prepared when you have to be. If you are savvy with electronics you can also use this magnetic enclosure to install a radio monitoring (audio/video) device where one isn't normally expected. If you are savvy with pyrotechnics you can create a handy little diversionary device.

One great feature with this particular device is that it is plastic. If you want to make sure it isn't detected by any type of metal detectors or EMF detectors you can remove the two magnets on the back (*see figure 4*) and instead outfit it with something like Velcro or adhesive tape.

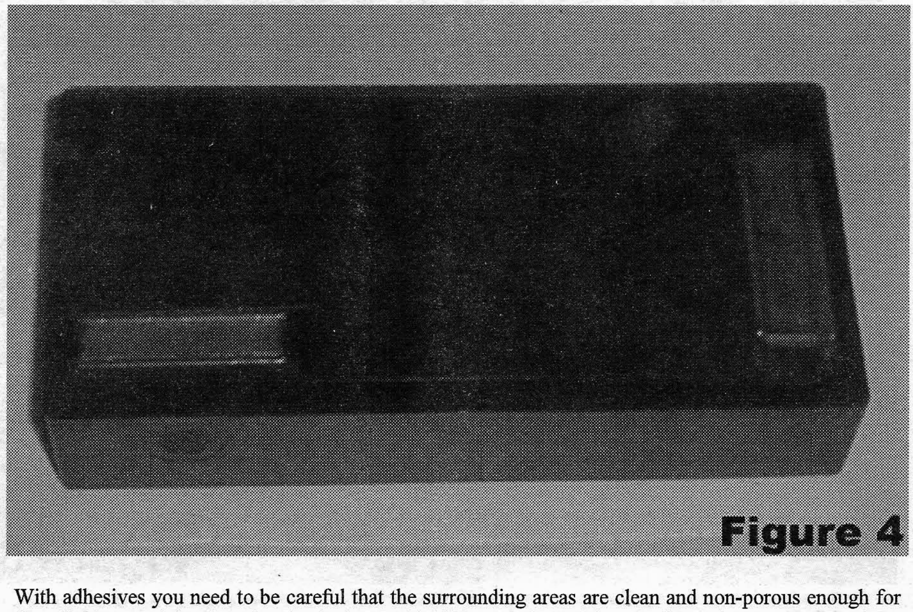


Figure 4

With adhesives you need to be careful that the surrounding areas are clean and non-porous enough for the adhesive to stick otherwise the device could fall into obvious sight a lot faster than you expected.

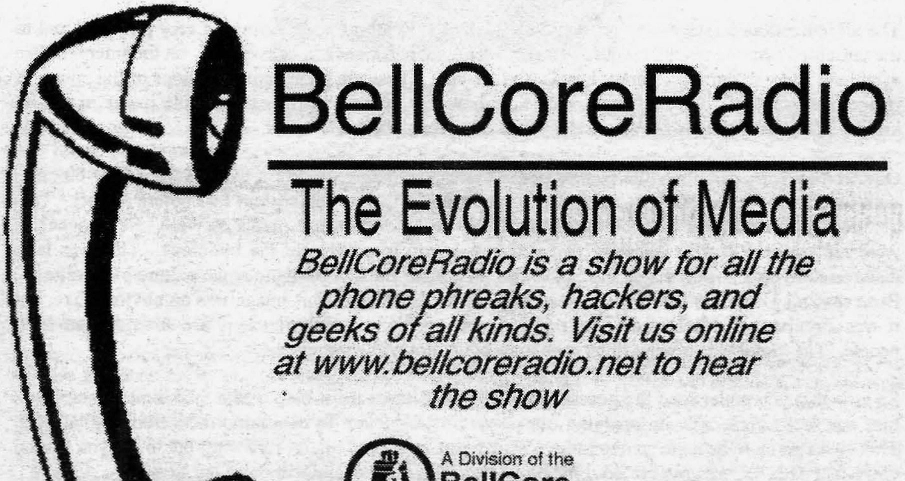
The Plastic Magnetic Key case is meant to be stuck in places with shadows and visual obscurity in places it would unlikely be like under a fender or in a wheel well. It is black and has a matte finish so that it doesn't shine and call attention to itself. You can take further steps to camouflage its appearance by adding bits of fabric to fuzz its outline better so that it becomes harder to detect visually.

In this article I've demonstrated different ways to take a device beyond its original design for usage that may have been unintended by the inventor. I've also discussed what not to do with this device – especially if you intend to keep things you value. Other similar devices come in different forms such as hollowed out objects that are usually supposed to be where they are found like rocks, shaving cream cans, cola cans, soup cans. These have more of an intention to hide objects of value so that in the case of a burglary or general search the item is more likely to go unnoticed than say a shoebox under the bed. Lastly, I've demonstrated how dangerous even the simplest information can be when falling upon unintended parties. **Be aware of your surroundings - if you aren't then someone else just may be.**

Keeping it 'rael,
Israel Torres

Links mentioned in this article

http://maps.google.com/
http://www.globexplorer.com/
http://www.qrz.com/
http://www.myspace.com/
http://en.wikipedia.org/wiki/Cold_War
http://sfy.ru/sfy.html?script=hackers
http://www.hillmangroup.com/acc.htm


BellCoreRadio
The Evolution of Media
BellCoreRadio is a show for all the phone phreaks, hackers, and geeks of all kinds. Visit us online at www.bellcoreradio.net to hear the show
A Division of the
BellCore
Omnimedia Group

The Art of Electronic Deduction

By: StankDawg@stankdawg.com

Deduction is the act of applying reason to arrive at some conclusion. It is a skill that is important to detectives or investigators, but it is a skill that can come in handy for everyone, including hackers.

Your powers of intuition and deduction should be something that you always have turned on. Think of it as the hacker's version of "Spidey-sense". As the type of people who question everything and believe nothing until we have confirmed it with our own eyes, analytical skills play a huge part in most hacker's personalities. When you see anything on the internet, or anywhere else for that matter, it should always be studied and questioned. In the age of journalists who make up fake news stories and fudge the facts, and in a world where any image can be easily altered (or even created from scratch) by software, why would we believe anything that we see anymore? The old adage of "seeing is believing" doesn't have the same meaning as it used to. This is why it is important to develop your skills of deduction.

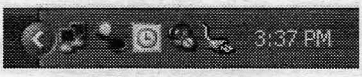
Electronic deduction is a very vague term since the word "electronic" can refer to a lot of things. This vagueness is intentional. Electronics can be as simple as understanding how technology works and questioning any claims made by salespeople or television commercials. Don't be led by employees of "Best Lie" or electronics superstores who will tell you anything to get your money. Question them. By understanding the technology of the subject matter, you can catch a salesperson in a lie very easily. You can recognize lies in commercials instantly. More to the point for this article, however, is electronic deduction on a computer.

The aforementioned image-altering software (such as Photoshop, or the gimp) is very powerful and to the untrained eye, the results can be very convincing. Contests are held every day on the internet. We even have them in our own Binary Revolution forums. These are great demonstrations of the power of image manipulation. Those people who know how this process works can take the image apart and know whether an image is fake, or real, by analyzing the data itself.

One well-known example is the picture of the tourist standing on top of a world trade center building with the 9/11/2001 (*never forget*) hijacked plane seen in the air behind him just before impact. This picture made rounds not only on the internet, but in the mainstream media as well. News agencies were reporting on it with the story that it was found in the rubble of the buildings. This was later discovered to be a hoax, created in Photoshop. One other notable example is the picture of George W. Bush reading a children's book in front of a Houston classroom. This image was an obvious fake, but it was circulated and believed to be real by most people. Luckily, hackers are smarter than most people. The moral is to always think with your brain, not with your eyes.

So now that you understand the general possibilities of how easy it is to create fake digital data, let us turn our focus more now on applying our powers of deduction to determine facts from digital data. This could go on to become an enormous lesson in metadata and digital forensics, but to get you started down that path, we are going to do some basic footprinting as an application of our deductive skills.

Take this first example below. It is obviously a screenshot that most readers will immediately recognize as Microsoft Windows XP. This is our first assumption. Right now, we can make that assumption, since there are no other public versions of MS operating systems that have the same look that Windows XP does. There are pre-release versions of Windows Vista out there, which could be mistaken as XP, but they are not that prevalent yet. If there are multiple possibilities, you may not make such a high percentage assumption as this example. You may see a Linux toolbar that does not give you any clue as to which distribution of Linux is being used. It is still worthy of note, because in further investigation you may find another piece of software that may combine with this fact to give you a better profile of what you are dealing with. This is the most important point of this article. You do not have to arrive at absolute facts. You only need enough information that combines to form an assumption that may or may not be an absolute fact. It may not be conclusive enough for a court of law, but it can certainly create a preponderance of evidence for real-world scenarios.



From this picture we can make a series of assumptions that may be questionable individually, but when combined together, help create a profile. This simple example can be done quickly by brainstorming while looking at the screen capture above.

We already know that it is the Windows XP operating System so let's look closer at the clües presented to us. The next thing that you may notice is the icon of an "electric" cord. This is not normally seen on desktop computers, so we can assume that this was taken on a laptop (that was plugged in at the time of the screen capture). It could also have been a desktop with a battery UPS, but this is much more rare since few people actually use a UPS. This is an example where the observation cannot be conclusive by itself, but let's see what else we can find to corroborate the profile.

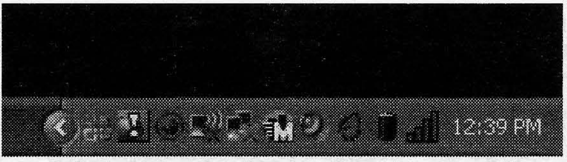
There is a speaker icon showing, but it has the circle with a slash though it which indicates that the person has muted their sound. When would someone do this? It isn't very often that someone would mute the sound in their own house. This may be the corroborating evidence that we need to back up our earlier laptop assumption. You have made your first deduction and filled in a piece of the puzzle on the profile of this user.

We also see other icons that may or may not be familiar to you. You may have to research some of them on the internet. In this example, we see the MS Outlook icon. This is very common and may not lead to anything conclusive, but we note it anyway. Another icon is for the chat application called Trillian which is a program that allows people to use multiple chat protocols (AIM, Yahoo IM, MSN, etc...) in one client. This icon holds a lot of information. Firstly, you can tell from the yellow at the top of the icon that the person is connected. Trillian will show "black" if it is not connected to any services. At the same time, the bottom part of the icon is black, meaning that while they are connected to a chat service, they are not connected to all available chat services. This chat connection is confirmed by the network icon on the far left. This will only show when the person is connected to a network.

So with this small bit of information, what kind of a user do we think this belongs to? We have a profile that shows them to be a laptop user, and someone who uses MS outlook for their mail client. Since the mail client is the only other software open besides the chat client, we realize that this user apparently has a need to be connected to information. We also can make a small assumption that the user has some experience and comfort with computer in general. Trillian is not an application that a basic user would know about. With the volume turned off, this is not likely to be a home computer, so two possibilities that jump to mind are that it is a laptop belonging to a student or a business person. It could be either, but personally, I would assume a student to have even more software installed and more icons showing.

For the record, this was a screenshot from my work laptop taken in an airport terminal where I was connected to the internet and doing some work for a client. This holds true with almost all of the assumptions that we made and it fits the profile that we came up with. With one small screenshot, a very accurate profile of the user was made. The time on this image is 3:37 PM, which doesn't have any significance in this example (other than confirm that it was taken during work hours), but it is an Easter egg that you can research on your own.

Let's try another example. Look at the taskbar screenshot below. I am intentionally using small screenshots of the taskbar for these examples because it best illustrates the power of deduction. You can apply these techniques to full screenshots, videos, or anything else that you can think of. If we saw the full screen, we could see wallpaper that may describe a personality, icons for installed software, filenames that may holds clues such as names or businesses. The possibilities are endless.



Let's take this example and put it through some actual steps that you can recreate on your own. We can create an organized, structured approach that we can use consistently until you get the hang of doing it in your head. Creating a structured approach makes the analysis much more thorough so let's break the process down into the following steps:

1) Determine the Operating System being used.
2) Determine hardware being used.
3) Enumerate the software being used.
4) Analyze status of hardware and software by analyzing each one individually.
5) Note other items such as system settings, time/dates, colors preferences, and other information.
6) Analysis/Conclusion.

First off, we can determine once again that this image is a screen capture from Microsoft Windows XP. Keep this is mind as a clue to other software. Some software packages are OS exclusive and if you see software from another OS in use, you may have a contradiction in logic that may force you to re-evaluate your assumptions.

How do we determine hardware? There are a couple of ways. Most hardware requires a piece of software called a driver to get the OS and the hardware to communicate. This piece of software usually shows up on the computer. In this screenshot we see signs of hardware. What does the existence of the battery icon represent? What does it indicate, if anything? What about the bars on the far right next to the clock? This indicates a wireless card is present and if you know the specific icon, you will know what type of wi-fi card it is. If you determine what type of card it is from the icon, you will reveal a clue that confirms the manufacturer of the laptop. The network icon with the red "X" on it indicates that the network connection is disabled. Why would someone intentionally do this?

Next we can enumerate the software. It is important to point out that education and, more importantly, experience plays a large part in this process. You may not recognize all of the icons in this image. The more experience you have with different software packages, the more evidence you can compile in your analysis, and the more accurate your findings will be. I will quickly point out the icon with the exclamation is an application that ships with Dell computers called "Dell Support Alert" which sends out alerts from Dell computers for those of you who may not be familiar with them. Knowing that piece of software helps confirm one of our hardware assumptions.

Other software includes MS Office (on the far left), MS Money (the icon with the letter "M"), and GetRight (a download tool). The download tool is an interesting inclusion since it is not something that your typical user might have. The specific icon for MS Office is also a special icon. Some research on it will give you more information about the status of that particular MS Office installation. And what type of user uses MS Money? That is not something you find in an office or from a business user, so what other type of person may use this software? Our profile is starting to become clearer as we continue the process.

Now that we have broken down most of what we see on the screen, is there anything else that we missed? What other clues are there which may be significant? It is difficult to tell in this cropped image, but we can see a small portion of the desktop wallpaper showing in the image (If you cannot see the image clearly in print, the original image will be available online via stankdawg.com). Some of you may recognize it as the default wallpaper on many Dell machines. That is noteworthy, since it further confirms our earlier conclusions about the manufacturer of the hardware. Also, the time of day on the clock may or may not be relevant, but it still should be noted in our analysis. The time of day is 12:39 PM. It doesn't carry much value in this case, but what if you saw 2:35 AM? What kind of user would be up at that time of day? What if the time was shown in military time? What kind of person would set their computer clock in military time?

So you have a pretty lengthy checklist of information now. Some of it is clear based on hardware and software while some of it is circumstantial and may not mean anything independently. The point is not to make individual conclusions, but to combine all of this information to form a strong profile. What conclusion, if any, can we arrive at based on what we have seen in this tiny image? I think we can safely assume the following:

- This user is probably somewhat of a power user based on the settings that we see applied and the types of applications being used.
- This user has software installed that is not typical of an office environment. This is most likely a home user or possibly a student.
- MS Money is very closely associated with home users, and not with students. This circumstantial evidence lends more towards our home user theory.
- The system is almost definitely a laptop.
- It is almost definitely a Dell brand laptop due to the Dell Alert software, the Dell wallpaper, and the dell wi-fi icon.

All of this adds up to a very accurate profile of the user of this screenshot. Once again, the user in this scenario is me but the system was a little but different. The system was a new desktop from Dell that still had preinstalled items on it, but was also in the process of being customized. I use it on the airplane and took the screen capture while flying so there are no networks present (which is why they are disabled). It came preinstalled from Dell and I have not bothered to uninstall the Dell Alerts software that you see, nor have I activated the MS Office installation (which is why the MS office icon is in the taskbar). I use Get Right because airport wi-fi connections are notoriously unreliable and I want interrupted downloads to pick up where they left off. Can you see that there is certainly enough information in that tiny screenshot to make a very precise profile of me as a user?

This is a great exercise that anyone can do. This article started off as a little game that I made up for my local BinRev meeting and it is a fun exercise that you can do at your local meetings or just privately to hone your skills. You may have never thought of looking so closely at something as common as a screenshot. Not only does a screenshot reveal a lot of information, but metadata in all electronic files can reveal enormous amounts of information. Think about that the next time you upload anything or see anything uploaded. As it turns out, a picture truly is worth a thousand words. The next time that you see a screenshot somewhere, make sure that you apply your skills of reason and practice the art of electronic deduction.

"The Revolution Will Be Digitized!"

Shoutz: The Digital DawgPound, BR561, Jawga, Acidus, Phizone, MC Frontalot, Zearle.

Listen!

Introduction to Scanner Monitoring and Short-wave Listening

By M L Shannon

Author's note: This article was originally published in Blacklisted! 411 about two years ago, as "The Ear". Since then it has been expanded to include new material about scanning, and short-wave listening. Rather than repeat all of the original article, I have shortened it to include the most important parts: How to learn to Listen!, to quickly identify the type of transmission, of service. Following that is the first half of a long list of services, stations of all kinds, that there are to monitor.

Part Two will have the rest of the list, and info on data transmissions, the trunked radio system, nearfield scanning and repeater input reception, and a little technical material on radio communications.

Disclaimer of Liability.
The Scanner Book is written for information purposes only. Neither the author, the publisher, or the seller assumes, or will assume, any responsibility for the misuse of the information contained herein, nor will the author, publisher, or seller, be responsible for the consequences thereof, either civil or criminal. If you have doubts or questions as to what is or is not unlawful, please consult an attorney.

Scanners and The Law
Federal and local laws prohibit monitoring some types of transmissions. This includes cellular and cordless telephones, commercial paging and federal agencies using encryption, though you can not unscramble their transmissions. The Communications Act of 1934 restricts us from repeating anything we hear except from transmissions intended for the general public; commercial broadcasting, amateur and CB, and emergency distress signals.

There are also state laws.
Apparently in Indiana, using a scanner while in a motor vehicle or while walking or bicycling is illegal. Other states have their own laws. Some do not apply to two way radios possessed by licensed ham operators, even if they can tune police frequencies. They also do not seem to apply to transceivers, even if they are capable of out-of-band reception; capable of scanning other than ham radio bands.

Decoders
It is possible that mere possession of devices that can decode transmissions, such as pagers, may be unlawful even though they have legitimate uses in amateur radio.
To learn more, check: http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1994/orcc4010.txt

INTRODUCTION
These two articles are about the many fascinating signals there are to monitor with scanners and short-wave receivers once you learn to Listen! Knowing what you hear, not just scanning. With the information here, and some practice, you will soon be able to quickly determine the type of service you are tuned to. Those of you who are new to this hobby will find these techniques useful and even experienced "scannists" may learn a few things.
Read on, and you will learn about them.

But be warned; the more you learn, the more you may find it difficult to tear yourself away from listening. You might tend to put off things until you can figure out that 'mystery' signal, maybe a 'spy station' that you stumbled across but haven't been able to identify. And you might be tempted to spend the rent money to buy more radios!

Frequency Allocations
Now, back when I got hooked on monitoring, there weren't many frequency guides, only a few regional lists were available, so you had to go to a field office and search through a microfilm ('fiche') reader which was a very time consuming process. Then Kneitel's Top Secret registry was published in about 1978 by CRB Research, and today, there are many frequency guides available. Books and CDs. Using them to look up a frequency that you are monitoring may solve the mystery of an unknown station, but then it might not. The actual FCC listings, which are available on CD, sometimes reveal very little information. A license may be issued to the ABC Corporation but this may not tell you exactly what it is; the radios may be used by taxicabs, a construction company or whatever else.

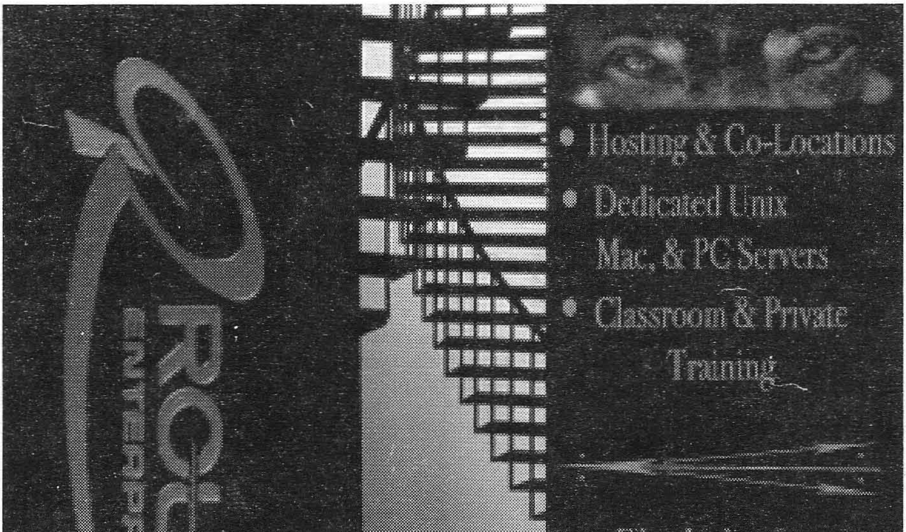
Federal agencies such as FBI, Secret Service, etc. are not licensed by the FCC so they are not included in FCC records. The Internet is the best source, with hundreds of sites packed with information and a few are listed in Part Three.

A good start is to become familiar with allocations, rather than specific frequencies. Bands that are used for specific purposes, such as business, military, federal agencies, police and fire departments. But what you might expect to hear in a particular area of the RF spectrum, and what you may actually intercept may not be the same. While the radio spectrum is divided into many bands, there is an overlapping of what agencies, businesses, individuals, might be using them at any given time.

An excellent aid is the frequency spectrum poster available from the US Government Printing Office. This is a 30" x 40" chart that graphically lists all allocations in the Radio Frequency spectrum. As you will see on the chart, sometimes the same bands are assigned to different services, shared by both government and non-government agencies, so you might hear the local police or a three letter agency or business radio. What a particular business uses in one area may be used by someone else in a different location.

A Head Start in Listening

To some extent, you have already acquired this skill, but in a way that you may have not realized. Television. Think about it. You are watching a sitcom in which the typical American family are in the back yard playing with the typical American family dog. Instantly, the playful yips and yaps are coming from another dog in another typical American back yard, and Lorne Green is telling you about how great Alpo is. (I wonder if he has actually tried it). The networks



are sneaky in how they work these commercials into the program, and if they switch back to the program quickly enough, some folks might not even realize it *was* a commercial. This is almost subliminal; for some reason they feel the need to go buy that brand of dog food. Even if they don't *have* a dog!

Some people are more astute. They instantly see that this is a commercial. And, again, so it is with scanning. As your radio hops from one station to another, you soon learn to tell that you are receiving a different station, based upon having learned how to Listen!
Now, here are some things to consider. To learn.

Listen! Learn to identify what you are tuned to
There are a lot of stations out there, a lot of services. This chapter is about how to quickly recognize and identify the type of service you are tuned to. Some things to Listen! for. And while everything here is reasonable accurate, based upon many years of monitoring, it is not absolute. There are exceptions.

Signal Strength and Clarity
Commercial and government radio systems are designed so that that reception is full quieting meaning no background noise, and sound quality is such that the transmissions are clearly understood. For law enforcement and other emergency services, lives often depend upon radio communications.

So if you tune in something where the sound is muffled, like the voices are " inside a barrel" this should start to narrow down the source. You may be intercepting a baby monitor or if your are lucky, even a surveillance transmitter. Think frequency. Most baby monitors use cordless telephone channels in the low VHF range; 46 and 49 MHz. Surveillance 'bugs' can operate on virtually any frequency but those used by amateurs are most likely on or just above and below FM broadcasting. An experienced spy will use other frequencies and the Feds probably use Spread Spectrum which you aren't likely to hear at all.

Duplex and Full Duplex
Duplex refers to radio services where the mobile units can talk to each other through the repeater but only one can transmit at a time. Full Duplex means both parties can talk at once. So, when you hear this, you are most likely tuned to a wireless telephone. But, it could be a phone conversation between two actors in a TV program, or cable TV leakage. Think frequency.

Length of Transmission
Wireless telephone (cellular or cordless) conversations may go on for hours. Cellular calls, which once were kept short due to the high cost, tend to be longer now that the price has dropped and usually longer than commercial two-way radio which tend to be brief. Local police departments sometimes need to make long transmissions when describing several suspects at a crime scene, but will usually break them up into a series, to temporarily clear the air for an incoming emergency call. Fire department transmissions are usually short and somewhat terse.

Gender
Once, the world of radio communications was male dominated. Today, this is no longer true. And while you can not necessarily identify a service by the sex of the person speaking, you may be able to narrow it down.

Police dispatchers are more often than not women, particularly in large cities. Here in San Francisco, I sometimes hear one male but the rest are female. Fire Departments are more likely to use male dispatchers for some reason. Taxicab companies may be either sex but are more often males. Most of the voices you hear on Federal law enforcement agencies will be male, but not all.

Age
Sometimes you can make a good guess as to the approximate age of a person, sometimes not. Elderly people may sound their age, as might the very young. It is unlikely that, at either extreme, they will be dispatchers for a police or fire department but they might work for a cab company.

Neither are likely to be dispatching for a federal agency, or to be an agent on the other end of the communication, but people of all ages may use the General Mobile Radio Service (GMRS) as well as amateur radio frequencies and of course, wireless telephone.

Voice Quality
It is easy to tell when you are tuned to a commercial station. Professional broadcasters such as newscasters disk jockeys and people who make TV commercials are easy to recognize; you hear them every day. So should you hear these 'polished' voices on your scanner, you may wonder why. There are a couple possibilities.

You may be hearing a remote broadcast channel; an on-location reporter relaying to a radio or TV station. Or, in the UHF bands, you may be hearing the audio from a TV station which is FM. Hint: if you hear a lot of 'buzzing' sounds that lock up your radio and you have to keep hitting the SCAN button, then this is probably what you are tuned to.

What frequency band are you on?

Terminology

You hear 'Dry Standpipe', 'Phantom Box', or 'Engine Company', then you are tuned to a fire department.

Ambulance attendants and Paramedics frequently use phrases like' conscious and breathing' or 'equal and reactive'.

Should you tune in a taxicab company, you will hear terms like 'No-Go' (passenger wasn't at the pickup location) 'Bingo' (after dropping a passenger, at that location there was another one waiting for a cab) 'Stand' (A taxi stand, a place where cabs wait for the next assignment) and you may also hear conversations if the cab company has duplex radio system; the drivers talking back and forth. I drove a cab for a while after graduating from college, and I can tell you it can get really interesting. Especially late night at a small company.

Physical descriptions of a person, height, clothing, etc. usually means police but could also be a private security guard company. And remember voice quality and background. It could be cable TV leakage or someone on a wireless phone with the TV turned on.

If you hear the word 'signal' you may be tuned to the FBI as this is a word they sometimes use for agent. Another FBI term is '91' which means a bank robbery and they frequently ask for signal check; radio signal quality.

The Secret Service often use the agents name and city. 'Baker, San Francisco' is agent Baker calling the San Francisco dispatcher, and on Customs Service channels you will frequently hear the word 'sector'

What seem like ordinary household items such as pillowcases, towels, sheets, might not be emanating from someone's house; you may be hearing the house-keeping staff at a hotel. Their security guards may use the same frequency, and these channels can get very interesting! If you hear 'Raven' and 'Eagle' you are probably tuned to Hilton Hotel security.

Emotion

If you hear someone getting emotional, raising their voice, screaming, you may be tuned to a commercial station (movie, sitcom), relay link or cable TV leakage around 150 - 170 MHz, or wireless telephone. Perhaps business bands, taxi companies (not all that unusual), and some local government agencies such as public works, street cleaning and etc. Some of the people at these agencies here in San Francisco get real chatty, since they (apparently) don't know the new trunked system can be monitored.

Amateur radio is another possibility, what with the way it has deteriorated in recent years. But this is rare on law enforcement radio.

A few years ago, I was sitting here typing when I heard gunfire. Full automatic and not far away. A few seconds later I heard sirens. I spun the knob on my R7000 to the Police Instant Communication channel 3 (460.075) and heard 'code 33'. Police codes vary from one area to another but in San Francisco, 33 means restricted traffic; an emergency situation.

A sniper fired dozens of shots, hitting several people including two police officers. Even though two cops had been shot, the officers and dispatchers maintained the same calm professionalism as always. True, as an experienced scannist, I could sense the stress in their voices but no one lost control through the entire incident until the final Code 4: 'Suspect in custody'.

Laughter

On how many stations you monitor will you hear people laughing? Well, you rightly figure wireless telephones and the Family Radio Service, of course, GMRS (General Mobile Radio Service, a Citizens Band on UHF) which is also likely, and perhaps some business channels as well as, yep, taxicab companies. Also commercial radio and TV stations and remote broadcast locations, and possibly on amateur radio. On Fire department channels this is most unlikely but don't overlook police departments. It is not unusual to hear people chatting and laughing quietly in the background at the San Francisco Police Department.

Profanity

Profanity, 'foul language' or whatever you want to call it is a no-no, but you still hear it. The most likely service is, of course, wireless telephones. Other possibilities are amateur radio (especially since unlicensed operators can walk in and buy two way radios at Radio Shack) and possibly GMRS and FRS. As you already read, cab drivers sometimes get a little hot and become rather expressive. Like when a competing cab company 'spears' (steals) their passenger at a pickup point. Yup, some cabbies have scanners, too.

On law enforcement, this is unusual in big cities. In years of monitoring I heard only one such incident. An officer referred to a wanted person as a 'SOB'. This person had fired at one of their vehicles and one can hardly blame to officer. In small towns, the officers may be a little less 'formal'.

Background Sounds
The music announcing the TV news is much the same from one station to another, and it is something you instantly recognize. If you hear it, it could be, again, wireless telephone with the TV in the same room, but not police or fire departments. It could be a surveillance transmitter but not a baby monitor. A taxi dispatcher is a possibility but business band probably not.

Sirens in the background is likely police, fire, ambulance, but if you also hear music, then wireless phone is likely as is cable leakage. People screaming- any number of possibilities. I heard on San Francisco, a crack house raid going down. Lots of screaming, no music, and as it was an undercover operation, no sirens. Until later, that is, when there were a lot of them.

Put It All Together
Your radio stops on a signal and you want to know what it is. You stop the scanning and wait for the next transmission. Think about what you have learned so far. What frequency is in the display and what does that tell you? How long do the transmissions last? Is the sound quality good; easily understood or is it muffled? Can you hear both sides of the conversation? Are the voices excited? Are they cussin' up a storm? Listen for the terms you have read about. After a while, all these things will become second nature and you will quickly know what you are hearing.

Hear! The Many Transmissions on the Airwaves
The following is Part One of a general guide to the many services that use radios to transmit various kinds of information, analog and digital. It is an overview to give you an idea of what there is to monitor. Some services may no longer be used and there will be some I have overlooked. (I am presently in New Zealand).

It is not intended to be a complete frequency list. Although I have added some frequencies along with comments and explanations, they aren't necessarily the same from one location to another. Remember that frequencies are often re-assigned, such as when a business closes or relocates, and that some agencies, especially federal, have many different channels and might be heard just about anywhere in the spectrum. Therefore, while I can not guarantee that any of these listings are absolutely current, the areas in which most of the stations/agencies operate are for the most part accurate. GMRS is the same everywhere, the aircraft band is the same, and so forth.

With this information and a little research, you will be able to compile a list of everything you want to be able to monitor. And now, what might you Hear! if you Listen!

ACARS
Aircraft Communication & Reporting Systems This, ACARS, is a method of intercepting signals from commercial aircraft and being able to plot them on a computer screen map. You can actually track the flight of a given airliner. For details on ACARS and amateur packet radio, see http://web.usna.navy.mil/~bruninga/acar.html

Aircraft
Private, commercial and Air Traffic Control For the most part, these will be AM transmissions in the 108-136 band. Basically, the lower half is for navigation and the upper for communications. There are also voice communications from 138 to 150 and 162 to 174 which is where many of the federal agencies operate.

Aircraft Communications
Private, commercial and Air Traffic and Ground Control. For the most part, these will be AM transmissions in the 108-136 band. Basically, the lower half is for navigation and the upper for communications. There are also voice communications from 138 to 150 and 162 to 174 which is where many of the federal agencies operate.

Aircraft In-Flight Telephones
http://www.csgnetwork.com/phoneinfo2.html

Aircraft Navigation
Here will be data signals, 108 to 122 or so. NavComs, Omni signals, and etc.

Air National Guard
These sites have some regional listings, and some frequencies will most likely be shared nationwide.
http://users.aol.com/dramboyer/selfridg.html
http://www.panix.com/~clay/scanning/index.cgi?military

Airport Baggage Handlers
Around 450 and the 800 MHz bands.

Airport Misc Vehicles
Push-back and tow, the yellow trucks that move aircraft around the tarmac.

Airport Security
Can be on many channels, more often UHF than VHF. Some are around 450-455 MHz and some have moved to the 800-900 bands. Also security for some of the individual airlines will be around 450 - 455. Now, you might expect that these agencies use encrypted radios. Perhaps they sometimes do, but the last time I listened, they did not.

Airport Shuttles
Can be on most any band, typically 450 and 800.

Air Shows.
Including the Blue Angels. Check this site. http://radioscanning.wox.org/Scanner/miscfreqs/blue_angels_frequencies.htm

Amateur Radio
Well, usually just hams yacking back and forth, but during an emergency this can get interesting. I was on the air during the Loma Prieta earthquake and able to deliver a few messages to some frantic people. There is also the auto-patch, hams can place telephone calls through the repeaters, transmissions from the space shuttle are rebroadcast on 2 meters and there is NewsLine, the ham radio news broadcast.

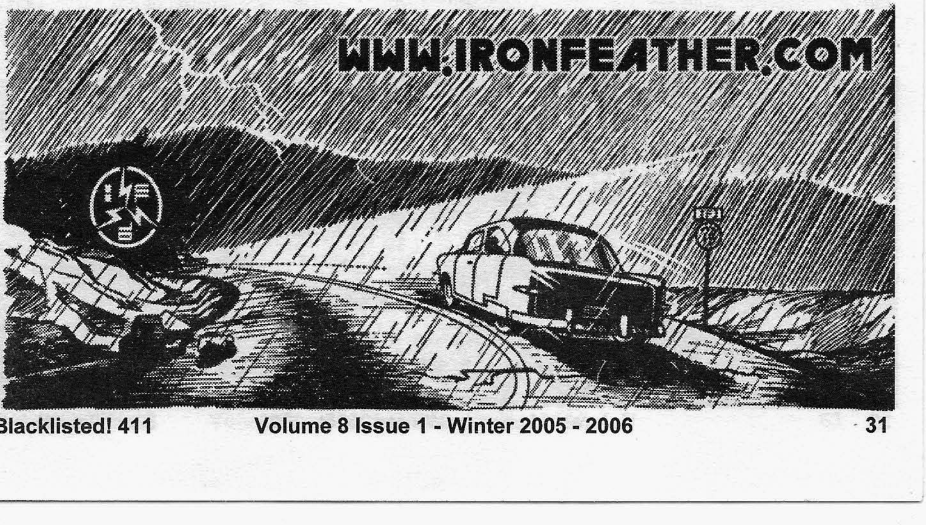
The Discriminator Output
In semi-technical terms, this is the point at which the incoming signal has been tuned in, converted to IF frequencies, RF amplified, and detected. The signal has been converted to audio, and then feeds into the audio stage, amplifying it so that it is loud enough to be heard through a speaker. However, the signal, which is 'pure' at this point, will become distorted as it is amplified. It is at this point that connection is made to various types of decoders, for packet radio, paging (unlawful to decode or monitor) and other data signals

Amateur Packet Radio
Ham radio operators can communicate using data over the ham bands similar to commercial pagers, using a computer and two way radio connected together with a Terminal Node Connector; TNC, with a format much like pagers.

AMPS
Advanced Mobile Phone System - an analog system from the years before cellular. Possibly but not likely still in use in some areas.

Amusement and Theme Parks
Another type of place where, I hear, scanners are not welcome. FRS radios and ham transceivers may be an exception and there are combination two way ham and scanners that may be permitted. Here is another example of how useful the little Alinco 'credit-card' radios are; they can be modified for out-of-band reception.

Analog cell phones:
I wrote a long chapter on cellular monitoring in one of my books, but that was some years back, before the digital system. I guess analog isn't used much any more, and I am not aware of any radios that will decode digital cellular. That is, that we hobbyists are likely to ever own. The frequencies are on any number of web sites, and there are still some scanners available- such as the PRO-2006 that tune them, but again, remember- this is not legal.



Baby Monitors
Is Fisher-Price broadcasting your intimate conversations to the neighbors? Something to consider if you plan to buy one of these transmitters: Some brands will advertise that they are secure; that they can not be monitored by *other baby monitors*. This means other baby monitors *of the same brand*. They use a simple encryption scheme, presumably fixed baseline frequency inversion, to 'scramble' incoming transmissions unless both units are set to the same 'code'. But, at least the one I tested, the outgoing transmission was ***not*** encrypted. So, they can be monitored by an ordinary scanner or communications receiver. Most are around 46 and 49 MHz and depending on conditions can be heard a couple blocks away or more, with a sensitive receiver and a good antenna.

Battlefield Soldier intercoms around 300 MHz
From what I have been able to determine, they use headsets on or around 300 MHz.

Beacons, Low Frequency
From about 100 KHz up to the beginning of the AM broadcast band, they may be identified by two letter Morse code such as OH, 218 KHz, LY on 225, PP on 245 and etc. (These are around Wellington, New Zealand).

Bicycle Messengers
Here is another service that can get interesting. I worked as a messenger for several years, and have heard some minor arguments with the dispatchers, and sometimes very heated disagreements. It is a dangerous occupation and can be very stressful with accidents not unusual. Messengers are usually identified by number (I was 33) or street names. We had 'Mongo, 'Rico', 'SilverWheels' and many others. All business bands may be used, VHF and UHF, also text pagers and NexTel. Some of the trucks use Mobile Data Terminals.

Boy and Girl Scouts.
Check ham frequencies.

BPL
Broadband over Powerline is a fairly new system where high speed Internet access is through the electric power distribution system. It has been installed in some areas and tests have shown that it causes massive interference over much of the HF, up to 30 MHz or so, making international shortwave transmissions difficult if even possible to hear. Your signal reports may be useful, so please keep a log.

Businesses of all kinds
Many bands are assigned to businesses. Some that I used to listen to were Blue dot, Green dot, and Red dot on VHF and on UHF, Silver star, Blue star, Red star and Gold star. One of these was used by the Guardian Angels in San Francisco. There are also private businesses on the 'low-bands' from 30 to 50 MHz. But with cellphones, pagers and Email, two way radio systems don't seem to be used as much as they once were.

Cable TV leakage
The signals on cable TV operate on a fairly wide range of frequencies, and because of leakage can interfere with the signals you want to hear. I had this happen many years ago and was unable to get the cable company to do anything about it until I complained to some of the organizations that use these frequencies. Then, it seemed to go away.

Casinos
You can be sure that security is very tight in places like Las Vegas, and I have heard that taking a scanner into some of them is prohibited. But at DEFCON 13 I had a U-16 and PRO-95 belt clipped under my shirt and they didn't set off any metal detectors, if there were any when I blew $55 on the crap table at Terrible's. I looked for security people carrying radios, and didn't see any Motorola Saber series. Perhaps they are using ordinary analog FM systems, though with the funds they spend on security, they could easily afford encrypted radios. National Communications magazine has a good article on this.

Cellular Telephones
Monitoring cell phones is flat out illegal, whether old analog, digital or Spread Spectrum. In the US the original 832 channels are from 825-849 input and 869-894 repeater output. Cellular types include:

- CDMA, Code Division Multiple Access, which is Spread Spectrum, can not be understood with scanners or communications receivers.
- GSM, Global System for Mobile communications, which is digital and also can not be understood with scanners or communications receivers.

Citizens Band AM
Ah, well, even if you have never owned a scanner, you probably have a good idea what you will hear here. Truckers, of course, but also weirdos who get some kind of kick from interfering, broadcasting sound effects and re-broadcasting other services such as law enforcement. There are 40 CB channels, from 26.965 to 27.405 and may be AM or SSB.

Citizens Band, FM
This is GMRS or General Radio Mobile Service with repeaters operating on 462 MHz. Using GMRS requires an FCC license and permission to use the repeaters. GMRS is used by private businesses, radio sales and repair shops and in some areas, emergency groups. At times, it much resembles the AM Citizen's Band but in San Francisco there wasn't very much traffic. I had their channels on my Icom U-16 in case I couldn't raise any one on the local ARES (Amateur Radio Emergency Service) frequency.

Civil Air Patrol
A part of the US Air Force, the CAP provides emergency services such as search and rescue. A few frequencies to try are 121.6, 122.9, 123.1 which you now know to be in the aircraft band so are AM, and also 143.9 and 148.15 FM. Just above and below the ham 2 meter band, some amateur radios may work slightly out of band to cover them.

Coast Guard vessels
On many VHF marine frequencies. National Communications magazine has a good article on the US Coast Guard with many frequencies.

Cordless Telephones
Also illegal to monitor, which is a kind of paradox. What if you hear a neighbor plotting a serious crime, and report it? You could be prosecuted as well as sued. It has happened before. Some of the early cordless phones operated on 2 MHz. Older but still in use are around 30, 46, 49 MHz, and the license free 802-826 MHz band. Also they operate on 2.4 and 5 GHz.

Delivery Vehicles
Virtually any commercial band; VHF, UHF and up in the 800-900 area. Some larger companies have data terminals as do some cab companies. A list of dozens of .wav files of data transmissions is available from the publisher, on their new web site.

Dog 'Yard Guard' transmitters

Emergency Services
Emergency Broadcast System, Red Cross, FEMA. Search and Rescue operations. Much of this traffic will be on 30 to 50 MHz for long range comms, but all bands will be in use.

Family Radio Service, a license free band anyone can use. Details here:
http://wireless.fcc.gov/services/personal/family/
It is interesting that many people who use these radios are unaware that they can be monitored. So, they often are very chatty, verbal, open in what they have to say. Kids at the mall get out of range, or can't remember where they parked the car and they get frantic some times as evidenced by their choice of expletives!

1. 462.5625, 2. 462.5875, 3. 462.6125, 4. 462.6375
5. 462.6625, 6. 462.6875, 7. 462.7125, 8. 467.5625
9. 467.5875, 10. 467.6125, 11. 467.6375, 12. 467.6625
13. 467.6875, 14. 467.7125

Fast Food drive-up windows employees
Ever wonder what the people in the car ahead of you are ordering? Ever wonder if the people in the car behind you will hear what you are ordering? A Google search will return lots of frequencies, such as 30-31, 457-466 and 170 MHz.

Federal agencies
The feds have frequencies all over the spectrum. They have satellite systems, highly directional Yagis for line of site and who knows what else. For the most part, they use UHF in the cities and now and then if you have a good list, and especially if you have CAS, you might hear a drug bust going down or a bank robber being caught. If you hear the

word 'RAT' it means they are using the system that tracks a transmitter hidden in the stolen loot. You might also hear 'how many bars' which refers to the signal strength of the transmitter. A few other terms that may still be in use and to listen for are 'Sector' which is US Customs, 'Signals' and '91' (bank robbery) which is FBI. Some Secret Service words are 'Charlie', 'Wheels Up', 'Package Delivered' 'Lead', and 'Tracker'.

Unfortunately, just when it gets interesting, they switch modes from 'in the clear' to digital encrypted. A web search will get you many lists for federal agencies frequencies. While I have never heard, on shortwave, transmissions known, verified, to emanate from the FBI or DEA etc. it would be illogical to assume that HF is not being used by these agencies. Their offices are not all located in the federal facilities. They also rent in many privately owned buildings. So, if you look carefully in a large city, you may see tri-bander (HF) beams on the roofs of some tall buildings.

Fire Departments
Municipal will likely be around 460 - 460.6, 489, or 800 MHz trunked. Rural volunteer departments may be on many frequencies, even CB if they lack funds for a better radio system.

Fire networks, local and federal
Bob Kelty has a detailed list. I have an old one and might post it on my site if I get permission.

Ferries and Tug Boats
Check the marine VHF bands, and UHF.

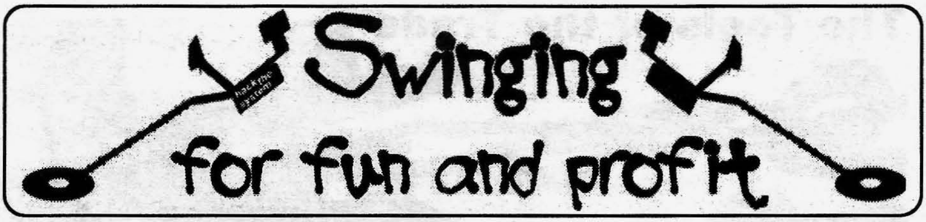
Forest Rangers
Also on the Kelty floppy disk.

Sources
Please consider a subscription to National Communications (www.nat-com.org) which is a first class source of information. Great articles, not just frequency lists. An excellent magazine, available in print or downloadable as PDF.

Optoelectronics
http://www.optoelectronics.com/
Manufacturer of excellent equipment including the Scout and Xplorer.

Shomer-Tec
http://www.shomer-tec.com/site/index.cfm
Mostly law enforcement equipment, but Shomer has radio antennas, long play recorders and other goodies useful to anyone who is into serious monitoring.

SWS Security
While not directly related to monitoring, they sometimes have radios for sale. Hand held two way, mobile units, Motorola Saber secure encrypted portables (NOTE: Sales Restricted) Inventory changes almost daily. You never know what you might find at SWS. But remember: Some equipment is restricted to law enforcement agencies. Serious inquiries only, please.



Swinging for Fun and Profit

By **Wirechief** <sgtrock@camalott.com> and **Israel Torres** <israel@israeltorres.org>

Introduction

That's right folks **swinging** for fun and profit is one of the only "legal" hobbies that most humans of any age can willingly participate at any time of the day with minimal investment and **great monetary gain**. If you haven't figured it out by now I'm talking about the lost and forgotten hobby of **metal detecting** also known as *treasure hunting*, *swinging*, and *walking the dog*. Wirechief and I got our heads together after he posted about metal detecting on the blacklisted411 forums not more than thirty days of this writing.

I had always toyed with the concept of finding millions of dollars worth of treasure in a remote beach setting after reading several stories here and there that made such tales into reality. Until recently enlightened I never found the practicality of slowly scanning the land for trinkets of value long lost and forgotten. Then I started to think about one of my other favorite hobbies known as **wardriving** and I started to put the similarities together. Instead of driving around for miles logging geographical locations of detected signals in the air, I am slowly walking around scanning right in front of my person for precious metals, coins, and jewelry! Both need special equipment to enjoy the hobby and both are dealing with radio waves to find things. In my previous article (*Hardcore Wardriving: Sanity is Temporary, Glory is Forever BL411 V7 I4 F05 pp 71-72*) I quote myself with "*If time is money and you are wardriving then logically you are making negative dollars per minute per mile*". The main difference between wardriving and treasure hunting that is that the more time you spend treasure hunting the more likely it is you will make positive dollars per swing you take. **That's right**, though depending on where you are on the planet and how the laws apply in your areas there is a good chance that **the rule of "finders keepers" works in your favor.**

When some people think of metal detecting they think of late night cable broadcasts with some guy trying to sell a product so he can get rich by trying to sell you the idea of getting rich (usually riddled with a chorus of them showing various treasures found with their product). Others hear the word metal detecting and think of gray-haired overweight people slowly getting their daily exercise in the early AM before calling it a day. Ok, well yes this is true as I've seen it first hand. Though you cannot let this stereotype deter you from making a profit using technology that your grandparents have been using for years. As children we are brought up with the idea that our elders do things for reasons, and as evolved adults we realize a lot of these reasons are really from experiences learned (*and not damaging habits*). From a common perspective **this is a cheap**(er) **and easy hobby that enables you to spend a few hours here and there to potentially find hundreds or even thousands of dollars worth of treasure**. You really have nothing to lose – In fact you are only bettering yourself with each outing and honing your treasure hunting skills. The better skilled you become the smarter you can scan an area effectively enough to know you haven't been wasting your time as well as to find enough treasure to upgrade your unit as needed to find more treasure!

The Tools of the Trade

To become a decent treasure hunter there are a few tools that you must use to get the job done (*See figure 2*):

- Metal Detector
- Digger *(strong small shovel for grass and dirt)*
- Sand Scoop *(for sieving through sand)*
- Apron/Pouch *(for carrying trash and treasure)*
- Headphones *(for hearing sounds of what you are detecting)*
- Knee pads *(recommended for constant kneeling)*
- Extra Batteries (*for Metal Detector*)

The Tools of the Trade

figure 2

As time goes by you'll build a detecting kit with specialized tools and devices of convenience such as a pinpoint detector (a wand-like device to pinpoint the object). Other tools of interest would be a gem analyzer, a diamond detector, and a gold tester to name a few. You may bring a camera along to take pictures of the sights as well as your finds.

The Person

Not everyone has what it takes to be a treasure hunter. It takes patience, tenacity, curiosity and drive to keep going. It isn't like in the movies where you are a tomb raider running around chased by pygmies and getting the babe. In reality you are spending a lot of hours refining your skill and learning new things about yourself. A lot of the times you may question yourself why you are doing this, but don't convince yourself that you are wasting your time. All it will take is a nice diamond ring or dated coin to bring your spirits back up. Though do not expect to find something until you have refined your skill. Until then you will find thousands of pull tabs, bottle caps, and rusty nails just to name a few pieces of junk. You simply cannot hide the fact that if you are a scavenger or packrat this hobby is for you.

The Metal Detector

If it isn't obvious, the metal detector is the most important tool for a treasure hunter (in the interest of metal detecting). The adage of "***you get what you pay for***" is true in the case of this hobby. Though you want to thoroughly research all the options out there for what you want to do. Starting out with a general detector is good if general is what you plan on doing. You may also want to research if there are after market replacements (mods) for your particular model for finer usages.

The Anatomy of a Metal Detector

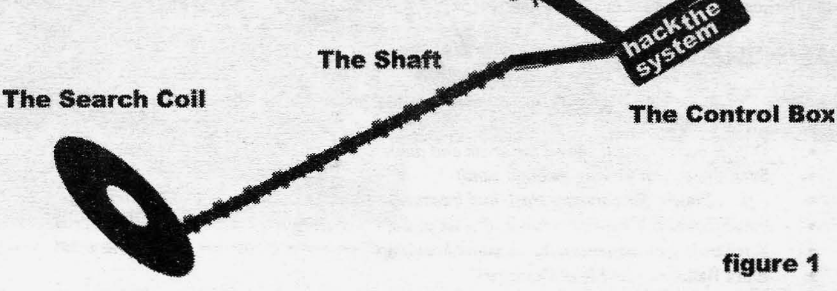


figure 1

The Anatomy of a Metal Detector

The metal detector is a very basic device that has been around for a very long time, and even to this day still consists of 4 basic components (*See figure 1*):

- **The Stabilizer** is the part of the metal detector that usually binds to your arm in a fashion to balance the unit and allow free motion to sweep the unit with far less fatigue so you can swing longer. (This component is optional depending on the model, but you may adapt with after market mods.)
- **The Control box** is the brains of the metal detector it contains the electronics (controllers, processors, circuits) and power for the unit.
- **The Shaft** also commonly known as the Rod is what connects the control box to the coil (often collapsible and adjustable to suit your stature).
- **The Search coil** is basically the antenna for the control box and sends the signals to the control box to be analyzed and interpreted to the user.

Overall the metal detector is a very light device so that a person may carry it for long periods of time without tiring out easily. The device is often balanced to assist in distributing its weight evenly also allowing for longer periods of usage. There are methods to make the device even lighter on your arm by moving heavier parts such as the power pack to a remote waist band, also some units allow for a remote set of controls and LCD. Some units use LCDs and some do not (and settle for analog needles).

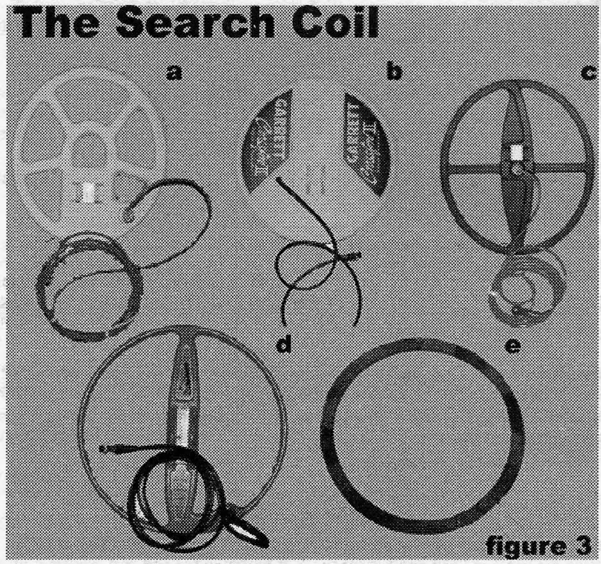
The Control box

The control box is the brains of this device. Think of it as a small computer that has input via the search coil and controls and output via the speaker (jack and headphones). It juices up the coil and processes all the information that the coil is returning. Some control boxes also have a display unit in the form of an LCD, and others have analog needles that allow you to view when an object is present in one form or another.

The standard controls that are featured on a medium priced analog detector are usually a Discriminator, Threshold, Sensitivity, Ground Balance, Pinpoint and probably a frequency shift switch. You can choose with a switch the all metal mode (no discrimination) or the discriminate mode. The operator can also detect in the silent search mode or use the Threshold mode. The discriminator control is labeled so you can choose certain objects to be ignored by the detector electronics and reduce unwanted signals. Detectors are now being fitted with stereo 1/4" jacks for headphone usage. I highly recommend a good set of quality headphones which will completely cover your ears to stop background noise with a volume control included. Detector headphones can be a bit expensive but worth every penny. And speaking of audio some of the high priced detectors have what is called tone I.D. Some units have as much as 4 different tones depending on the conductivity of the target. I personally enjoy this feature very much since I like to hunt by ear anyway. Most but not all detectors include a built in speaker if you just don't like the headphone mode.

Most metal detectors require the operator to tune the device before immediate usage. Some require tweaking a few knobs to help filter our noise and unwanted objects and the minerals at the site you are at. Others require you holding the unit up in the air and pressing a button and then touching the ground and pressing the button again so that it creates an automatic filter. The units I have used have threshold sounds some of them constantly hum a sound and others only generate a sound when something of interest may have been found. The latter are much better and don't make you feel like you are losing your hearing by using it.

The Search coil



When you purchase a metal detector it has a coil already mated and ready to go into the field. But there are a few companies that focus on manufacturing after market search coils which can be a big improvement over some stock coils. The coil is mounted to the support shaft with a nylon type bolt and wing nut and can be tilted forward and backward to get the proper angle to sweep with. (*See Figure 3*)

a. Tesoro 9x8 Elliptical concentric search coil.
b. Garrett 12.5" crossfire concentric (for deep targets)
c. Tesoro 10x12 DD Elliptical (for going deep and reducing the effects of hot ground conditions)
d. Coiltek 15" WOT DD round coil (for handling hot ground to seek out gold nuggets – they go deep)
e. The bare coil (stripped of housing)

Metal detectors come in these three flavors:

- Very low frequency (VLF)
- Pulse induction (PI)
- Beat-frequency oscillation (BFO)

Search coils come in all different shapes (*round, elliptical, or rectangular*) and sizes and are interfaced to the control box through a shielded cable. I will focus on the **VLF** type of search coil. VLF tend to use frequencies below 30 KHz. To understand this better think of a metal detector as nothing more than a radio. The search coil component resembles a loop antenna and is a very critical component of the metal detector system. The constructing of search coils is an art in itself and there are not many that are able to build a water tight good performing search coil. Most search coils are waterproof so that it can be used on the beach or under water as much as 200 feet deep. Once a coil is sealed it is a done deal. Epoxy type resin can be used for this phase of coil construction. Coils are nowadays supplied with replaceable scuff covers to protect the bottom, sides and edges of the coil. They are a life saver when you are bumping up against rocks and posts or trees.

Besides varying sizes search coils come also solid, spoked or have an open center (like a doughnut). When you purchase a (waterproof) coil it will already have the interfacing cable on it that plugs into your unit's control box from the factory. The size and type of coil will be determined by what kind of loot you are looking to find. Some coils can be as much as 25" in diameter and as small as 4". All of these attributes are configured for specific metals and levels of depth you are targeting. There can be many variables that can determine actual depth but it is commonly accepted that if a coil is 20" in diameter it will have a detection depth of 20". The size of the target has a lot to do with detection depth. I know what you are thinking, so I will go out and get a 30" coil or bigger but you have to consider the weight of such a large coil if you're going to be swinging it all day! Another drawback of very large coils is they are not as sensitive to smaller objects such as small coins or jewelry. A very large coil will also be more apt to pickup unwanted targets such as junk iron or metal because it is sweeping over more real estate than a smaller coil. A smaller coil can actually get between trash targets more easily therefore reducing the number of unwanted signals. Some treasure hunters carry a smaller wand-like detector to be able to pinpoint probable targets after first detecting them with their primary detector.

Search coil variance also can be attributed by coil type known as concentric, coplanar, wide scan, or DD.

Concentric and Coplanar

Coplanar is round in various diameters. There are 2 separate coils but located in the same plane. The transmit coil is in the outer diameter and the receive coil is in the center and situated such a way that it doesn't get saturated by the transmit signal. As soon as the instrument is turned on the transmit coil is energized and creates a constant electromagnetic field (EMF) which is shaped like a fat doughnut and extends above the coil as well as below it. The further from the coil the field gets it begins to take the shape of an ice cream cone. So at maximum depth the field is quite narrow and that is why you need to overlap each sweep of the coil. The field can extend out to the sides of the coil also. This is why we have a coil shaft that is nonconductive as not to cause any false signals above the coil. When a conductive target such as iron enters the field and not filtered by discrimination it distorts the EMF and causes a phase shift of the field and is sensed by the receive coil and sent to the control box to be processed, and eventually identified. The swept target actually becomes energized and emits its own eddy currents to the receive coil. To eliminate extraneous and unwanted noise a Faraday shield is sprayed onto the surface of the receiver during manufacturing. The thickness of this shield is very critical. Too much shielding and you lose sensitivity, too little and you will have excessive noise. The windings are bundled together in a non-uniform pattern. The geometry of the windings will also have a substantial bearing on how well your coil will operate. Some builders use magnet wire, or Lietz wire.

Inductance values in search coils can vary from just over 300 uh to as high as 500 uh or more to match the instrument being used. Resistance values are very low from 1 ohm for transmit to as much as 6 ohms for receive. Wire size is also another critical issue and for the transmit coil the wire gauge may be around 20 awg while the receive coil being very critical might range in size from 28 awg to 30 awg with half point sizes like 28.5 awg. The Q of the coil needs to be kept at a low value also. Capacitors and resistors can be installed in the coil to attain proper operating parameters also but capacitance must be kept at a very low value. Actually the most difficult part of coil building is the construction of the coil itself. Getting everything properly positioned and spaced can mean the difference in a good performing coil or one that doesn't work at all! A handy instrument to have around is an LCR meter along with a DMM so you can make actual measurements for coil parameters.

You are probably wondering why metal detecting works only if you swing the detector, here is why. A search coil works like a generator from the standpoint that you have to have motion so that the lines of force, being the Electromagnetic Field (EF), will be cut across if there is a metal object in the ground and then the metal object will emit its own field to the receive coil and on to the control box to be processed. Also the electromagnetic field has a set frequency that it oscillates at. Say we are at 10 KHz then the field is changing polarity 10,000 times per second and the field from the target will be opposite to that of the transmit coil.

Double-D coils

There is also have another factor called ground noise or ground mineralization. This can be a very real problem for people that are located mostly in gold bearing country. States or countries can have tremendous amounts of minerals in the makeup or matrix of their soils. This also includes wet sandy beaches and ocean water that of course contain salt. These minerals can easily mask a valuable target to where you may not see an indication of it's presence at all. So that is why a good many metal detectors have built in ground balancing circuits and can be manually set by the operator or they may be built with auto ground tracking so you the operator will not have to be constantly adjusting this control. So now I introduce the DD coil or Double-D (Don't laugh, I know what you are thinking…). This type coil can be of an elliptical shape or round. It has two separate coil windings each shaped like the capital letter D. The two coils are positioned in the coil form so as to have the flat sides back to back slightly overlapping. The amount of overlap is somewhat critical to its performance. The pattern of the field is like a blade which runs down the center of the coil to its full length. This overlapping of the two coils has a noise canceling effect on ground mineralization and is popular with the electronic prospector crowd that hunts for gold nuggets. Also since the field runs the full length of the center of the coil it helps you to cover more real estate quicker. One side of the coil transmits while the other side receives. Depth is also quite good with these coils.

Wide Scan Coils

Another type of coil is the rectangular wide scan model which has a great advantage of really covering a lot of ground! They can be as much as 18" long and also fight ground mineralization. They are favored at beaches because of these abilities. The depth detection is not as good as other coils so you have to determine the type of detecting you want to do when using this coil. They can be somewhat cumbersome because of the length which also shifts the balance. Remember weight is a big factor in how long you can stay with it during the course of a day's detecting.

As mentioned prior coils come in many flavors for different uses and different users. Experimentation often evolves into more experimentation .For example there are even coils that have circuitry embedded in them to communicate with the control box to let it know what frequency to operate on so that you get a great match up! I just found out there is a company that has designed a double coil that is mounted side by side; this will be interesting no doubt. I have also heard of a figure 8 style coil. So there is much room for experimentation and I think this is one aspect of this hobby that makes it fun.

The Rest

The shaft that support the control box and search coil are user adjustable and come in 3 pieces normally so it can be broken down for traveling or hiking or biking or whatever.

Metal detectors are like everything else, they are becoming more and more digitized. Even the analog units have some digital stuff in them. For example the Lobo SuperTraq which has analog and micro processing circuitry involved in the design. The auto ground tracking is monitored and operates through a microprocessor circuit so you don't have to continually be making manual adjustments to compensate for changing soil conditions. There are several models that have full digital displays and DSP circuitry. These units can get very expensive but can be well worth the extra expense as long as you know how to utilize them to their full extent. The Minelab Company has just released a mid-priced design that is practically all digital. It uses a technology that has been dubbed as V-Flex Technology by Minelab. It uses DSP to convert the analog signals from targets to the digital domain therefore attaining a much more clean and stable and sensitive response. Even the audio is digitally recreated which to me sounds very good! This model has a large LCD readout that indicates approximate depth of target, whether it is ferrous or nonferrous, a numerical indication of the conductivity, sensitivity, volume, ground balance. It has all metal mode or two different memories for customizing your own settings that will remain until you change them. It has tone I.D. and overload tone when the coil is saturated by a large or near target which overloads the electronics. All of this and more in a single pod that sits atop the handle grip which can be removed and carried in a coat pocket. This unit will also have various accessory coils for other frequencies so that it can be more focused to a particular type of detecting. All of these various parameters are set or changed via a membrane type switch pad.

There is also a company that installs all of the electronics in the headphones making the adjustable shaft even lighter. You can even order them with an external pin pointer that is detachable and mounts on the shaft. Stand alone pin pointers are very handy in helping you locate the target when it gets lost in the loose dirt or sand. This detector has three control knobs on the earmuff labeled Discriminator, Volume, and Sensitivity. They are made in several configurations to suit your hunting style. I have the Landpro with either an 8" coil or 10" coil. They work quite well and are very easy to operate.

I am not going to go into prospecting detectors because they are in a different category and price range all together. Goldnugget hunting is a whole different ballgame and isn't like a drive to the park. I will say these types of instruments go very deep and involve a little more than just strapping it to your arm and walking the dog! Overall most detectors are easily learned in a short time span with the exception of the top end digital models. When you start finding targets to dig I will recommend you get a quality digger instead of going to your local K-Mart and buying a $3.00 garden trowel because you will bend it in short order, believe me I did it too. Get something to put the junk you dig in one pouch and your treasures in the other, something like a carpenter's nail pouch. Remember even if it is trash that you dig take it with you to a garbage can so others won't waste precious time digging it back up.

Hacking and Mods

Modifying metal detectors is definitely for the experienced technician especially with the SMT circuitry involved. The big drawback is that detector companies guard their designs very closely (- *make sure you find out if your local, state and federal laws allow modifications before publishing them, or attempt to sell them*). Even detector dealers can't get any schematics from the big boys in the business. This is because they quite simply don't anyone to hack their designs (*even if it is for the better*). Making any type of modification (or even repair) may violate any further service from a company that issues lifetimes warranties on their products. In reality most of these instruments are coming out of the factories with peak performance so the most desirable thing would be to take a low cost model and upgrade its status to meet that of a more expensive unit (*without paying the higher price*). One unnamed company produces its cheapest model with the ability to do just this. The front panel template has extra holes drilled out to add the additional controls for a few more features *(See Figure 4)*. So if you know what your doing you could possibly upgrade the model another 3 levels. The best thing to do is pickup an older model that has thru-hole PCB's or point to point wiring to satisfy that urge to explore or experiment.

Some of the more expensive digital models run on software and can actually be reprogrammed and updated to enhance the performance in a particular function. There are a few books that have been published on some of the more popular detectors to fine tune them using these methods. I have also seen a couple of advertisements selling chips that are enhanced with better software to improve certain areas of performance. Research any type of hack or mod thoroughly to be sure it is for real and won't send your machine into a meltdown mode. Older models found at garage sales often perform quite well (depending on how it was treated before it was posted for sale). If you choose to hack a detector, be sure you have got the equipment to do a good job. I believe there is an unnamed detector company that uses the modular board design approach where you can change the boards to get an upgrade which is very nice. I have heard that it is a very good detector.

Hacking and Mods

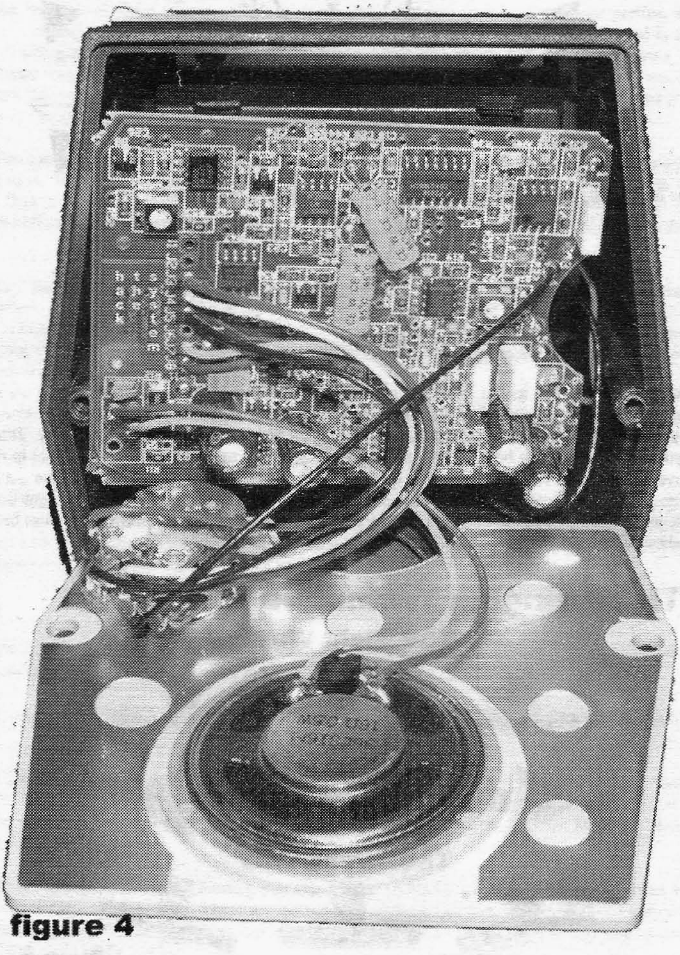


figure 4

The Technique

Metal detecting relies heavily on knowing how to use the detector. Sure anyone can pick up a $1200.00 unit and skim the beaches and find something. But without precision you will be missing a lot of potential finds that others will find eventually. One of the common understandings is to swing slow and low. You can't be in a hurry because you are never going to get done. Just scan the area you are interested in until you are no longer interested in it. Come back later but keep in mind a few landmarks or GPS coordinates if you want to extend your search further. Many times I've gone over the same area over a few days time and have found something new. Don't be afraid to let the coil glide over sand peaks or grass. This is why you have a coil cover to protect your coil. Logically you don't want to drop your coil or use it as a shovel but it is made to tolerate normal usage. If you swing too high off the ground it is likely you aren't going to hit the depth the detector is rated for and again be missing potential objects that could be yours.

Swinging slow and low (See Figure 5)- The idea is to make very slow and deliberate swing motions and walk in a straight line. You will appreciate using the stabilizer if your unit has one. Doing this for hours on end gives your arm quite the workout!

The Technique

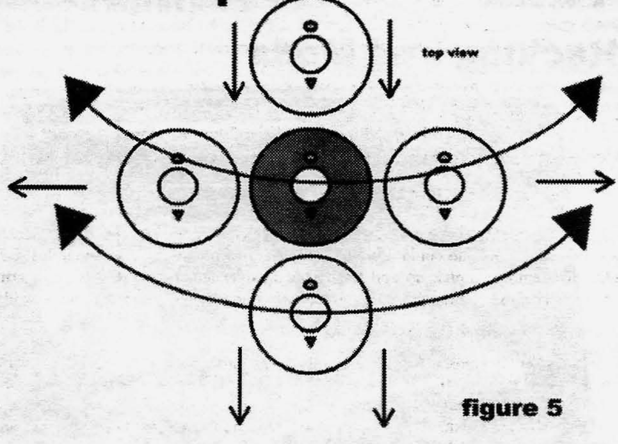


figure 5

Be very careful to keep your coil as flat as possible without letting it canter up or down while you are swinging (*See figure 6*). This will give you false readings because you are exposing the head to other elements. You must be very robotic about your motions. There is no need to give powerful swings to surround your entire body. This is all wasted movement if your coil canters. It is better if you are deliberate and keep to a few feet at a time right in front of you. It is OK if you overlap your coil swings. Remember the EMF is in the shape of a very small cone and not necessarily as large as the size of the entire coil. Keep focused and move slowly. I like to engage in long straight lines or create a grid with 90 degree angled patterns to be very consistent with an area. This way I know the area has been completely covered to the best of my ability.

The Swinging Technique

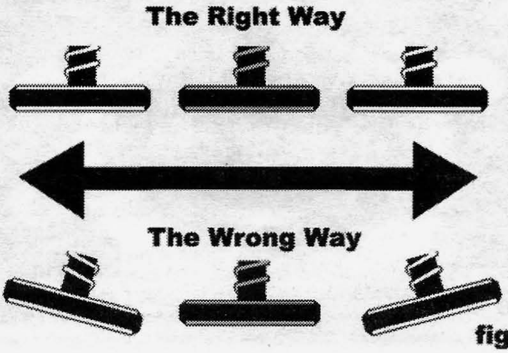


figure 6

Lastly watch where you are going, and be aware of your surroundings. I like to treasure hunt with at least one other person in case things get hairy, but I haven't had a problem to this day. One tip is that when you have identified an object as being valuable - **do not** jump up and down yelling **EURKA**! This will draw unwanted attention to yourself. You would be surprised as to how many all-of-a-sudden owners say the object is theirs! It is best if you quietly place the found item in your apron for later analysis and determination in the safety of your garage. Remember Finders Keepers (*where applicable*).

The Targets

Objects of value will be found where people frolic and congregate. The more people that saturate the target at different intervals, the more likely you will find something after they all leave. Some treasure hunters like to hit the scene at night when everyone has just left, others save their energy for daylight in the early morning. This game is all about the bird and the worm. If you are looking for cash, coins, jewelry, and much much more you can check out these places:

Beaches: During the summer time beaches offer some of the best cycling of summer parties by the fire pits, and the highest saturation of people during the hot days. If your detector is water proof a low tide proves well for finding lost rings where people wade but forgot to leave their rings at home. Using a sand scoop (sieve) to quickly seek your finds proves best. Most of the time nature will plug up the holes within a few minutes.

Parks: Similar to beaches these places offer best when they are packed full of summer parties, BBQs, picnics, birthday parties, receptions and etc. The one real big downside that some of us have experienced is that digging 10 inches through crab grass and then plugging the hole to make it look like no one was ever there takes a lot of work and effort. Sometimes more than you want to put into finding a penny. Be sure to respect the place you are hunting at. Also make sure it is legal in your parts of the woods. A lot of parks that are protected and preserved prohibit treasure hunting and you can get heavily fined and get your toys confiscated!

Sand Pits: You can usually find these where parks are so the kiddies can play in the sand or wood chips. These areas usually don't have very deep sand and could use a quick sweep over just in case someone lost a ring, or some villain buried razor blades. Remember to pick up and trash you uncover and report if you find harmful findings to the authorities immediately. The less you touch something the better chance there is of finding the villain through forensic science.

Ghost Towns / Battlefields: It is possible if your area has some history that you may have a few abandoned towns that you are allowed to pick through. If you are looking for old coins or pieces of history like fired rounds to collect make sure it is legal first. You will have better luck by researching old maps of your area to see where the ghosts of the past bade their time. Make sure you are well equipped if you are trekking out to no mans land. The last thing you want is to become a piece of history while looking for history!

Public Land: You can search maps and state records for areas that allow treasure hunting. Many clubs have this information available for interested parties, sometimes for a fee. Make sure the information is current before going out there; also travel safely if you are unfamiliar with the place you are going. Think "*Leatherface*".

Some things to keep in mind while treasure hunting is what is known as **The Halo Effect**. For example when a coin has been in the ground for many years (e.g. 50 years or more) the coin tends to mix with the minerals surrounding and makes the coin look bigger than it actually is. This makes it more difficult for you to zero in on it. Don't give up and apply the techniques you have learned in this article!

The Decision

You now know just about everything there is not know about metal detecting. With this knowledge you are now able to wisely choose whether or not this hobby is for you.

Before going out and spending some serious cash (or credit) on a shiny new detector consider these few words of advice.

- Chances are you know someone who tried out metal detecting for a few days (before realizing it wasn't for them). If they are the packrat you remember them to be ask them to borrow it and try it out (they may be willing especially if you seem interested enough to take it off their hands for at least half of what they got it for.)

- There are several types of hunting you can indulge in which might be looking for coins, relics, jewelry, prospecting, or meteorites. There are instruments or machines that can do all of the above and others are geared more toward one or two types of detecting. If you like them all you may end up picking up more than one as time goes by.

- If it sounds too good to be true it is. Don't be so cheap that you end up fooling yourself into thinking that metal detector from Target is a good buy. You get what you pay for. You will get the most out of your money by familiarizing yourself with what is out there and what deals are coming down the pipe. Visit your local dealer and ask them when a deal may be happening. They are usually nice enough to let you know, or may even offer you a deal on the spot. Selling metal detectors is a very small niche market so it takes a certain type of person to want to sell these, and most of them really want to inform you on all they have to offer before even suggesting you buy one from them.

- Know ahead of time what you plan to hunt before purchasing just any detector. Some have better discrimination and depth and noise canceling ability, along with a price tag to match. Researching is a very important aspect of treasure hunting.

- The instruments they are making nowadays are really much better than even 5 years ago. If you can afford to buy a new instrument do it. This isn't your grand pappy's hobby anymore! Though if he doesn't mind you borrowing his hardware go for it!

- Don't go over the top - you can go out and buy a $1200.00 instrument but unless you know what you're doing it will not find any more than a $99.95 detector from your local radio shack. Practice makes perfect and perfect it you should.

- Look for name brands; some of the companies that are currently manufacturing these devices are: Tesoro, Minelab, Garrett, Detector Pro, Whites, Bounty Hunter, Compass, Troy, and Fisher. In my opinion all of these companies make fine instruments and of course they all can have a lemon from time to time. One of the most basic detectors is the Tesoro Compadre. It is a turn on and go instrument with one knob operation and is priced right. The performance is excellent and it is fun to use.

Here is an example of using a basic unit and making out like a bandit: I was out in the front drive not long ago with the Compadre in hand when I got a really sweet tone on the headphones and 4" later I pulled out a 1942 wheat cent in very nice shape. But wait a minute, I scanned the hole again and still had a nice signal when I pulled out two more wheat cents, a 1942 and 1951.

The Tips

One thing you should do is after a day's worth of detecting is remove the cover and clean out the fine dirt or sand that can get in between the coil and cover itself. This material can cause a lot of false signals if not cleaned out regularly and build up occurs.

By searching for garage sales you can often pickup older detector models that look brand new because the owner got frustrated after a couple of hours of usage (*usually a month or so after Christmas*) Be sure to check for signs of battery leakage. These detectors have probably been in the back of the closet for several years. By using your SE skills you can pretend that you don't know anything about them and get it for less than if you talked as if that was what you have been looking for.

Always recheck your dig to see if there might be multiple targets, which is not uncommon.

If you hunt in the discriminate mode and you're mainly searching for gold rings or chains not to turn the discriminator control too high. It seems the laws of physics have determined that **foil and pull tabs have the same signature or phase shift as gold rings and jewelry**. You would think that a gold chain would present a pretty good target to your detector but since the links are loosely coupled it might only see one or two links. So if you choose to ignore pull tabs and foil on the discriminator setting then you could miss that $50,000, 3 carat wedding ring!

Always check out abandoned cigarette packs. Your detector may pick them up in the sand, but did you know that people often stash money and other valuable there before entering the waters at the beach. They later end up flipping the pack over with their towels in a rush to dry up and end then up not being able to find where the pack inadvertently got buried (or plain just forgot). There are a few famous stories around about one fellow who found 7 – 100$ bills in a cigarette pack. Be sure to check out the pack before carrying it around just in case there is something else stashed in there that you wouldn't care to be caught with.

… there are millions of tips out there and the sites cited below contain more than enough to fill a book – Remember not all secrets are shared, which means you'll have to dig deeper to find them.

The Conclusion

Treasure hunting isn't your grand-daddy's hobby anymore. There are tons of clubs out there that hone their skills using many types of pinpointing games, and identification games. There are group outings to faraway potential digs and contests to keep the hardware rivalry going. Competition is one of the better ways to evolve.

One thing I would love to see with the generations to come is seriously modifying the standard metal detector with portable computers to make this a more efficient hobby without making it too expensive. It seems that even though metal detectors have been out for a long time, they haven't evolved with the rest of the world in terms of technology. I'd love to see a hardware hack that allowed you to use your PSP and somehow enable your shoes to become metal detectors. Perhaps even some type of USB, WIFI, BT, GPS configuration that allows your unit to keep track of everything it has logged and where to become closer to the aspect of wardriving and the details it keeps. I could see a contest coming up where you can create a autonomous robot to scan an area and let the observer know it found a precious metal, maybe even contain it for further analysis! – GET TO IT!

When it comes down to it you have to look at treasure hunting as a form of scavenging things that are lost (*legally*). We hunt for things you lose. Finders keepers, losers weepers!

The Shout-outs

cynric (blacklisted411 forums)

The History

Wirechief has been metal detecting for over 12 years and is currently a dealer for metal detectors you can find his site at http://www.johnsdetectors.com/

Israel Torres has been metal detecting for less than 30 days as of writing this article. You can find his collection of treasure and junk on his treasure hunting blog: http://www.chroniclesofatreasurehunter.org/

This is the post where all this began:
Metal detecting for extra pocket change
http://blacklisted411.net/forums/viewtopic.php?t=313
Sun Nov 27, 2005 4:47 am

The Misc

There is plenty of material on the metal detecting / treasure hunting hobby. Here are a few magazines you can find at your local magazine shelf to keep updated with the latest tips and technology of the trade:

Western & Eastern Treasures
World's Leading How-To Magazine For Metal Detectorists Since 1966
http://www.treasurenet.com/westeast/

Gold Prospectors Association of America
Gold Prospector Magazine
http://www.goldprospectors.org/

The URLS

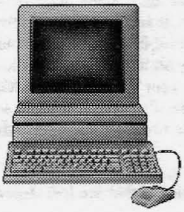
This section contains sources cited and references to further investigate regarding this article:

How Metal Detectors Work
http://home.howstuffworks.com/metal-detector.htm

Metal Detecting Tips
http://gometaldetecting.com/tips-metal-detecting.htm
http://www.tomstreasures.com/tips.html
http://www.treasurefish.com/thebest.htm
http://support.radioshack.com/support_tutorials/games/metdet-2.htm

Metal Detector Sales
http://www.johnsdetectors.com/

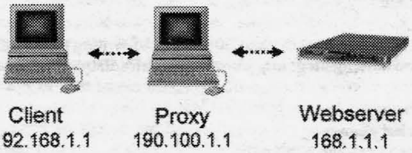
Metal Detectors in General and additional answers to questions
http://www.google.com/



Proxies Declassified

Introduction:
This tutorial deals with the techniques and methods of using a proxy.

What is a proxy?
A Proxy is essentially a gateway or middle man. Its main purpose is to receive data from one pc and forward it to another pc after changing the headers of the packet to appear as if the proxy itself has sent the request. Proxies also have a secondary use. Some proxies are configured to cache websites that are frequently accessed. This will essentially reduce the number of request to the web server. If for some reason the web server was overloaded or shut down, the proxy (If configured right) would send the requested data back to the client.



In The Above Example the Client(192.168.1.1) would ask the Proxy(190.100.1.1) to request data from the Webserver(168.1.1.1). At no time would the Webserver(168.1.1.1) know that the Client(192.168.1.1) was the computer requesting the data. It would respond to the Proxy(190.100.1.1) as if it was the client. The proxy would then send the packet back to the Client(192.168.1.1). This method is one of the most common ones today. This setup would provide the client with "Anonymous" internet access. Any logs that the web server might have would only show the Proxy(190.100.1.1) as the requesting host. This would provide the Client(192.168.1.1) with protection against being identified or attacked.

While this setup may seem like an impenetrable defense, it is really not. Most proxies will keep a log of the clients that have requested its services for around a month. If a DoS attack was launched against the web server using the proxy it would keep the IP, Time, and Date of the request in a log. Unfortunately if the admin of the web server examined his logs and saw that 190.100.1.1 launched a DoS attack against him, he would simply have to find the owner of the proxy and request that the logs from the proxy be sent to him so that he could easily pinpoint the original attacker. If he was able to obtain the logs he would see that the attacks originated from 192.168.1.1 rather than 190.100.1.1.

Another problem with this setup is that since you are using the proxy server for all data being sent to the web server, all private or confidential data sent might also be logged or cached. That means if another host where to request a login session with xyz.secure.com and if your session did not already expire with them, they would be given access to your account and information. To avoid this problem make sure that the proxy doesn't cache cookies or https requests. If it does simply don't log into anything you want to keep (emails, ISP etc..). Some newer proxy servers allow a special feature that caches the cookies into a separate folder for each user.
Example:
User one visits mail.xyzsecureemail.com
Proxy then writes the cookies to (c:\proxy\temporary1\)
If user two connects they wont have access to the cookies from user one.

Even this will still have a problem. If the admin of the proxy server wanted to take a username and password and use it for himself, he could easily access the cookies from temporary1 and use a replay software to connect to mail.xyzsecureemail.com. To fix this problem make sure that your secure site has an option to login from a "public place" this usually sets the timeout to somewhere around 1 min or so. If anyone tries to access it, it will tell them that the session has expired.

Well now that you've learned the basic security problems with proxies it's time to move on and learn some more proxy methods.

Finding A Proxy Server

Finding a good proxy is not usually to hard to do. A lot of websites keep an up to date database of proxies from around the world. Using the simple tracert command in dos will provide you with a detailed explanation of where the proxy exists. Another alternative is to use a online visual trace server. These are free and allow you to pinpoint the exact location of the server. All you have to do is enter the IP or url. The following are a couple of online visual tracing servers.

http://www.all-nettools.com/tools1.htm <-- Doesnt include visual trace but nice tools *1
http://visualroute.visualware.com/
http://visualroute.visualware.co.uk/
http://visualroute.brd.net.au/
http://visualroute.webhits.de/
http://www.visualroute.it/vr.asp

These links will provide you with a map and a graph showing where the server is located.

Using the proxy server

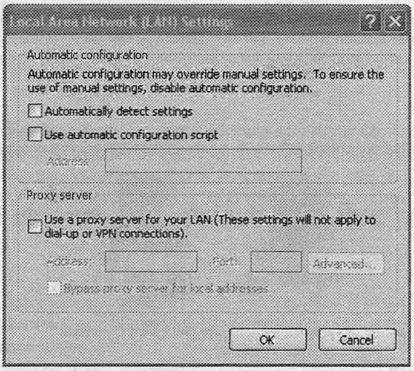
If you have already found some proxies you can begin testing them. Probably the first thing to do is ping them to see if they are even alive.

```
c:\ping xxx.xxx.xxx.xxx
```

If you get a timeout from the server or it drops packets then its probably not a good idea to use that proxy server. After you found some proxy addresses that actualy exist it is probably best to see if you can actually connect to them.

Depending on what software you are using there are different ways of doing this.

In Internet explorer you can configure your proxy from Tools-->Internet Options-->Connections-->Lan Settings



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

□ Bypass proxy server for local addresses

Proxy Config In IE

The bottom part is the part you need to configure. First make sure the checkbox next to "Use a proxy server for you LAN" is checked. Next enter the the IP or url of the Proxy server into the Address Field. Next you have to enter the port on which the proxy is running on. Some common ports that are used by proxy servers are 8080, 80, and 81. Usually the people that you get the proxy from will provide you with the port number. It is important that you enter the port number correctly. Now that you finished configuring the page click ok and go back to IE. Now its time to test it. Type in a url that you know will work. For example www.google.com. If you get a time out error or page can not be displayed then its probably a bad proxy. If you where to type in www.google.com and get some website like fakeproxyserver.com then you probably entered a http server and you are simply getting the default page. Now if a proxy requires a login you probably will get a access denied or please login request. You can try and brute force it if u want or look for possible exploits for the server.

Q&A

Wait im not getting any pictures? This is probably because the server is blocking them to reduce bandwidth.

I cant seem to login to anything (forums, mail, etc..)?
Well this probably mean that your proxy server wont accept the cookies needed to login to most sites. You can configure your browser to not use a proxy on the https and ftp servers. To do this simply use the advanced button in the IE configuration window.

It take forever to load a page.
Probably a slow proxy server.

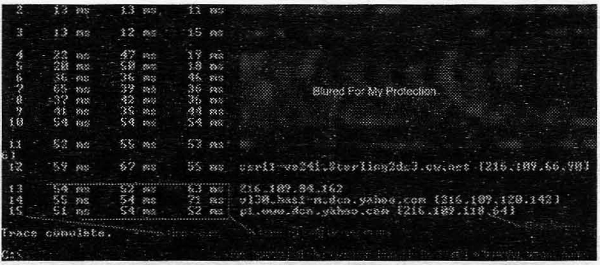
I found a proxy, how can i make sure im totaly hidden?
Well first you're going to need to know your IP. You can test it to ways. The easiest is by going to a site that will display your IP.

Listed below are a couple of webpages that should allow you to do this.

http://www.whatismyipaddress.com/
http://www.netins.net/dialup/tools/my_ip.shtml
http://checkip.dyndns.org/
http://www.dynip.com/main/ns/146/doc/69
http://visual-basic.org/ip.asp
http://ip.nefsc.noaa.gov/ (Goverment Website.)
http://www.webcogs.com/whatsmyipaddress.asp

The other option is to use the tracert function.

Start--->Run--->Command (Hit Enter)



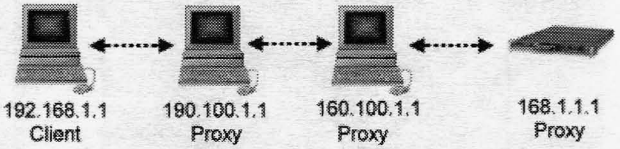
```
  2    13 ms    13 ms    11 ms
  3    13 ms    12 ms    15 ms
  4    22 ms    47 ms    19 ms
  5    28 ms    58 ms    18 ms
  6    36 ms    36 ms    46 ms
  7    65 ms    39 ms    36 ms          Blured For My Protection.
  8    37 ms    42 ms    36 ms
  9    41 ms    35 ms    48 ms
 10    54 ms    54 ms    54 ms
 11    52 ms    55 ms    53 ms
 12    59 ms    67 ms    55 ms  csr11-ve241.Sterling2dc3.cw.net [216.109.66.90]
 13    54 ms    52 ms    63 ms  216.109.84.162
 14    55 ms    54 ms    71 ms  v138.bas1-m.dcn.yahoo.com [216.109.120.142]
 15    51 ms    54 ms    52 ms  p1.www.dcn.yahoo.com [216.109.118.64]

Trace complete.
```

[redacted]

The first hop is the start. This should be your IP. The last Hop is usually the destination. Some times you will get a timeout which simply means the server did not respond in time. The "time to ping server" tell us how long it took the proxy to respond. If you see the proxy in one of the hops then it probably means that it is working. The only problem is that the proxy might be forwarding your IP to the server. I suggest you use both methods. If the proxy isn't shown in this method than it probably means that your settings arnt configured right and it isnt going through the proxy.

Proxy Chaining

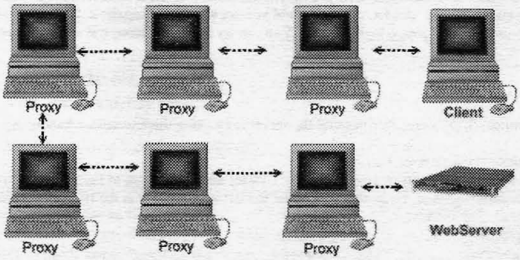
Proxy chaining is one of the more advanced proxy methods. In consits of linking more than one proxy together to provide you with extra protection.



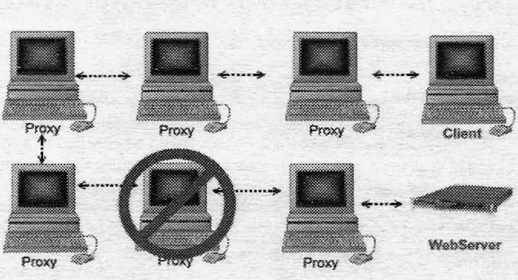
The above is an example of proxy chaining. As you can see there are two layers of proxies.

Client one is masked by proxy(190.100.1.1)
Proxy(190.100.1.1) is masked by proxy(160.100.1.1)
Proxy(160.100.1.1) requests the data from 168.1.1.1

This will provide you with extra protection. In fact if you would like to increase your protection you could link hundreds of proxies together. There is one problem with this, if one proxy goes down then your whole chain will collapse. Unfortunantly the only way to fix this is to go back and check every single proxy to see which one was the broken link. You could also use the tracert function to see which proxy was down. Then you would simply have to remove it from your chain.



Example of A Working Large Proxy Chain



Example of working chain that will simply not work at all
(Remember this. "A proxy chain is only as strong as the weakest link" *2)

As you can see in the above example that if one proxy die's the whole chain will no longer work. In LARGE proxy chains, finding the one proxy that has failed can be a long and tedious task.

Proxy chaining VIA Browser:

One way to proxy chain is simply in your browser. In fact there are actually two ways of using proxies in IE.

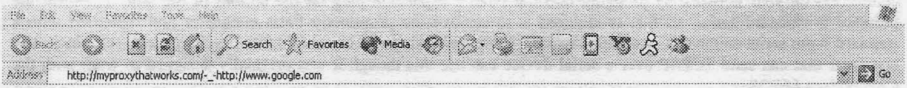
Proxy Chaining VIA HTTP Requests
Proxy Chaining VIA Proxy Configuration

Both ways are equally useful in different situations.

First we will cover Proxy Chaining VIA HTTP Requests. This consits of using the internet browsers address area to manually forward your request through a proxy. There is no configuration necessary within the browser option menu. All proxy setups are done directly into IE. This can be somewhat tedious since it can often take a long time getting everything typed out. Probably the best way to do it is to compile a list of proxies(WORKING) and then create a chain in notepad. Then simple copy and paste it before the URL. Below is a quick example of HTTP Request Chaining.

Option one:

http://myproxythatworks.com/-_-http://www.google.com



http://myproxythatworks.com/-_-http://www.google.com

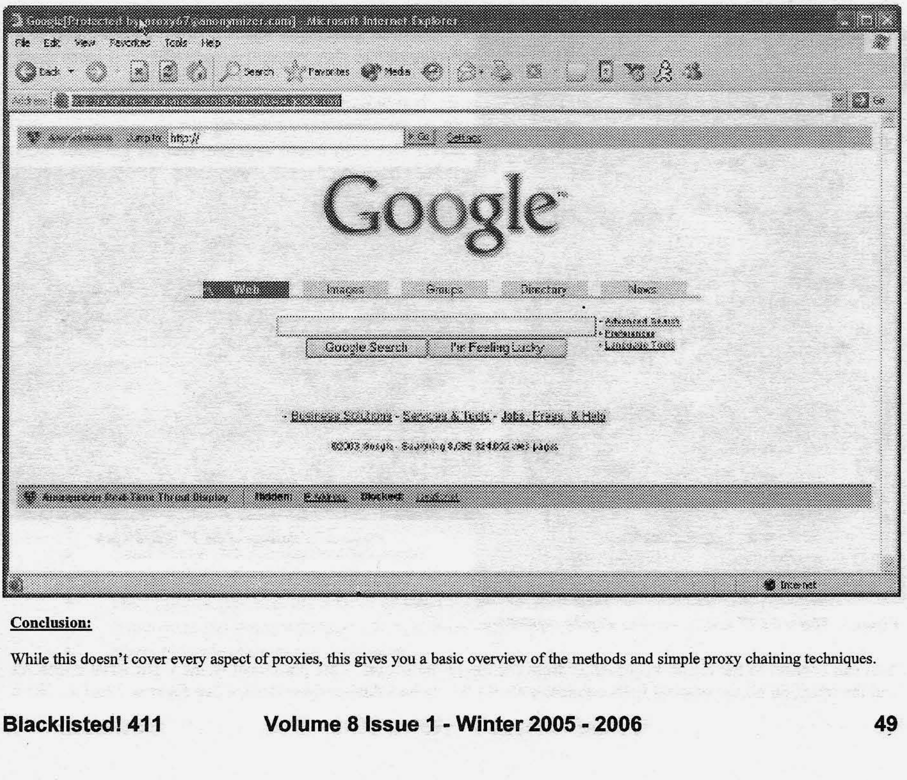
Option Two

http://ProXy:8000/http://MYProxy:8001/http://www.yahoo.com

This example above alows use to go through two proxies. It firsts starts out at ProXy running on port 8000. Then it goes to MYProxy running on port 8001 then it requests the page from yahoo.com.

http://anon.free.anonymizer.com:80/http://www.yahoo.com

That is a working example. Click on it and see what happens :)



Conclusion:

While this doesn't cover every aspect of proxies, this gives you a basic overview of the methods and simple proxy chaining techniques.

Inexpensive Ethernet for 8bit PC's

By TechWolf

Do you have an older 8 bit computer that you wish you could use online with your broadband connection? Do you have a bit of retro-computing nostalgia but wish you had a bit more functionality? Well, if it is capable of using a standard RS232 serial connection, and has a TCP/IP stack available for it, now you can, with a fairly cheap device and a little bit of soldering skills. If you're familiar with the Lantronix UDS-10, this is very similar.

The Device

The Palm Ethernet Hotsync Cradle, model 3C10149U is what we will be modifying. It can easily be found on Ebay by searching for "Palm Ethernet." This unit was designed to allow standard Palm PDA's access to an Ethernet connection on your network by plugging into the Palm's expansion plug on the bottom of the unit, and since the protocol is standard serial, all that is required is to remove the proprietary Palm connector and replace it with a standard 9-pin serial connector. As of this writing, Ebay had listings for ones at $3.99 up to $5.99 with shipping. Any computer that can send TCP/IP over a serial device can use this though it was originally designed to work with the Commodore 64/128.

Here's the connection list:

Palm cradle	db9 female
1	1,4,6
3	2
4	7
5	3
6	8
10	5

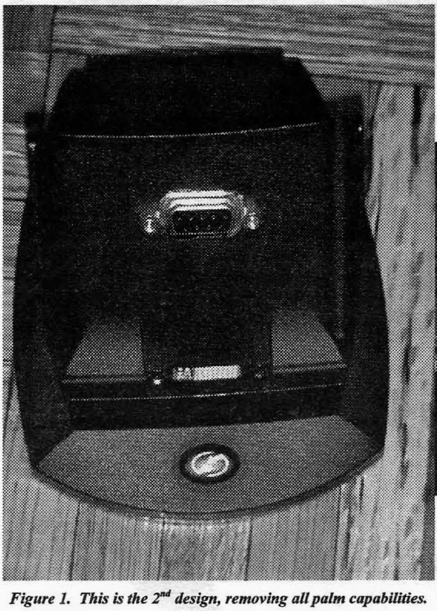


Figure 1. This is the 2nd design, removing all palm capabilities.

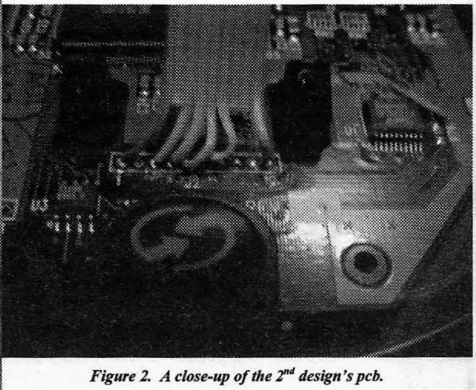


Figure 2. A close-up of the 2nd design's pcb.

You can connect to the circuit board either from the top or the bottom – the placement of the 9-pin serial connector and the retention of the original Palm connector allows this to be a dual-purpose design. *See Figures 3 and 4.* Use a

Dremel or other tools to cut a hole in your desired location for the 9-pin dsub serial connector. After the connector is mounted, simply screw the unit back together and proceed to testing.

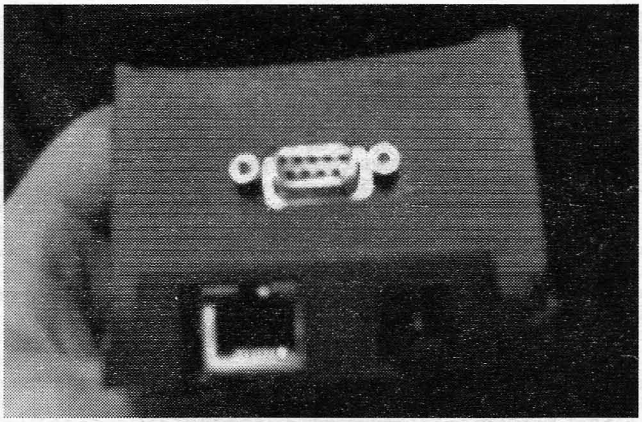


Figure 3. 9-pin in the back so the cradle can still be used with the palm.

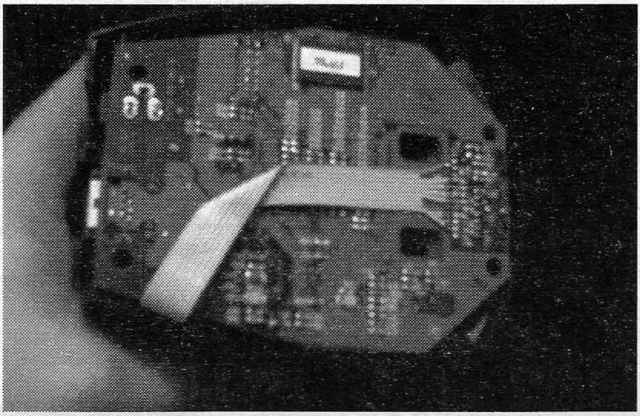


Figure 4. Connection soldered to the underside so the original palm connector is still available for use.

Using the Device

So you've finished constructing the device and you want to try it out. First, some basic information about the unit:

- The cradle is designed to use a standard 9pin male-female cable. Your Computer needs to have RS232 capability. For Commodore 64s, a user port serial adapter such as a Turbo232 or Swiftlink Cartridge is necessary. Also, plans are available online to make your own.
- The cradle does not support baud rates less than 19,200 BPS.
- At higher baud rates hardware flow control and a software FIFO are a must (in other words, if it doesn't work at 115,200 BPS, try a lower baud rate).
- The cradle does not handle PPP magic number negotiation correctly. If your PPP driver does, make sure this feature is turned off (Linux/BSD PPPD use a nomagic option). A sign of this may be that the link seems to be working fine but after a minute or so the link will drop.
- The cradle does not require any password authentication. If your PPP driver requires it, the cradle will accept any user ID and password combo. If it doesn't, a user ID of "Palm" and a password of "Palm" may be used.

Based on my experiences the green LED acts as a link light and will also pulse when there is network traffic. The amber LED appears to be a status indicator. It will flash while it's trying to request an address via DHCP and should go solid after a successful exchange. Otherwise the amber LED will just keep flashing. It's possible it could indicate other problems, however the DHCP logs should be checked for a problem first. The cradle's MAC address may be showing up in the log even if your router does not assign an IP address.

The Palm Ethernet cradle hack does have its limitations due to its nature and inexpensiveness. Most of the ports are locked down, and it is unlikely that you will be able to use this to run a server on your 8 bit computer. However, if you are primarily concerned with getting on the web, this device will serve that purpose. If you need to run a server on your 8-bit computer, I would suggest springing for the Lantronix UDS-10 or using a null-modem connection to bridge to a PC.

Currently, there are three major software packages for the Commodore 64 that work in conjunction with the Palm Ethernet cradle. They are: Wings, which is a Linux-like O/S replacement for the 64; the Wave, which is a graphical web browser for Wheels (an upgraded version of GEOS); and Novaterm (terminal emulation software). Caveat: Both Wings and the Wave require the use of CMD's SuperCPU accelerator. Using Wings with the Palm cradle can be problematic if you do not have instructions. Once you know how to do it, however, it is quite simple and can be automated with a startup script. To use in Wings:

- Run uart.drv (loads the serial driver and should automatically detect your user port serial cartridge)
- Run tcpip.drv (loads the software TCP/IP stack)
- Run PPP –d /dev/ser0 (runs PPP through the serial device)

After the last command, you should see some text; that is the PPP connection being negotiated. Once it's done, Wings is connected to the network and all networking commands *should* work. I have successfully used both the text-based and graphical-based IRC clients in Wings, as well as the telnet and ftp clients.

The Wave, the graphical web browser for the 64, includes its own TCP/IP stack and dialer software as part of the browser package, which allows us to use it with the Palm cradle. To use with the Wave:

- Start the Wave.
- Select Open/ISP Directory in the wave, then click "Add"
- Give your account a name – (I use "PPP access")
- Communication Method – Select "Null Modem"
- Select a login method – Leave it as "PAP Login"
- Your DNS Addresses – "My ISP assigns them" (If your router or network supplies DHCP – Otherwise select "I will enter them" and enter your network IP address.)
- Enter your Login Username: (This doesn't matter – enter anything you like, it's ignored)
- Enter your password: (see above. Use anything, it doesn't matter.)
- Confirm it: (type it again)

If that is your only entry in the ISP directory, you should be able to type in a web address and have it automatically connect you. I tested this with various web sites, including Google.com. Obviously, there are limitations to the graphical web browsing capabilities of the Wave, but more and more Commodore web sites are being written as "Wave friendly."

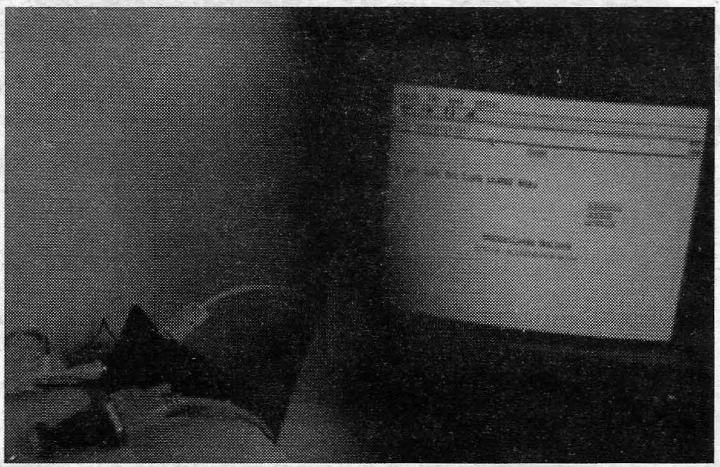


Figure 5. The cradle in action – filter used so the screen is visible.

Using with other computers

While it has not yet been tested, other computers that have serial capability and TCP/IP stacks should work with the Palm cradle. I plan on trying it out with my Amiga 2000 as soon as possible, and I should have very little problems adapting it to this use. I suspect that it could easily be used with early Apple or Atari computers as well, provided they also have serial and TCP/IP capabilities. However, my expertise is limited with those systems. I'd love to hear about successful tests with other computers!

Resources:

The Wave:
http://www.cmdrkey.com/cbm/wave/wave.html
Wings O/S:
http://wings.webhop.org/
Novaterm:
http://www.zimmers.net/anonftp/pub/cbm/c64/comm/Novaterm/
Home-brew Serial Port Cartridges for C=64:
http://jledger.proboards19.com/index.cgi?board=qlink&action=display&thread=1125678547
http://members.tripod.com/~ilkerf/chard/rs232c96.txt
http://members.cox.net/bbrindle/Qlink/easyc64rs232.jpg
SuperCPU Accelerator:
http://www.cmdrkey.com/cbm/supercpu/index.htm

The Palm Ethernet cradle idea was designed by JM with help of our friend EK. This documentation was created by me, with assistance from JM. This article is dedicated to JM & EK, without whom this device would not exist.

TechWolf has been using Commodore 64's for the past 18 years, since he was 10. He has been hacking since he got his first 1200 baud modem for the Commodore. TechWolf has his Associate's degree in computer science and is a member of one of the last Commodore 8-bit user's groups in the USA. He is an active collector of "antique" computer hardware and video games, and loves working with multi-media and hardware.

PORT KNOCKING SIMPLIFIED

by dual_parallel

Humans Really Can Learn

Humans learn in different ways. There are four ways, or styles, of learning. These styles are divided into auditory, visual, tactile and kinesthetic learning. This article is a demonstration of kinesthetic, or mechanical, learning.

Mechanical learning is not learning by rote. Here it means that one's most effective learning comes from doing. Not simply tactile examples, but hands-on hacking and perseverance.

Time to Learn

One day I chose to learn about port knocking. I'll spare you and omit what brought me there. I headed to portknocking.org, where probably everything I wanted to know about port knocking at the time resided. I read the front page. An immediate urge to create struck. So I struck out to create a simplified, if not hacked together, port knocking mechanism. Its creation taught me the basic concepts port knocking, and sharing the process and code with you, the reader, transfers that knowledge - as well as, hopefully, a little inspiration.

I gathered the tools needed to own this bit of knowledge. I adore Linux, so that was a given. I can get around in Perl. There's always a little bash, no matter what you do. The target service would be SSH.

I did have a need for something that would shut down SSH when not in use, and start it up on demand, reducing exposure. This hack was it. I wanted SSH to be exposed as little as possible, even in a home-broadband environment. There are a few users of this service and no major traffic. There are however many denizens of the Internet that are extremely curious about SSH.

At a 30,000 foot view, port knocking is the sending of connection attempts to certain closed ports in a certain order. When a set of requirements is met, the target service, for example, is activated. I do that here in a simpler manner.

Walk Through the Code

All code was authored on Red Hat Enterprise Linux (RHEL) 3. It was tested on RHEL 3 and 4. The code is immediately usable on any recent Fedora or RHEL-derivative distro, like CentOS or Scientific Linux. All scripts are placed in /root/bin.

The first thing I needed was a listener. To concentrate on the concepts of port knocking, I chose to use open ports and socat for the listener. socat is essentially netcat++. Plus I had never used it before. I decided to use some high ports that a standard nmap scan wouldn't hit: 59000, 59001, and 59002. A simple bash script called in /etc/rc.local would start three instances of socat and another script discussed later.

```
#!/bin/bash

# begin.sh

# Start socat listeners
/usr/bin/socat tcp-l:59000 localhost &
/usr/bin/socat tcp-l:59001 localhost &
/usr/bin/socat tcp-l:59002 localhost &

# Start socat_monitor
/root/bin/socat_monitor &
```

Each socat command starts a TCP listener, tcp-l, on the respective port of localhost. Upon a TCP connect, the listener simply dies. Perfect. Almost. I found Red Hat's firewall tool inadequate. A new iptables script took care of that. Here are the pertinent lines.

```
IPT="/sbin/iptables"
$IPT -A INPUT -p tcp -m state --state NEW --dport 22 -i eth0 -j ACCEPT
$IPT -A INPUT -p tcp -m state --state NEW --dport 59000 -i eth0 -j ACCEPT
$IPT -A INPUT -p tcp -m state --state NEW --dport 59001 -i eth0 -j ACCEPT
$IPT -A INPUT -p tcp -m state --state NEW --dport 59002 -i eth0 -j ACCEPT
```

The listeners were working, ports forwarded through a router. Now I had to monitor them. A Perl script, using the Watchdog::Process module, would work nicely.

```
#!/usr/bin/perl -w

# socat_monitor.pl
##################

# Include Watchdog
##################
use strict;
use Watchdog::Process;


# Define socat processes and
# create new Watchdog objects
#############################
my $name1    = "socat1";
my $pstring1 = '/usr/bin/socat tcp-l:59000 localhost';
my $proc1    = new Watchdog::Process($name1,$pstring1);

my $name2    = "socat2";
my $pstring2 = '/usr/bin/socat tcp-l:59001 localhost';
my $proc2    = new Watchdog::Process($name2,$pstring2);

my $name3    = "socat3";
my $pstring3 = '/usr/bin/socat tcp-l:59002 localhost';
my $proc3    = new Watchdog::Process($name3,$pstring3);


# Check on socats every minute and
# start sshd if they're down
##################################
while (1)
{
  if (! $proc1->is_alive && $proc2->is_alive && ! $proc3->is_alive)
  {
    system ("/usr/bin/killall socat");
    system ("/sbin/service sshd start");
    last;
  }
  elsif ($proc1->is_alive && $proc2->is_alive && $proc3->is_alive) { ; }
  else
  {
    sleep 300;
    system ("/root/bin/reset");
  }
  sleep 60;
}
```

socat_monitor checks on the three listeners every minute and starts sshd if the right combination is met. Here that is TCP connects to 59000 and 59002 within one minute. sshd is then started the next minute. Any other combination shuts everything down for five minutes. After that everything is reset with, well, reset.

```
#!/bin/bash

# reset.sh

# Restart socat listeners
/usr/bin/killall socat
/usr/bin/socat tcp-l:59000 localhost &
/usr/bin/socat tcp-l:59001 localhost &
/usr/bin/socat tcp-l:59002 localhost &
```

A major benefit of this exercise is to reduce SSH's exposure. I wanted SSH shut down if no one had logged in within one hour. So if someone had logged in at 7:50 PM, a script would see that when it checked at 8:00 PM and leave SSH on. At 9:00 PM the script would see that no one had logged in within the hour, shut down SSH and initiate the socats and socat_monitor. This script is sshd_monitor and it uses Watchdog::Process as well.

```
#!/usr/bin/perl -w

# sshd_monitor.pl
#################

# Include Delta_Days and Watchdog
##################################
use strict;
use Date::Calc qw (Delta_Days);
use Watchdog::Process;

# Declarations
##############
my @secure;
my @logins;
my $last_login_mon;
my $last_login_day;
my $last_login_hour;
my $mon_to_num;

# Define sshd and socat_monitor processes
# and create new Watchdog objects
########################################
my $name_ssh    = "sshd";
my $pstring_ssh = '/usr/sbin/sshd';
my $proc_ssh    = new Watchdog::Process($name_ssh,$pstring_ssh);

my $name_mon    = "socat_monitor";
my $pstring_mon = '/usr/bin/perl -w /root/bin/socat_monitor';
my $proc_mon    = new Watchdog::Process($name_mon,$pstring_mon);

# Get script run time
####################
(my $yr, my $mon, my $day, my $hour) = (localtime)[5, 4, 3, 2];
$yr  = $yr + 1900;
$mon = $mon + 1;

my @now = ($yr, $mon, $day);

# Open and slurp secure log
###########################
if (-s "/var/log/secure" > 0)
{
  open SECURE, "</var/log/secure" or die "Can't open log: $!";
  @secure = <SECURE>;
  close SECURE;
}
elsif (-s "/var/log/secure.1" > 0)
{
  open SECURE, "</var/log/secure.1" or die "Can't open log: $!";
  @secure = <SECURE>;
  close SECURE;
}
elsif (-s "/var/log/secure.2" > 0)
{
  open SECURE, "</var/log/secure.2" or die "Can't open log: $!";
  @secure = <SECURE>;
  close SECURE;
}
elsif (-s "/var/log/secure.3" > 0)
{
  open SECURE, "</var/log/secure.3" or die "Can't open log: $!";
  @secure = <SECURE>;
  close SECURE;
}
elsif (-s "/var/log/secure.4" > 0)
{
  open SECURE, "</var/log/secure.4" or die "Can't open log: $!";
  @secure = <SECURE>;
  close SECURE;
}
# Shut down everything if there are no logs
else
{
  system ("/sbin/service sshd stop");
  system ("/usr/bin/killall socat_monitor");
  system ("/usr/bin/killall socat");
  exit;
}


# Get time of last login
########################
foreach my $line (@secure)
{
  push (@logins, $line) if $line =~ /Accepted password/;
}

# Shut down sshd if there are no logins
unless (@logins)
{
  if ($proc_ssh->is_alive)
  {
    system ("/sbin/service sshd stop");
    system ("/root/bin/start_socat");
    exit;
  }
  if (! $proc_mon->is_alive)
  {
    system ("/root/bin/socat_monitor &");
  }
  exit;
}

my $last_login = pop (@logins);

if ($last_login =~ /(^\w{3})\s+(\d{1,2}) (\d\d):\d\d:\d\d/)
{
  $last_login_mon  = $1;
  $last_login_day  = $2;
  $last_login_hour = $3;
}

if    ($last_login_mon =~ /Jan/) { $mon_to_num = 1; }
elsif ($last_login_mon =~ /Feb/) { $mon_to_num = 2; }
elsif ($last_login_mon =~ /Mar/) { $mon_to_num = 3; }
elsif ($last_login_mon =~ /Apr/) { $mon_to_num = 4; }
elsif ($last_login_mon =~ /May/) { $mon_to_num = 5; }
elsif ($last_login_mon =~ /Jun/) { $mon_to_num = 6; }
elsif ($last_login_mon =~ /Jul/) { $mon_to_num = 7; }
elsif ($last_login_mon =~ /Aug/) { $mon_to_num = 8; }
elsif ($last_login_mon =~ /Sep/) { $mon_to_num = 9; }
elsif ($last_login_mon =~ /Oct/) { $mon_to_num = 10; }
elsif ($last_login_mon =~ /Nov/) { $mon_to_num = 11; }
else  { $mon_to_num = 12; }

my @then = ($yr, $mon_to_num, $last_login_day);


# Compare time of last login and stop
# sshd and start the socat listeners
# if no logins w/in the last hour
#####################################
my $diff = Delta_Days (@then, @now);
```

```
if ($diff >= 1)
{
  if ($proc_ssh->is_alive)
  {
    system ("/sbin/service sshd stop");
    system ("/root/bin/start_socat");
    exit;
  }
  if (! $proc_mon->is_alive)
  {
    system ("/root/bin/socat_monitor &");
  }
}
elsif ( ($hour - $last_login_hour) > 1 )
{
  if ($proc_ssh->is_alive)
  {
    system ("/sbin/service sshd stop");
    system ("/root/bin/start_socat");
    exit;
  }
  if (! $proc_mon->is_alive)
  {
    system ("/root/bin/socat_monitor &");
  }
}
```

From boot, begin is called in rc.local starting the socat listeners and socat_monitor. socat_monitor checks on each listener each minute and kills the remaining listener, starts sshd and exits if the right combination is met. It also locks up for five minutes and calls reset if the wrong combination is met.

sshd_monitor, called each hour by cron, looks for the running sshd process and shuts it down and calls start_socat if no one has logged in that last hour.

Lessons Learned

At first I didn't have a penalty for wrong or random connects, so I tacked on five minutes. Of course it doesn't mean much for the massive three-factorial combinations of this simple example. It does for more complex knocks.

Speaking of complex knocks, a bash script can automate knocking, making complex port connects simple. You can also provide such a script to users. GnuPG it up and send it off whenever you change the knock. For this example:

```
#!/bin/bash
/usr/kerberos/bin/telnet HOST 59000
/bin/sleep 1
/usr/kerberos/bin/telnet HOST 59002
```

Also, sshd_monitor does a little more than stated above. I oringinally didn't account for various processes dying unexpectedly. It now handles upkeep of the other associated processes.

I was well aware that there is no security through obscurity before writing this article. This is addressed beyond the front page of portknocking.org, and I do not, nor should you, count on this instance of port knocking, or any other, to secure a service. Although, even using open ports, the above port knocking implementation dramatically reduced the number of attacks upon the target service.

The most important lesson learned is that self-sufficiency is the penultimate of hacking. Hacking is not about buying the latest gadget. Nor is it using code you can't see, learning curtailed at the end of the clicks. It is the do-it- yourself attitude that is the ultimate pay-off to the hacker.

If you need or are intrigued by something, dive in. Especially if it's "beyond you." Determine how you learn best and extend the possibilities of your favorite certain technology. It is then you will extend yourself.

So many thanks to one of my best friends, bland_inquisitor.

DRM

By Ustler

Introduction

DRM, or Digital Rights Management is not new, but often confused by consumers with Content Protection. With current technology unable to "protect" copyrighted content the RIAA and MPAA have been scrambling to implement new technology to ensure their profits. In this article we will take a quick look at DRM technologies, weaknesses in HDCP and finally a look at audio watermarking and how it could infringe on free speech. As Walt Disney's board member Peter Lee says "If consumers even know there's a DRM, what it is, and how it works, we've already failed". Hopefully, with this article, we can show you the true problem with DRM.

What is DRM?

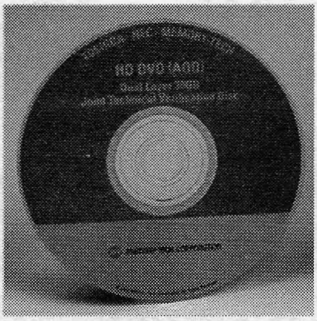
One of the most common misconceptions is that DRM is simply a means of copyright protection. Unlike past technology implemented to prevent piracy, newer DRM extends far beyond previous protection schemes and can easily be abused. A simple form of DRM is currently being implemented in today's DVD, and is known as Region Locking (Where a user was unable to play a DVD unless they had a DVD player with the proper region code). New DRM technology implements things such as blacklisting, strong hardware protection, and granular control over rights. For example, let's say I purchased a HD-DVD. First off, I would have to have a HD-DVD drive to play it and an operating system that supported it. I would also have to have a compatible Monitor, Motherboard and Video Card that supported HDCP (High-bandwidth Digital Content Protection). You may be wondering "What if I already have a monitor I like?". Well to bad, you're going to have to run out and purchase a new one in order to play your HD-DVD or "Premium Content". If the monitor doesn't support HDMI, then you will either get an extremely low resolution, or be presented with a black screen. So in this case, the HD-DVD would have a few rules.

1. Region encoded to play only on Region 1 HD-DVD players
2. Requires hardware capable of HDMI
3. Requires Hardware and Software capable of PVP-OPM
4. Checks hardware and software against a blacklist to weed out "Hackable" hardware/software.

If one of these conditions is not matched, the video won't play. But let's take a look at DRM as it applies to Music. In the case of protected audio, DRM would give the record company control over things such as: Ability to burn a CD, devices that are allowed to play the music, copy protection, etc.. For example, someone who purchases music but has an older MP3 player not supporting the DRM implemented would not be able to copy it onto the device. On top of that, even if they had a compatible MP3 player, they would be required to "update" the license every 5 days or so (Which would allow a record company to "Blacklist" a license or player if someone found a way to bypass protection). Of course, DRM is not all bad. If used currently, DRM offers businesses with a new level of protection. If a business where to implement a form of DRM on confidential documents, it could prevent an employee from copying it onto a removable media drive and selling or distributing it to competitors.

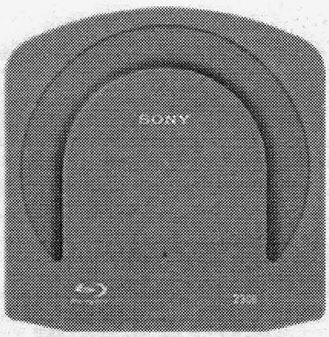
The media lineup

There are actually two forms of media to look forward to: Blu-Ray and HD-DVD. Both will be implemented.



HD-DVD

Pioneered by New Line Cinema, Paramount Pictures, Universal Studios and Warner Bros, HD-DVD has the capacity to hold 15GB on a single-layer disk, 30GB on a dual-layer disk, and 45 on a triple layer disk. The main advantage of HD-DVD is the backward compatibility for DVD. In this case, a HD-DVD player would be able to play both your DVDs and HD-DVDs all in one player. Cost of a player is relatively high and will range around 499 to 750, according to Wikipedia.



Blu-Ray

Blu-Ray is Sony's format, although multiple companies are supporting the technology. Unlike HD-DVD, Blu-Ray can offer 23.3 to 27 GB per a single layer disc. Multilayer disks are capable of up to eight layers making a single disk capable of holding 200 GB if all eight layers are used. Another neat feature that Blu-Ray has is a special polymer coating developed by TDK which prevents scratching. Evidence has been presented that the polymer coating is so effective, it can withstand attacks with screwdrivers. Backwards compatibility is optional and left up to the manufacturer of the drive. The cost of the player and the media is expected to be more than HD-DVD but the technology is far more expandable.

Technology – Operating System

Microsofts DRM Plans

Protected Video Path is expected to debut in Windows Vista (Longhorn) and was designed in order to satisfy the demands of content providers. Even though Microsoft developed it as a means to control content, we shouldn't blame them for the technology. If it wasn't for Microsoft, the content providers would be unwilling to allow their content to be played on any PC. PVP has two parts to it, "Output Protection Managment " (PVP-OPM) and "User Accessible Bus" (PVP-UAB). For audio, Microsoft has "Protected User Mode Audio" (PUMA). Before any of these is implemented, a Hardware Functionality Scan (HFS) is performed.

Hardware Functionality Scan (HFS)

HFS is a way of authenticating the graphics hardware to ensure that is indeed an actual device and that the manufacturer has met the standards required for premium content playback. In order to do this in a secure manner a question is presented to the device. This is chip specific and uses a seed value to prevent replay attacks. The question asked must be complex enough that any emulation software would be impractical. Microsoft also has the ability to revoke the signed driver if they believe it is leaking premium content for any reason. Depending on the vulnerability in the graphics card, Microsoft may choose to revoke the certificate permanently. If the flaw is hardware based the device may be unable to play premium content indefinitely. This presents a problem since purchasing new hardware may be required to play any form of HD-DVD or Blu-Ray content (Even though you purchased the correct equipment in the first place).

Protected Video Path – Output Protection Management

PVP-OPM is the technology that limits premium content to "Secure" outputs on the video card. Windows Vista does not provide applications the means to control video outputs, but rather uses a Media Interoperability Gateway (MIG). The Media Interoperability Gateway function is to provide policy interpretation that is included with premium content. If premium content has a policy requiring the use of "secure" outputs, MIG will require the outputs to be turned off before playing the content. Card manufacturers are required to provide device drivers capable of monitoring the status of output ports in order to prevent software or hardware modification that permits a user to activate a port once the premium content has begun playing. PVP-OPM is only part of Microsoft's plan in controlling playback.

Protected Video Path – User Accessible Bus

PVP-UAB is a way of preventing a "hacker" from sniffing data on the hardware level. In order to do this, an authentication sequence is performed between the system and the hardware. This is done in a few ways. First the video card is authenticated using a Hardware Functionality Scan (HFS). Then a session key is derived from the graphics card public key. This is used to encrypt data using 128 bit AES. Data is encrypted over the PCIe bus and is decrypted by the graphics card using hardware decryption. The only purpose of PVP-UAB is to prevent hardware sniffing of video data.

Protected User Mode Audio

Protected User Mode Audio (PUMA) is Microsoft's attempt at controlling audio. It is very similar to PVP, but only applies to audio

Of course the above information is very elementary and does not encompass all technical aspects of Microsoft's plan to implement strong DRM in there product. The obvious question for Linux fans is "What about linux?". Well currently it appears that Linux users will either need to purchase a HD/Blu-Ray DVD player, or resort to Windows Vista. Documentation describing premium content protection in Windows Vista is provided by Microsoft in a 45 page white paper at:

http://www.microsoft.com/whdc/device/stream/output_protect.mspx

Technology – Hardware

High-Bandwidth Data Content Protection (HDCP) is the technology that will be implemented in Blu-Ray and HD DVD players and Windows Vista. HDCP specifications are proprietary, but we do know that data is encrypted on the High-Definition Multi-media Interface (HDMI). Similar to PVP-OPM, HDCP requires devices to support HDMI and will refuse to output HD content to VGA and other devices that do not support encryption. A strict set of specifications is implemented for hardware manufacturers and the ability to "blacklist" devices is implemented. If a device is found to be leaking the premium content, newer HD and Blu-Ray discs will contain an updated blacklist preventing the player from playing its content. The problem with this is simple. If a method for obtaining keys is found (And one has already been found, but we will talk about this later), a hacker in a country that does not hold the same laws about copyright protection may decide to distribute the keys which will effect many innocent consumers. For example, a key from a HD-DVD player is cracked and the private key is derived and distributed on a anonymous publishing service such a Freenet. If the governing body of HDCP hears about it, it will be added to every new DVD released. This can force consumers to purchase new hardware since their old hardware is no longer working. Spending 1,000$ on a TV may be ok the first time, but once the key is compromised and revoked, the HD-DVD player will refuse to send anything to the device. This essentially will force you to purchase a new TV set in order to view HD-DVDs. Sure, hardware manufacturers might enjoy the prospects of returning customers, but will consumers really want to spend more money only to risk being forced to purchase new hardware again?

Of course, we haven't really talked about how HDCP really works yet. To make it quick and easy, HDCP is a proprietary technology that implements encryption from the DVD to the player and to the display. HDMI is the cable specifications used to transfer data from the DVD player to the TV. It can also be used to transfer data to something like your surround sound system.

HDCP Protection Broken?

Recently HDCP has come under much scrutiny. Since the Digital Millennium Copyright Act prevents the publication of research that could compromise copyright protection schemes, information about breaking HDCP keys are at best, rumors. What we do know is that noted cryptographer Niels Ferguson has claimed to be able to break HDCP in a reasonable amount of time. Since he often travels to the US for business, he fears that even though it may be legal in his country, the publication of a paper that shows the inherent flaw in HDCP may lead to his detention when visiting the states. Also, understand, this is not recent news. His original discovery occurred back in 2001, but even though he made claims, the media industry continued to put the technology into production. On November 19th of 2001, not long before Niels made his announcement about his discovery, a paper titled "A Cryptanalysis of the High-bandwidth Digital Content Protection System" was released by Scott Cosby, Ian Goldberg, Robert Johnson, Dawn Song and David Wagner. Scott Crosby says this after noticing his mistake of releasing the paper to the public

> *"What wrathful gods one can risk angering by a 20-minute straightforward application of 40-year-old math. For me, this was an accident, not a habit. Like other researchers, I do not want to be smited by angry gods, thus I do not expect to analyze any more such schemes as long as the DMCA exists in its current form."*
>
> *Scott Cosby*

According to his paper, the flaw he identified gives him the ability to:

- Eavesdrop on any data
- Clone any device with only their public key
- Avoid any blacklist on devices
- Create new device keyvectors.
- In aggregate, we can usurp the authority completely.

A fully copy of his research can be found at http://apache.dataloss.nl/~fred/www.nunce.org/hdcp/hdcp111901.htm. For obvious reasons, we won't attempt to explain the technical aspect or talk about what the flaw was.

Another supposed attack on HDCP was distributed by a copy called Spatz. While claims could not be confirmed, Spatz says that their product is capable of removing HDCP protection from video (Meaning removing encryption from the video signal and providing an unprotected output). How you might ask? Simply by taking HDCP chips out of HD Ready displays and forcing them to fool the DVD player into believing they are a legitimate device. Since HDCP relies on authentication of displays to ensure that it is compliant, an easy attack would be to modify hardware to get analog output. At some point, the TV must decrypt the signal in order to display it. If modification plans where to be released, a possible blacklisting of all devices vulnerable to such modification might occur. Furthermore, a possible blacklisting of all Spatz DVIMAGIC devices is possible in order to protect copyrighted material.

(More info at http://www.engadget.com/2005/07/21/the-clicker-hdcps-shiny-red-button/)

Watermarking Video, Will it really work?

Recently proposed Bill H.R. 4569 will require analog recording and conversion devices to detect watermarking. Just in case you don't know what watermarking is, its embedded data that is hidden but detectable with the right equipment. The proposed bill I'm referring to implements Video Encoded Invisible Light or VEIL. If passed, analog devices would be required to detect and prevent recording of video containing the Veil Rights Assertion Mark (VRAM). VRAM may seem like a practical decision when preventing digital tape recorders from pirating the latest box office hit, but Bill 4569 goes far beyond simple protection for movies. The purpose of this is to simply prevent you, as a consumer, from using a video camera or VHS recorder that might allow you to copy copyrighted content. This technology can be implemented in anything from your favorite television show to even audio. More importantly, television shows may be subject to the "No Copying" rule in an effort to force consumers to purchase the boxed DVD set.

The first implementations of VEIL existed in toys that allowed a consumer to "unlock" special features by watching the show and allowing the device to read the hidden data (Just some trivia info). The obvious question is, how does VEIL work and will it survive compression? The answer is unfortunately yes. VEIL does not actually change the video, but rather modifies the brightness of a picture in a certain pattern. For example, one frame from a certain video could be brighter than the next frame, which would signal a 1 to the device. The watermarking technology is cheap since its only measuring the intensity of what it's capturing. VEIL actually comes in two versions, VEIL-I and VEIL-II. VEIL-I is the earlier technology that was implemented in the toys that I reffered to earlier. VEIL-I is capable of transfer 120 bits per a second and changes the intensity of the entire frame. VEIL-II on the other hand is capable of transferring 7200 bits per second by using multiple lines to transfer data. The VEIL implemented in VRAM is VEIL-I since only very limited amount of data needs to be transferred in order to instruct the device to allow or disallow recording.

VRAM as a protection scheme is at best a hindrance for piracy. With the right equipment and hardware a hacker will be able to strip VRAM protection. In order to do this, the video is simply converted to digital format and run through a custom program that uses the same VEIL detection means implemented in chips. After identifying the pattern, the hacker can remove protection by normalizing the intensity on those frames. Furthermore, unless the government is willing to recall every video camera that is in the hands of consumers not containing VEIL detection, implementation in newer devices would be pointless. Claims about implementing the detection ability in consumer and high end video editing software may also be used to control "piracy". In this case stripping the protection before editing it may be necessary to prevent detection.

Please understand, I do not promote piracy in any form. I just feel that this technology will be abused to prevent consumers from rightfully making copies of television shows. If I want to make a tape of my favorite television show and edit it and save it on my computer, I should have every right to. Newer digital recorders will allow you to record television shows that permit copying, but will prevent analog output if required to. Furthermore, television shows may require you to record them in low quality in order to prevent "Piracy".

Watermarking Music

Watermarking music is also another possibility. Implementing some form of watermarking system that could be integrated into radio, CDs and more, is also very dangerous. Just imagine cell phones that won't record audio if music is playing in the background or high end video cameras that could detect both audio and video watermarking and refuse to record if it's present. Could the government implement such technology and then abuse it? Imagine having reporters unable to record because background audio is being played by law enforcement. Since Video and Audio watermarking is rather simple, the removal of such prevention methods would be very easy to implement. Of course the DMCA prevents any information from being published that might cause content protection to be removed. Since the DMCA only applies to the US, what will prevent other countries that don't have similar laws from allowing software and hardware development?

Final Words

Of course, artists have every right to receive money for there work. The problem is that the technology being implemented is being controlled by the same people receiving the profits. What prevents the media industry from enforcing DRM in such a strict way that it increases their profits while frustrating the consumer? If HD-DVD players are blacklisted, consumers have no other option but to purchase new hardware which gives the people who blacklisted the device in the first place more money for licensing fees. What will prevent the industry from purposely overlooking hardware flaws only to turn around and blacklist them once they are discovered? Furthermore, the DMCA only prevents flaws from being uncovered, it doesn't fix them! I wouldn't be surprised if devices where blacklisted every few years after a vulnerability was found that might allow piracy. Flaws in a system should not be protected by law. This would be similar to protecting weak encryption systems from having their vulnerabilities published. In general, DRM gives to much control to the entertainment industry and removes the ability for the consumer to use what they have rightfully purchased.

Hacking Before PC's:

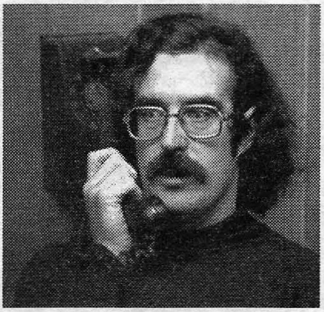
A Personal Recollection

By Grandpa Hackman

The technology junkies of today will have a hard time fathoming it. Once there were no home computers. You find yourself asking, "What did people do all night? Gaze at the constellations?" Nah, we still had TV, I'm not going that far back. We thought TV was content. We wondered "What did people do all night before TV?"

What was there to hack before new millennium tech and the veritable home computer came along? Hardware. Lots. There was once a lot of tech manufacturing going on in the USA. This was before companies thought about cheap labor in Mexico and other places. The stuff was mostly analog, but from the 60's onward came the digital walk of life. We kept hearing about pictures and text being shipped to our home computers. I thought to myself, "What? Why would I want that? I don't even have a home computer yet."

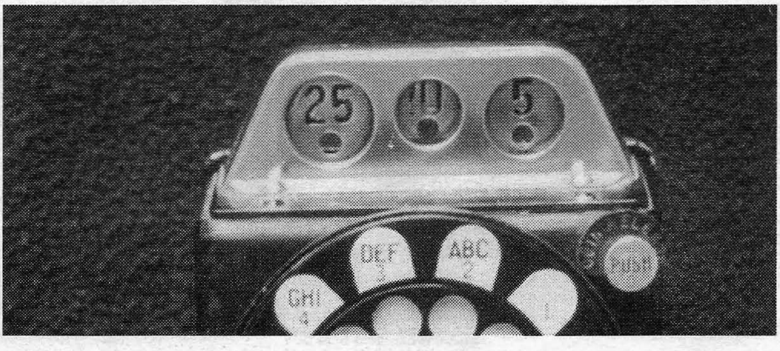
In the "wonder years" back in the sixties & seventies, a mind thirsty for tech understanding didn't have many other places to go other than electronics. Computers were around but nobody had one at home.



John Draper, aka Captain Crunch

One of the early beginnings of hacking was the Captain Crunch saga. Captain Crunch and his famous whistle. If it's before your time and you don't know the story, briefly he logged into "trunk level" on the telephone company phone lines with a whistle he got out of a cereal box. The "new" touch-tone control systems for Ma Bell's computers were wide open for such tom-foolery. Once at trunk level he was able to call anywhere and everywhere for free. He couldn't have cared less about the free calls, it was all about learning the ins and outs of the phone company computers. The technique was actually discovered by a blind phone phreak named Joe Engressia who had perfect pitch and could whistle the proper 2600 cycle tone himself. Captain Crunch added the just too cool whistle idea. And a lot of hassle for himself, like jail time.

But holes in the system like that are far & few between.



Old Bell System Pay Phone

When I was in high school we did an early form of phone phreaking. It was back in the day of the coin operated phones with the big holes up top to drop your coins in. 25 10 5 were imprinted in the back of these holes, remember? Sigh.

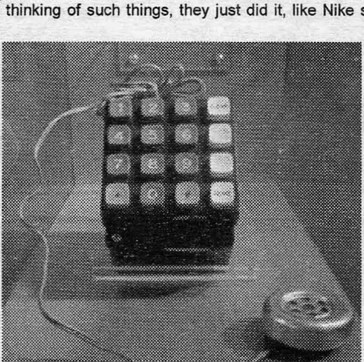
So anyhow, somehow we figured out that we could make the calls that cost everyone else back then a dime for one penny.

With a 5/16" strip of stiff paper stock about 10" long, hey, the back cover of the phone directory worked nicely. They supplied enough to make several penny calls from each phone book. You'd stick the cardboard jimmy down the nickel slot and drop your penny in it with the shim behind. Then slowly pull the cardboard out of the slot. Sometimes you'd blow it by pulling too fast and it'd cost two pennies. And ridicule from your buddies. I can tell this story now because the statute of limitations has expired and besides, I was a minor at the time. I didn't know what I was doing. I do feel especially bad about all of those unsightly phone book covers though. I doubt if I made over 10 one cent calls, so if Ma Bell wants to send me a bill for $.90 I'll cough up.

After the Captain Crunch news hit, phone phreaking became very popular with the hackers. Few if any really cared about the free phone calls, it was the fact that you COULD make free phone calls with a little bit of knowledge. They made blue boxes and red boxes. Then it got easier: they just tape recorded control tones on portable tape recorders. But the really clever hack was the Radio Shack dialer conversion. They'd take one of these little handheld gadgets that were designed to rapidly dial your contacts by pushing one or two buttons on the thing, literally a portable speed dialer in a box. Hey, this was high-tech stuff back then. If you were on the road and needed to make a call there was the phone booth with your speed dialer or nothing. The phreaks would change the clock frequency on the dialer slightly and presto, trunk level tones were produced by the keypads. I think it qualifies as hacking. And it's definitely a hardware hack. More evidence to support my thesis that hardware hacking is where the evolution of the modern day hacker began.

Steve Jobs, left and Steve Wozniac on the right

Another piece of evidence I would point out would be two old school hackers you've probably heard of. Wozniak and Jobs, the founders of Apple, were a couple of hackers from the era, well Wozniak at least. Weren't they just some hardware hackers? Sure. Many of us were thinking of such things, they just did it, like Nike says. I think Forrest Gump observed "Some fruit company."



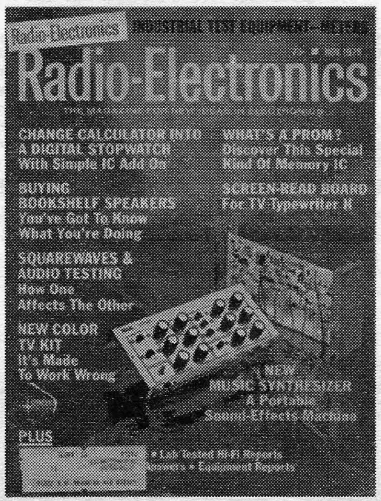
Steve Wozniac's blue box

Jobs was working at Atari as a technician. He and Wozniac attended the "Homebrew Computer Club" together. When the Captain Crunch news hit, these two fellows started making blue boxes. Of course, it wasn't long before Ma Bell put the damper on all the fun and just like today, try and use something like that and the phone police will be there shortly.

Jobs took on an assignment from Atari reducing chip count on a PC board for the "Breakout" video game. Now, the truth of the story is that Jobs had no real interest in circuit design. So he got together with Wozniac and contracted with him to do the design. Atari had offered to give $100 for each chip that was reduced from the board. Wozniac reduced the chips on that board by 50, that's 5000 bucks. Skullduggery was afoot however, and Jobs told Wozniac that Atari didn't give him the $5000 that was promised (even though they did) and forced Wozniac to accept $300 for his labor. Wozniac later found out and as you might guess, their friendship suffered greatly.

A year or two later Wozniac created the 1st Apple in Jobs' garage. A year after that came the Apple II and they were launched into the stratosphere. In just a few short years they were a publicly traded corporation on the NYSE.

You've probably heard the Apple story many times. I'm referring to it with regards to a hacker context. Without these types of out-of-the-box hackers, progress would take much longer if it happened at all. Fortunately for all of us, these types have been and will always be there, pushing the boundaries, regardless of the sophistication of the technology surrounding them. If we lived in the imaginary Bedrock of Fred Flintstone fame, the hackers would still be there, fixing and making things with rocks and pterodactyls. From phone phreaking to PC's to IPODs, it's still the hardware hackers that actually make the hard-core physical reality base that the software-only hackers can only dream about having.


Radio-Electronics
INDUSTRIAL TEST EQUIPMENT—METERS
Radio-Electronics
CHANGE CALCULATOR INTO A DIGITAL STOPWATCH With Simple IC Add On
WHAT'S A PROM? Discover This Special Kind Of Memory IC
BUYING BOOKSHELF SPEAKERS You've Got To Know What You're Doing
SCREEN-READ BOARD For TV Typewriter II
SQUAREWAVES & AUDIO TESTING How One Affects The Other
NEW COLOR TV KIT It's Made To Work Wrong
NEW MUSIC SYNTHESIZER A Portable Sound-Effects Machine
PLUS
Lab Tested Hi-Fi Reports
Equipment Reports

An example of an electronics technology magazine of the era

In those days before the net, the hard-core hackers kept in touch with the goings-on through trade magazines and electronics magazines. They had writers such as Don Lancaster covering the new wave stuff happening. Don wrote a couple of great books that I read, Cheap Video and Son of Cheap Video. They were about (gasp!) getting video output out of a computer - cheaply. Back in those days video was very difficult to get out of a computer, there was no just buy an AGP card & plug it in. Most home computers output data in binary, a row of lights that represented a binary number. Yikes! I have a hard enough time balancing my checkbook.

Don Lancaster is still _very active (and outspoken!) in the electronics/tech/many fields. He's all over Usenet, yahoo groups, etc.

Probably not much known to those outside of the industry, in the early 70's there was a lot of hardware hacking going on in the musical instrument field. To a musician of this era an amplifier was not what the proverbial golden eared audiophile sought, a clean, uncolored reproducer of sound waves. The guitar players of the day (and it was all about guitar players then) viewed their amp as an instrument, part of the coloring of their sound. The favorites were the class AB push-pull tube amps, if you know what that is, it was a very common amplifier design. They weren't the cleanest amplifier. But they were sweet sounding just the same, with their own flavor that's good even if a little distortion creeps in.

Way back to rockabilly times, like the "King", Elvis, the guitar boys were cranking those class AB's up into the distortion range to get "that sound." It wasn't long before the bread & butter local club players wanted to get that sound without the 747 equivalent decibel level ear damage the customers were complaining about. So in came the hackers, everywhere. Hackers all across the world were tweaking those tubes to make them scream, with better control of volume. Although the starving musician is more often than not a reality, they found the money to get their amps "walked on" to get the sound they wanted.

It took a special kind of hacker to trick out those old amps. You had to understand tube theory, which was a bit odd for a young electronics enthusiast such as myself. This was a time when transistors were just taking over the reins from tubes on most fronts. Most electronics oriented people wanted to know less about tubes and more about the new solid-state that was taking over. Before you knew it, those new-fangled IC things were coming out.

Because of the huge music boom of the mid-sixties to the mid-seventies, every electron path in that musical instrument chain, from guitar string to speaker was scrutinized and tinkered with.

That's what it was about before the "home computer" became commonplace. Hardware was what tech was made of. A lot of this same hardware is now traded amongst collectors. Many things are going digital, never to look back.

I don't mean to give the impression that I have something against that. If I can write a little code and have a computer take the place of the time-consuming process of design and production of a hardware device, I'll do it every time. But I'm still ready to pull out the soldering iron if I have to, to create something that I need if I can't get it any other way.

Another major contribution to the early hacking scene was made by the bulletin board crowd. That was the closest thing that most people had to the web in those days. Some boards were very specific, with specialized information and clientele. Some were warez BBS's and porno boards. Hey, sounds familiar doesn't it?

The inventors of the bulletin board were Ward Christensen and Randy Suess. They lived in Chicago where it was cold with tons of snow every winter. They spent the winter of 1977-78 coming up with the Computerized Bulletin Board System (CBBS). The next year they released it to the public and it was the 1st Bulletin Board System. This software made a computer react in a similar manner as a server today, serving out information, files, whatever to those that were subscribed to the Board. There weren't any point and click buttons, everything was done via text commands ala the command line. It was similar to telnet today, in fact a lot of nostalgic folks still run and access Bulletin Boards on telnet today.

The only modems available were 300 baud. If you don't know how slow that is, you can't imagine. Today's dialup is hundreds of times faster. I can still remember downloading my first 1 MB file. It only took a little over an hour at 1200 baud. Many folks ran bulletin boards from their home back in the eighties and it was the beginning of everyone being connected. Before that, some geeks were hooked up via modem between themselves. Other even more mainstream type of people were on Compuserve and Genie, like a dial-in AOL sort of network. Not much different than today, stock quotes and recipe exchanges but ALL text based, no pictures. However it was a tiny fraction of the people online today. The bulletin boards really spread the concept of connectedness. Most were free or inexpensive and the typical BBSer, as they were called, would stay up all night "hitting the boards." Email began to flow. It wasn't long before Bulletin Boards became social organizations, having meetings and the like, far beyond the original concept of file and information sharing.

An excellent web link that really gives you the feel for the old bulletin boards of that era can be found at: http://www.apocprod.com/Video/bbs_sim.mov.

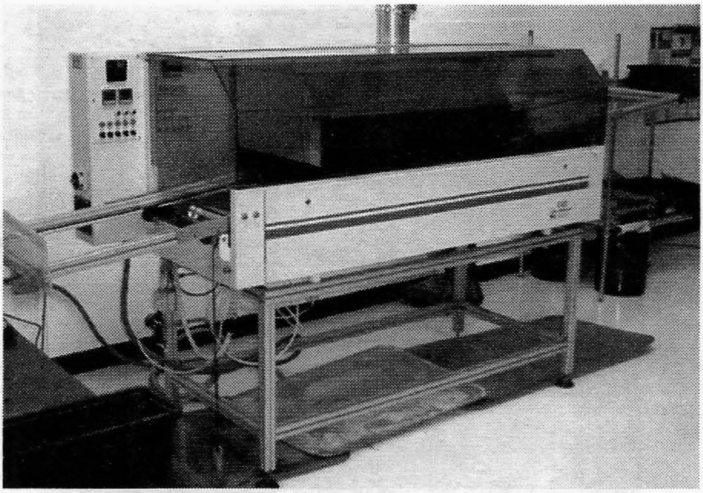
CBBS was morphed into ever more sophisticated versions and competing programs came along as well. Once again the hacker progression is at work. I can imagine this result, this similar item comes close, I'll modify it to get my desired result.

The best selling computer of all time

In the early eighties I was commissioned to make a computer controlled kiln for a company doing ceramic work. You could buy the things, but at the time they were $7000. This was a small company that suddenly found itself with a very large contract. The future looked bright, but the cash on hand was grim. I found a kiln of proper size for $1500. I purchased a Commodore 64 for about $298 and purchased some components for another $100. When I was done, we had a computer-controlled kiln that did everything the "official" one did, except drain your pocketbook.

The Commodore had input and output ports which I could read and control from software. I simply homemade an A/D converter and fed a thermocouple to it. The thermocouple produced a voltage corresponding to the temperature in the kiln. The A/D converter fed this data to the computer. I wrote a very simple basic program that looked at the temperature coming in from the A/D converter at intervals. On the output port of the Commodore I connected a homemade electronic power switch using a triac, the main component in a light dimmer. The basic program could then control the temperature of the kiln by turning the heating coils on and off. It worked great. There were no modifications to the Commodore, it was ready to do the job right out of the box.

This kind of task was par for the course in electronics work in those days. Another company I did some work for wanted a flow solder machine for a fair sized production line. As usual, they didn't have the money to buy a new $20-30,000 machine. We found an old one that had been owned by the U.S. Navy of all things for $1000. The machine itself would have lasted just about forever, but the controls and electronics from the early fifties were on their last legs. Rip, rip, then install new high tech temp controller and thermocouple for $500, good to go for another 25 years.



A typical flow solder machine. It would solder all joints on the pc board at one time, drastically reducing labor costs

I know that flow solder machine worked for at least another seven years, probably much longer. They got a deal out of it, it only took a day or two of messing with the machine to get it right.

As time went by, more and more manufacturing of electronic goods in the US went to overseas manufacture. It started in the early seventies and by the late seventies everyone everywhere in electronics could feel the pinch.

The electronic jobs became scarcer. There were niche industries, such as aviation radios, which had a good political lobby. They were required to be manufactured and serviced domestically. The video game industry took off in the mid-seventies, I completely missed that myself. Then there's always the government/education areas that employ electronic technicians. The government stuff could be especially interesting.

I worked at Fort Irwin where they still do the "laser tag" mock battles to train the army. It was thrown together like the Apple, no kidding. In the early eighties, someone convinced the top brass that laser tag battles and filmed and edited multimedia of these mock battles was the way to go and the National Training Center was born and thrown together almost overnight. Some of the equipment was so leading edge that it really looked as though someone in a garage had hand-assembled it, in fact I'm sure much of it was born that way. Often, you'd open an enclosure and inside would be several off the shelf items "kludged" together inside, mounted somehow, with fancy cables connecting it all up. One device I remember in particular had a handmade perf board assembly and we had no schematic for it. The technician that designed and installed it had a beef with the company and left, leaving us holding the bag. It was intricate too, and the $30,000 device that was broken depended on it to work. About 12" x 12" and chock full of IC's. That's the kind of hacker stuff I'd rather avoid.

The hacking was part of the operation though. Often these kludged together assemblies weren't designed properly to begin with, or were designed with lousy life cycles so that they were literally falling apart. Your Army depended on these training devices. So we made them work, whatever it took. Baling wire and duct tape wouldn't have been out of the question had they done the job, although I can't remember using either. But there were homemade patches galore, I did a lot of them. It's a nice luxury to simply make a phone call and have a new part delivered the next morning. In the real world, it just doesn't always happen.

One of the bright spots in my memory was that in spite of the demise of electronics jobs in the U.S. the surplus market thrived. You could get things that cost hundreds of dollars originally for a song. Experimentation was cheap, entertaining and sure beat the push content available at that time on the boob tube. At this time too come to think of it.

There are many "histories of hacking" available on the web. They all seem to go over the same material, the phreaking, the Apple story, etc. But those of us involved in technology at the time watching all of this go down perhaps had a bit of a different perspective. These are my recollections, not some encyclopedic history of hacking. An attempt to convey to you, the reader, the interpretations, the concepts and what they meant to me. Often my interpretations were incorrect, still they were my interpretations.

For example, the accomplishments in Jobs' garage weren't all that spectacular to me at the time. Not to minimize their accomplishment. It was just that I wanted to do the same thing and I know many others did too. I never found the money to throw something like that together at the time. Whatever the excuse, they did it.

My direction was with the progression of it all. I was trying to check out the whole forest, not a close up of the trees. Computers were coming, there was no doubt. It was something totally new like the automobile had been half a century earlier. Many people had the skill to design one in their garage, it was simply a question of cost and that wasn't cheap in those days. In my mind, the application, the melding of this new technology in new ways never possible before were much more exciting than the computers themselves. In essence, a very important missing link in robots was upon us, the "brain." I knew, and history bears out, that automated factory processes would utilize this new technology very soon to cut costs.

A typical plastic injection molding machine

An example of an industrial process I got involved in was a molding machine monitor. Molding machines suck a lot of electricity and everyone, in those days at least, financed each machine up to it ears. So the companies wanted them to operate 24 hours a day, 365 days a year. It was difficult for them to keep tabs on each machine in a large facility. The computer revolution to the rescue.

I built an S-100 bus computer from scratch almost as you would a PC these days. In those days the motherboard was simply a highway of wires (traces) that connected each card to the system. The CPU came on a card by itself. The RAM was on another card. The input/output functions on another.

This tireless robot brain would watch each and every machine throughout their mundane work cycle, keeping log of key important facts. Then the supervisory personnel in the office knew as much about the molding machines as if they were spending time on the production floor, rather than in the nice air conditioned offices with the coffee machine.

These were and are the applications that cause huge shifts in the order of business.

But you must be able to think out of the box. It seems that nowadays people just arbitrarily order a new widget when they need a repair. While that's fine and accepted by many as the best method, it doesn't give any experience for what to do when a part is not available for whatever reason, and that still happens all the time. And more importantly, the out-of-the-box thinking process is stifled. Without the brain exercise that naturally occurs with such tasks, I fear we might be letting our hacker side get flabby.

BLACKLISTED! 411 WANTS YOUR INPUT

We want to hear from our readers and get some input on every topic from the articles we print to the content on our website. If you have any ideas, comments, complaints or suggestions, the best way to get something done about it is to contact us and let us know what you're thinking. We are a magazine written for the hacker community. We want to have the best possible magazine with the most fresh ideas and subject matter. This is your chance to help out and get something done. Don't fall prey to the thought, "what I think won't matter" or "let someone else do it." You can make a difference!

We want to hear from hackers, event coordinators, group leaders, graphic artists, writers, creative assistants, magazine editors, system administrators, forum moderators, webmasters, photographers, electronic hobbyists, design engineers, technical writers, field technicians and anyone else who is interested in the hacker community in any way. Here's how to contact us:

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

Or make contact with us through our website:

WWW.BLACKLISTED411.NET

SUBTERFUGE

How Attackers Cover Their Tracks

By Dr. Fibes

The thing that makes an intrusion so unnerving is the arcane way in which an attacker will find you. It really doesn't have a lot to do with you, he's just looking and you happen to fall through the sieve. Because of this you have no warning beforehand and no indication afterwards. Unless you have a savvy administrator that can be everywhere at once, if you get targeted you will never even know it. And there is no way your administrator can be everywhere at once, 24/7/365.

He pings and probes hundreds of thousands of computers and yours got on the list. How would you even know?

Well, if you are running a server there are logs that keep track of all entries. Your administrator can look in the logs to find the suspicious culprit.

That's exactly where he'll hide his existence. He can't very well leave a digital record back to his IP address. So he'll delete his entries off of the log to leave not the slightest trace of his visit.

It all sounds so easy. But it is much more involved than that. There is a general five step process that an attacker would commonly use:

1. Gathering Data: He will try to learn as much information about your server machine and your organization as he can. He will be on the lookout for vulnerabilities and weaknesses.

2. Exploitation: If he finds vulnerabilities he will attempt to use an exploit against them. He is attempting to get the most bang for the buck: the most powerfully useable vulnerability with the least amount of hassle and the most minimal possibility of being caught.

3. Gain Administrative Privileges: Many times an exploit will only grant the hacker limited privileges. To cover his tracks and install a rootkit, he must get higher privileges.

4. Cover Tracks and Install Tools: Once he has completed step 3 he will be pretty anxious to install tools that will help in easier entry next time and other niceties. He will also want to destroy any sign that the system has been hacked, lessening the possibility that he will be traced. And also providing more time to gather sensitive information, the next step.

5. Gather Sensitive Information: This is what he came for. Username/passwords, Email addresses, home and business addresses and phone lists. Company secrets, upcoming transactions.

He can do all of the above steps without the administrator or anyone else realizing that he has even been there.

He has to gain entry into the server. If you were a company, he might do this by researching things such as mapping out your company's IP block using whois and DNS lookups.

Next he might do a ping sweep. He simply sends a packet of data to a range of ports on the entire IP block and logs the computers that respond. These have open ports. Any open port to the outside world is a security risk. If you have many, there's a good chance he can get through one of them.

In order for the ports to work for the services that utilize them they have to respond when queried. In the header returned by them from this query, the attacker can glean information such as the service running on that port, version number of the software, and possibly other tidbits of data. Many of these services have been compromised and if he finds one of those running it is his gateway in.

Through further communications with these vulnerable machines, he can guess with reasonable certainty which operating system is being used. He needs to know this to decide which method of attack to try. All of the operating systems have their own set of flaws.

The next step would be to try an exploit if he can find a weakness. There are "push button" programs available that take advantage of certain 3rd party programs that run on open ports. And of course, there are a number of other possibilities that he could try as well.

Once he gets in the most important goal at that point is to gain administrative control of the server. That will give him the keys to the kingdom. He can install programs such as keystroke loggers to see if the IT folks are on to him, gather passwords, etc. He can add users. To do this he must escalate his privileges. Often when he manages to get in he has only limited privileges.

He'll try to download the system password file and crack it. It's only a matter of time if he can download the password file.

He may try to install password sniffers and search for passwords that are being sent in cleartext. People typically use the same password in many places so if he can get an unencrypted password in a low-security situation, that same password may serve him well in a high security situation.

If these two methods don't work he will try known exploits with his background knowledge of the operating system involved.

If he's able to get administrative privileges he'll install a backdoor so that he can come back any time he wants. Also a key logger. Usually rather than installing several separate programs he'll install a rootkit which will install them all at once.

The key logger application is important to him, because by reviewing it he can determine if the administrator is on to him. And of course it's another easy way to pick up passwords.

Besides the backdoor and key logger, the rootkit will install Trojans to replace applications, such as the login application. This is another convenient way to gather username/password pairs. There won't be any hint that this login is any different, so this all occurs invisibly.

It will also infect the startup files to insure that things like the backdoor are always running.

It is possible to recover from a rootkit intrusion. There are many tools that can detect and remove rootkits. Then the system will be free of backdoors and other mischief.

There are a number of websites that specialize in these tools, a good search engine will find them instantly.

There are Intrusion Detection Systems (IDS) that attempt to recognize an attacker attempt before he can compromise the system. They also do such things as watch for suspicious activity and attempts to crack passwords. They also watch for port scanning attempts or new applications using an unusually large amount of memory. There are several other methods they usually watch for as well.

If your company is not running an IDS it might be a good idea to start using one. You can't stop the determined attacker, but at least you can raise the bar to a level where none but the best can get in.

It's important to keep in mind that one compromised machine will risk the entire company. A simple chat program running on a clerk's computer can sink the whole affair. So vigilance and education are key.

Another security measure worth the effort is to download a vulnerability scanner. These "hacker-in-a-box" type programs are excellent at demonstrating weaknesses in your system. The attackers themselves use them, so why shouldn't you have the same weapons available to shore things up?

These will also find things like vulnerable scripts and helper programs that are known by the attacker and used to assist him in his deeds. It will also find malicious java applets.

WinUAE: Your Amiga on x86

Yearning for the days of yesteryear? Well, yearn no more!

by MobbyG

Thanks to some very cool coders, the fun and coolness of the Amiga, is now able to be brought to the desktop of the average PC user. Some like to play, some are curious, others actually get work done! Whatever your interest in Amiga is, this will help you get an emulated one running on your PC desktop. First things first of course. You need the software!

NOTE: This article assumes you know some basic Amiga operation. If not, There are online resources available to learn the basics of Amiga DOS. Google is our friend!

You can find WinUAE, which is the windows version of UAE (Ultimate Amiga Emulator), at *http://www.winuae.net*. The current version posted as of this writing is 1.1.10, and is the version I currently am using on my personal PC. Aside from the WinUAE program, which is free, you're going to need ROMs for the Amiga. Now, we all know, if you look hard enough, you'll find pirated ones on the net somewhere. It's not like I can stop you from finding them and using them . But I would ask that if you are an Amiga fan, and I would assume you are since you're reading this, that you please support the Amiga community by not using pirated ROMs. Buy some or use the ones on your classic Amiga.

Now, if you're going to buy ROMs, then you can skip this part, but if you plan on using the ROMs in your Classic Amiga, then read on! Included in the WinUAE archive, are a couple programs that are really handy! They're transrom and transdisk. Transrom allows you to make an image from your Classic Amiga's Kickstart ROMs. Tansdisk allows you make make images of any floppy disk in DF0:. So get out your AmigaOS floppies, and have them handy and boot your Classic Amiga. Copy transdisk and transrom to an old PC Double Density (720K) floppy you may have lying around, and pop it into your Amiga's floppy drive. Don't have one? Then grab a High Density (1.44M) and cover the non-tabbed side of the disk. Format as a Double Density and viola'! Use CrossDos to copy transrom and transdisk to a drawer on your Amiga Hard drive. If you have your Amiga online, then go ahead and download WinUAE on your Amiga and unzip it and copy those programs to a drawer somewhere.

We'll do the ROMs first. Open a Shell...

Go to the drawer on your Amiga's hard drive where you copied the transrom and transdisk programs, and type the following command into the shell...

```
transrom ram:kick.rom
```

This will have transrom create an image of your ROM(s) that is in your Amiga and create a file in your ram drive, called kick.rom. Copy this file to floppy and then place it in the Roms folder in the WinUAE directory on your PC. If there isn't a folder created, go ahead and make one.

Now you need your Amiga OS. So take your Workbench floppy and place it in your DF0: and type...

```
transdisk ram:wb.adf
```

This will create a 900K image of your Workbench Floppy in your ram drive. Now, if you're using 720K floppies, you're probably wondering how to get a 900K file on a 720K floppy. Best thing I can say, is use LHA and compress the hell out of it. You should be able to get it down to about 300K. Repeat this for all the Amiga OS disks. Remember to give each one a different name or you'll just write over the file. Copy them to your PC and you're set!

Next we want to configure WinUAE. So install if you haven't done so yet and start it up. First thing we wanna do is go to ROMs and setup where WinUAE should look for ROMs. Now when you installed it, ROMfind should have searched any ROMs on your computer. If it didn't find any, you'll still need to tell it where they are. If it did, just double check that is has the correct path. Then we need to tell WinUAE where the images of the floppies are. So click on Floppies and click the "EJECT" button if something is in there and then put in the path to the Workbench floppy in DF0:

Next we setup some RAM. Click on RAM and for chip RAM, let's stay with 1Meg. Fast Ram set to about 8Megs. The Amiga OS needs very little for a simple configuration.

Go to display and set the window size to what you would like. I would suggest the default 800x600 for now. You can experiment later, but the purpose of this article is to get you up and running so you can as quickly as possible to play around.

Now go to Configurations, give it a name and save it. Then click OK, and the next thing you see should be a window with the Amiga Workbench running. Now this is a simple setup. You can create a hard drive image and install the OS on that within WinUAE and then boot from that hard image. To do that just quit out of the emulator and go back into the configs and to harddrives. At the bottom you'll see a greyed button for create, with a box asking for a number of megabytes. Just type in how big a hard drive you want and click "CREATE".

NOTE: This will create a file the size of the hard drive you want. So if you put in 200 Megs, it will create a blank 200 meg file! Amigas can run on hard drives as little as 20 megs and still have plenty of room. They get a touch cramped if you wanna do big things, but you can always add more hardfiles or create a bigger one. Remember, that the hard files are just like hard drives and that the Amiga OS can only handle hard drive sizes up to 2 gigs with some degree of reliability. Mathematically you can do just shy of 4gigs, but keep the hard files as small as you can for your purposes. This will save space on your physical hard drive.

Now you can use Windows folders as Harddrives. This makes it easier to add files to the emulated Amiga, but to me seems to slow things down. It's a personal preference.

To install the OS on your new hard file, simply go to floppies and "EJECT" the Workbench floppy and put in the Install Floppy and start your emulator. When booted, you should see the install floppy, the Ram Disk and an icon that says NDO: NODOS. That is your unformatted hard drive. Left click it once to select it, hold down your right mouse button and go to icons and select Format Disk. I prefer using FFS (Fast File System) and having a Trashcan on my dirve, but you can do what your like. Name your volume something, and click format. When down, you will have a hard drive ready to have Amiga OS installed on it.

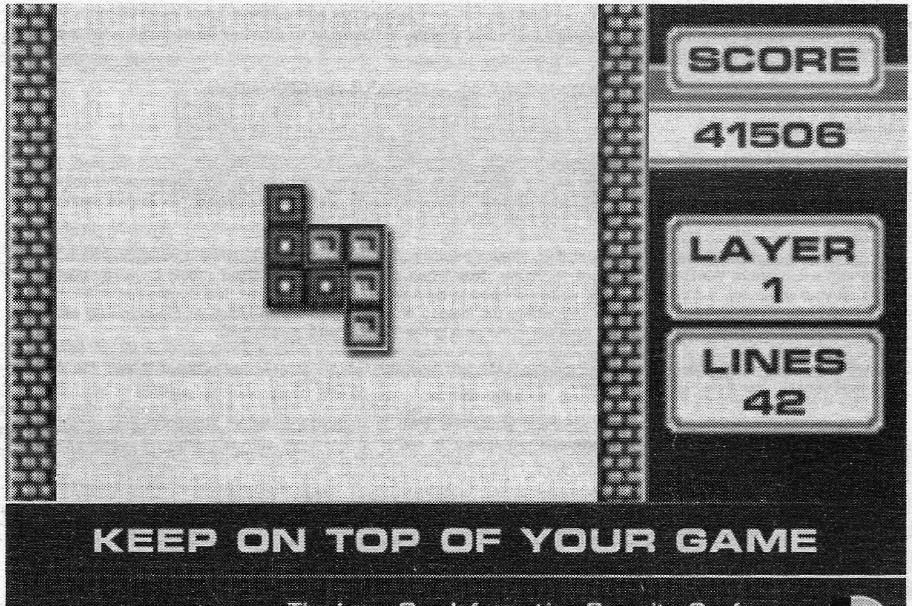
Now double click the install icon and go into the install drawer and choose the install language. From there simply follow the prompts to install the OS. When you get a requester asking for you to install a different disk, hit your F12 key to bring up the WinUAE control panel and go to floppies. In DF1: put in the path to floppy being requested and click OK. The installer will detect the disk change and will continue the install. Repeat the floppy swapping when asked. When done, just "EJECT" the disks and reboot! You should now have a fully working Amiga on your x86 machine! From there, you can tweak to your heart's delight!

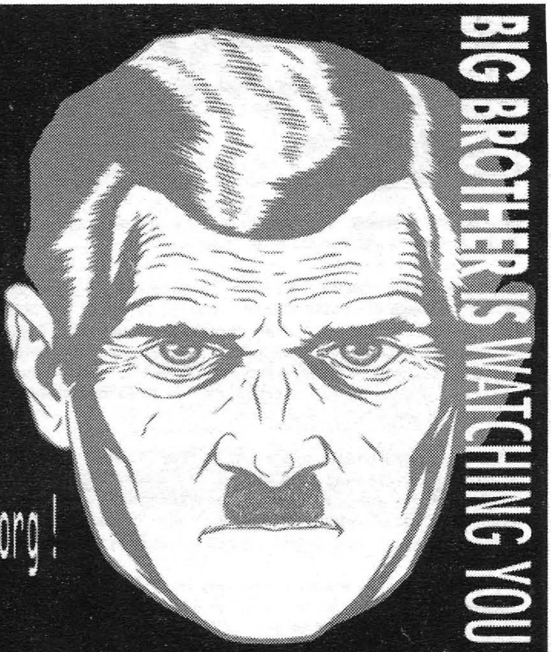
TIPS:

- Be sure to save your config after ANY changes. WinUAE will not save any changes you make, unless you specifically go back to the control panel to do it.
- To enable the internet on your emulated Amiga, make sure BSDsocket.library is checked in the Misc. Configuration section.
- The clock on the emulated Amiga will be faster then your system clock. There are programs to correct this but the latest version of WinUAE has a setting to do it in the Misc. Configurations.
- If you want to really tweak the look of your Workbench, get MUI, New Icons and the Picasso drivers from the web. Take a look at some of the Workbench pics posted on Aminet. They'll give you some ideas, or inspiration.
- If you don't feel like tweaking, the get a copy of AmigaSYS 3 or Amiga in a Box (AIAB). These are preconfigured setups so you don't have to deal with settings and such. But if you wanna play around, I suggest getting some of the software yourself and experimenting.

This article isn't meant to be a definitive guide on WinUAE. Just a primer to get you started and let you explore what you can do. Visit the Amigaworld.net and Amiga.org forums and find out what others are doing with their Amigas. Most are gaming, but some still use it as their everyday machine. Hope you enjoy your new Amiga!

In our next adventure, the care and feeding of your Amiga 3000!




BIG BROTHER IS WATCHING YOU

spying a spy

BY ISRAEL TORRES

Information is power. With enough of it you can rule the world. Lacking it you answer to those holding it over you. This is how the world works.

In the past information was very simple to get without too many questions (*even information no one else had a right to have*). Though due to the state of "*security*" you and I live in today, getting information isn't quite as simple. It seems everywhere you go someone wants to know something about you. Your name, your profession, what you eat, and what you drink. It doesn't stop there. They want to know anything and everything they can about you. Sometimes they will ask nicely, sometimes they will demand it, and sometimes they won't ask at all. One way or another they will get it if they really want it. Unless you were born in a box somewhere where there are no names someone already knows about you. Scared? You should be.

With today's technology anyone can be "**Big Brother**", it no longer applies to governments, and corporations. Anyone that has anything about you will *drop a dime* if the price is right because something is for sale if someone is buying. It started with junk mail and telemarketing and evolved into spam and phishing. Though now it doesn't stop at trying to sell you something or scam your money, it doesn't stop at stealing your identity, or even your soul. The truth is there is no end in sight for how valuable information will become or the means people will go to get it from you.

For most of you it is already too late. Most of your information is already floating around somewhere and "*manywhere*", never to be "*ungotten*" or forgotten. An entity that is interested in you can watch you from faraway lands or on the other side of your LCD. These spies use the same technology you use to post your blogs, and userspaces. The same technology you use to pay your bills and order sex. The same technology that keeps you alive can be your undoing. It's all ones and zeroes and it doesn't take much to turn one into the other. If you haven't started to panic, you are like the most out there that don't care. Not caring is one of the best tools out there. It is free, and requires zero effort. I can say you are one of the better *non-carers* I have met.

I bet you bought this magazine with your credit card, yes? You may have even used your trusty bookclub card to get a discount or accumulate points, how about a promo code? If you didn't then you took money out of an ATM to buy it and be extra slick and maybe even had a friend buy it for you. Come on stop lying to yourself. You don't care. Admit it. It is the first step!

The second step is to start caring. You can do this by finding out exactly how much about you is out there. Unfortunately you can't just throw a few dollars online to retrieve what the world knows about you like a credit report – that would be mighty convenient (and suspicious at the same time). It actually requires some work, most of it being time to research yourself from the perspective of a spy. Once you learn how spies spy you can spy on spies and feed them what you want them to know, never feeding them too much or too little. Sure you have to feed your spies, otherwise they die and you eventually are sought by other spies – better spies.

One quick way you can see if you are of any interest to the world is to search, and search you must. I would recommend starting with google (http://www.google.com). Search every which way you can that google offers, spend hours looking for you. Of course the more you search the more of interest you become to the search engine. Like it or not search engines are successful by knowing what people are searching for. Though searching could take hours or days depending on how popular you are. Good luck if your name is John Smith or likewise as common.

Let's say you want to be found by the search engines. Well in this experiment you do. Sometimes you may be interested in knowing how many things visit your blog, or website. You not only want to know how many but of the many, who. To keep this simple we will call our subject "**spy**". You can later name it whatever you'd like – for example using your handle, name, callsign, word not in the dictionary, whatever. I have learned the more unique it is the faster it may be found, indexed and easier to find publicly.

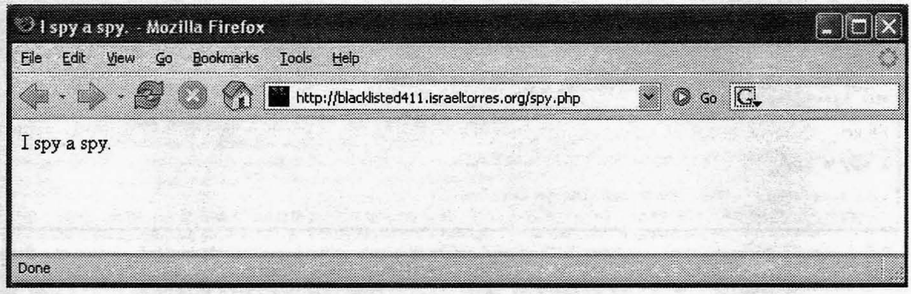
I have always been fascinated by tracking entities that visit me. I like to know who they are, what and who they represent. I've tried using the statistics pages that you get for free out there in the ether but none of them suited my needs. I wanted granular detail about each visitor, where they came from anything that could help me understand why they were visiting in the first place. After I have found out everything I need to know about them knowing about me the more I can understand about what they are looking for. Maybe I can help them… or maybe I can control them. **Information is power.**

Returning to the **spy** example I have spy.php as a file on a web server. Every time someone visits spy.php I will know.

I will know a few things about them, better yet things I'd like to know about them all without their knowing. Remember since most people don't care, they in turn don't care (to a degree). To have spy.php found faster I link it from my index page. You can hide it from obvious view in case you don't want someone else just running in to it and clicking on it by accident, and you can even wait for it to be found without being linked. The idea is that with time it will eventually be found, and you will know exactly when.

So spy.php is a linked file from my index and just has the words spy in it a lot. You can be a lot more convert by displaying something else such as "*Cannot Connect To Database*", tack on a picture of Paris Hilton, or leave it blank. Though if you try and be too "covert" things may not go as planned and the game will change.

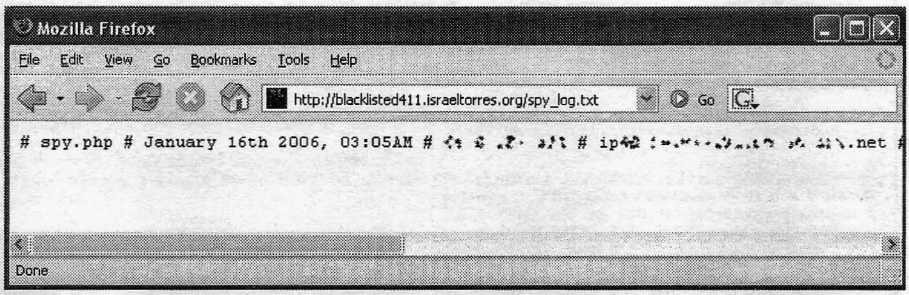
spy.php demo


I spy a spy. - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://blacklisted411.israeltorres.org/spy.php
Go
Done

I spy a spy.

When you click on spy.php it will take the information you represent and record it to a flat file on the webserver. You can click on it a lot and it will log a lot. This could be bad if you don't check every once in a while to make sure the file stays in manageable shape, but could be further helped along by obfuscation or moving away from the flat file entirely and into a database. This demo is simple enough to where you can just drop it anywhere of interest and include the function it needs. You can always view the log, but so can anyone else that knows the url of the log file. This can always be changed to make it more difficult to guess – if you do make sure you sync it with the function itself.

spy_log log file


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://blacklisted411.israeltorres.org/spy_log.txt
Go
Done

```
# spy.php # January 16th 2006, 03:05AM # [redacted] # ip[redacted].net #
```

The source code itself is straightforward and simple. It is also commented so there will be no confusion as to what is happening at any given time. You can type this all out or download at the site cited at the end of this article – you decide.

Spy.php really is of interest because this is where I am setting up and calling our main function to do all the logging and tracking. Just make sure you put spy_functions.php in the same directory and you should be golden. No matter which php file you put it in, the logging will show the file it was called from originally.

spy.php source

```
<html><head><title>I spy a spy.</title><body>

<?php
// Blacklisted 411 Article: Spying A Spy
// Israel Torres <israel@israeltorres.org>
// Required Files:
// - spy.php - the three operations below
// - spy_functions.php - the function spy_track
// - spy_log.txt - the log file (flat file)
/////////////////////////////////////////////////////

// Include spy functions.
include 'spy_functions.php';

// Find this page's name and save it as a variable.
$spy_fname = basename($_SERVER['PHP_SELF']);

// Track this file and interesting information sought.
spy_track($spy_fname);

?>

I spy a spy.

</body></html>
```

Spy_functions.php contains our tracking and logging function that ends up writing all the desired information to a flat file.

spy_functions.php source

```
<?php

// Blacklisted 411 Article: Spying A Spy
// Israel Torres <israel@israeltorres.org>
// Required Files:
// - spy.php - the php three operations
// - spy_functions.php - the function spy_track
// - spy_log.txt - the log file (flat file)
/////////////////////////////////////////////////////

function spy_track($spy_fname)
{
// allocate the server variables for later use
// retrieve the remote IP address
$spy_ipaddress = $_SERVER['REMOTE_ADDR'];

// retrieve the resolved host name
$spy_hostname = gethostbyaddr($spy_ipaddress);

// retrieve the user agent
$spy_browser = $_SERVER['HTTP_USER_AGENT'];

// retrieve the referral URL
$spy_referer = $_SERVER['HTTP_REFERER'];

// create a time stamp
$spy_time = date("F jS Y, h:iA", time()-1*60*60); // PST offset from server -1*60*60

// create the log template (one line)
$spy_log_entry_unfiltered = "# $spy_fname # $spy_time # $spy_ipaddress # $spy_hostname #
$spy_browser # $spy_referer #\n";

// remove extras from the log
$spy_log_entry_filtered =  stripslashes($spy_log_entry_unfiltered);

// allocate the log file name
$spy_lname = "spy_log.txt"; // You need to create this file and set rw permissions

// open the file for appending
$spy_hndl = fopen($spy_lname, "a");

// write to the log file
fwrite($spy_hndl,$spy_log_entry_filtered);

// close the log file
$spy_hndl = fclose($spy_hndl);
}

?>
```

Once you look over the code and read the comments you can add or remove anything missed or disliked. Though this is common information that can tell you a lot about a visitor and why they may be visiting. As mentioned above you can rename it and pass out the link and its message to someone you want to know more about without letting on that you are spying on them. You can also add this spying functionality to any of your php enabled web pages by simply running the three operations mentioned in the spy.php source. You'd most likely want to modify the filenames so make sure you sync them up with one another otherwise your results may vary drastically. You also want to make sure you check back once in a while on the flat file so that it doesn't fill up your userspace. It takes a while if you have light traffic and no one knows about it being there.

You'll notice a lot of search engines that visit your site. You will also find out more about them by the information they leave behind, some leave contact URLs with more information as to what exactly they are. Depending on where you are using it and who hears about the page could prove some very interesting results. For example I had an entire website set up to monitor all the pages on the site. I mentioned the link to one person and within a few days had several hits from people relating to this person. I even knew how they came to know of the site because of the referral link showing it came from a hidden forum. A lot of times I've seen links coming from gmail accounts; sometimes I wonder why depending on what the link being referred is. I have also seen offline rippers go to work on one of my sites from various companies thanks to their user agent information I know which software they used to rip my site(s).

Information is power. Don't let your information get the best of you; instead forge your information to work for you. Do it right and your only regret will be not doing it sooner. It is once again time to control transmission. Steal your stolen goods back and protect them as best you can. There is only one of you, keep it that way.

Thus, therefore, and in conclusion anytime someone gives you a link try and be more careful for they could be a spy. Or maybe you are just paranoid – you decide.

Keeping it 'rael,
Israel Torres

Downloads
Spy Source Code
http://blacklisted411.israeltorres.org/Blacklisted411_SpyingASpy_Source.zip

Spy Demo (Make sure you read this article first!)
http://blacklisted411.israeltorres.org/spy.php

The Black Market

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

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

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 I'm 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

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

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.

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.

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.

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

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.

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.

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

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

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

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

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

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.

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

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.

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

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.

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

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

HACKING, PHREAKING, computer security and education on the First Tuesday of every month in the Detroit area. Meeting is at 7pm at Xehdo's cafe in Ferndale. Bring your open mind and positive attitude.

I WANT TO OFFER my playstation 2 game burning service. Any game that you would like for a back-up or just for fun. Or maybe that Japanese game that just won't be out in the United states for a few months.. I have bundles that you can choose from if you want handfulls depending how much you order. the games are $25 each !PLEASE NOTE THAT YOUR PLAYSTATION 2 NEEDS TO BE MODDED I ALSO HAVE THAT SERVICE BUT YOU CAN ALSO GOOGLE SEARCH FOR PREMODDED SYSTEMS TO BUY. EMAIL IF YOU HAVE ANY QUESTIONS AT ALL.

ACCUSED OF A COMPUTER RELATED CRIMINAL OFFENSE IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in the defense of alleged cybercriminals, including but not limited to, hackers, crackers, and phreaks. Not a former prosecutor seeking to convince defendants to plead guilty, but an idealistic constitutional and criminal defense attorney who helped secure a total dismissal of all charges in Los Angeles Superior Court for Kevin Mitnick, who was falsely charged with committing computer-related felonies in a case with $1 million bail. Please contact Omar Figueroa, Esq., at (415) 986-5591, at omar@aya.yale.edu or omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Complimentary case consultation for Blacklisted 411 readers. (Also specializing in medical marijuana and cannabis cultivation cases.) All consultations are strictly confidential and protected by the attorney-client privilege.

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

I-HACKED.COM is a hardware hacking based website and it currently looking for articles! Membership is limited to contributing members, so come and share your knowledge with other hackers around the world. Topics we are currently looking for include: DVD "Dual-Layer" Firmware hacks, CD-RW / DVD+/- Speed Hacks, Video Card Hacks, Motherboard Hacks, IDE Card / Raid Hacks, Xbox Hacks, Playstation Hacks, cell phone tricks, or anything else you might have. Check us out @ http://www.i-hacked.com

SUPPORT OUR HACKER COMMUNITY! I happened upon this site looking for an image hosting service and thought I'd share it with the rest of the community. It's called Smugmug and you can find it at www.smugmug.com. Not only do they have a high quality service going on, but they also feel about hacking as we do. Check out what they say about hacks on their website! I've been using their service for a while now, and I can honestly say that what they pay attention to the little details. By far the best photo site out there! Because they understand what hacking really is, they know what they're talking about. Why does this matter? Well, they too are probably hackers and we all know that hackers can put together something great when they put their minds into it. Store unlimited photos starting at only $29.95/year....that's right a year! That's a great bargain! There is a free 7 day trial offer, and if you use the code NTQ0He0Ou527E you'll get a $5 discount.

DO YOU WANT MORE underground information? Are you ready to go to a whole new level of knowledge? Then you need to check out "Binary Revolution" magazine. <BR> is a printed hacking magazine put out by the DDP that covers hacking, phreaking, and other assorted topics from the computer underground. For more information on the magazine, forums, HackRadio, HackTV, or any of our other numerous projects, come to www.binrev.com and join the revolution. "THE REVOLUTION WILL BE DIGITIZED."

TUNE IN TO CYBER LINE RADIO on the internet, on the USA Radio network. We can be heard Saturday Evenings 9:00 pm to 12:00 am (Central). Heard Exclusively On The USA Radio Network & Via The Internet! We discuss Technology, Space, Hacking, Linux and more. For more details meet us at www.cyber-line.com.

BLACKLISTED MEETINGS will begin in Greece as the new year arrives, They will be held every 3rd saturday of the month and they will begin at 7pm. Meeting point will be the centre of Athens at the metro station Panepistimio by the fountains. Also check the webpage www.blacklisted411.gr.

A+ CERTIFIED TECHNICIAN offering cheap repairs in Louisville Area. Will make house calls or take home with me. I do everything from virus and spyware removal to networking. Send an email to alanb6100@gmail.com with your name and phone number as well as a description of the problem. Also I have Gmail invites available for a reasonable price. Louisville area only unless you want to Western Union me some money! Thanks!

SELLING USED HIRSCH SCRAMBLEPADS that retail new for around 500$ for your best offer! They are for very high security places, every time you press the START button on the keypad it randomizes the digits so that any onlookers cannot find a pattern in the digits you press. Also, you cannot see the numbers from the side, so for anyone to see your code they would have to be directly behind you. Email me for more information. guiltyspark414@netscape.net

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

HI, MY NAME IS RICK. Me and my friend Rob where looking for a low cost rackmount server one day to use for a web and mail server that we could have racked at a local datacenter, Not finding anything real cheap we decided to start our own company building fast cheap servers for you also. www.cheap1u.com was born. Mention this ad and get 10% off any server order. Also since I am the owner, if you mention this ad buy 10 servers and I will throw in the 10th server for free!

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

Extreme Pizza - 14141 Jeffrey Road, 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

Colorado

(719 Area Code) - Colorado Springs

DC719 - Hack the Rockies. Meetings held on the 3rd Sat. of every month. 8pm-11pm @ Xtreme Online, 3924 Palmer Park BLVD

Hosted by: DC719 POC: h3adrush

(303 Area Code) - Centennial

We meet the first Friday and third of every month at 5:00pm at the Borders café on Parker in Arapahoe Crossings.

Hosted by: Ringo

Florida

(407 Area Code) - Orlando

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

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

Hosted by: Whisper

Georgia

(678/770/404 Area Codes) - Duluth

Meetings are the first and third Tuesday of every month, in the cafe of Frys Electronics. They start at 6:30 until we get kicked out, and then continue elsewhere. Visit our site at www.HackDuluth.org and sign up on the forums to receive emails about the group.

Hosted by: P(?)NYB(?)Y

(678/770/404 Area Codes) - Snellville

Borders at 1929 Scenic Highway, first Saturday of every month. 8:00PM

Hosted by: iamsam (comingtoleave@gmail.com)

Illinois

(217 Area Code) - Urbana

Espresso Royale Caffe. 1117 W. Oregon St., Urbana, IL 61801. At the corner of Goodwin and Oregon, across the street from the Krannert Center for the Performing Arts. Every second Friday of the month, 8 PM

Hosted by: r3tic3nt (r3tic3nt@gmail.com)

Iowa

(515 Area Code) - Ames

ISU Memorial Union Food Court by the payphone. First Friday of each month, from 5:00pm onward.

Hosted by: Omikron

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

Texas

(713 Area Code) - Houston

In front of Rocfish on Westheimer/Kirkwood. Last Sunday of every month, 7:00pm till close.

Hosted by: MuertoChongo

(915/325 Area Codes) - Blackwell

John's Detectors, 501 W. Main St. Third Friday of every month. 7:00pm until...? For more information, visit our site at www.johnsdetectors.com

Hosted by: Wirechief

Wyoming

(307 Area Code) - Rock Springs/Green River

White Mountain Mall—Sage Creek Bagels. The last Friday or every month from 6:30pm until 9:30pm.

Hosted by: Phreaky

Mexico

(666 Area Code) - Tijuana, B.C.

Café Internet, Calle 12, Felix M. Gomez #844, Col. Libertad. In back room by payphone. First Friday of the month, 5:00pm to 8:00pm

Hosted by: Tom

YOUR MEETING HERE

Start up your own meeting and enjoy the benefits! Contact us right away!!

meetings@blacklisted411.net

History Of Blacklisted 411

Started as one of the first disk based hacker magazines in 1983, Blacklisted! 411 has evolved into one of the most widely distributed hacker magazines to date. Since its creation, the staff at Blacklisted! 411 have strived to publish original and controversial articles on a variety of subjects. With the beginning of 2006, Blacklisted! 411 will present new ideas and concepts for the entertainment and education of the security/hacking community. Shown below are some cover shots of past issues ranging from 1994 to 2005.

Blacklisted! 411

The Official Hackers Magazine

After 6 years, we're finally BACK! The premier issue of Blacklisted! 411

1994

Blacklisted! 411

The Official Hackers Magazine

Uh, not so "Secret" Air Base?

What is he doing in there?

1995

Blacklisted! 411

The Official Hackers Magazine

1996

Blacklisted! 411

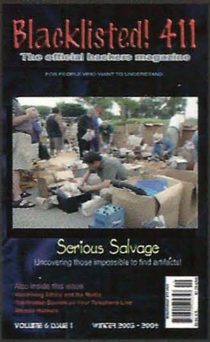
The Official Hackers Magazine

1997

Blacklisted! 411

The Official Hackers Magazine

1998

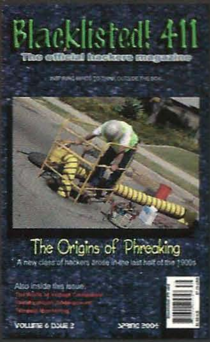

Blacklisted! 411

The official hackers magazine

Serious Salvage

Uncovering those impossible to find artifacts!

2003


Blacklisted! 411

The official hackers magazine

The Origins of Phreaking

A new class of hackers arose in the last half of the 1900s

2004

Blacklisted! 411

The official hackers magazine

Electronic Surveillance

Introduction to Wireless Networking

2005

Blacklisted 411 the Magazine

P.O. Box 2506
Cypress, CA 90630