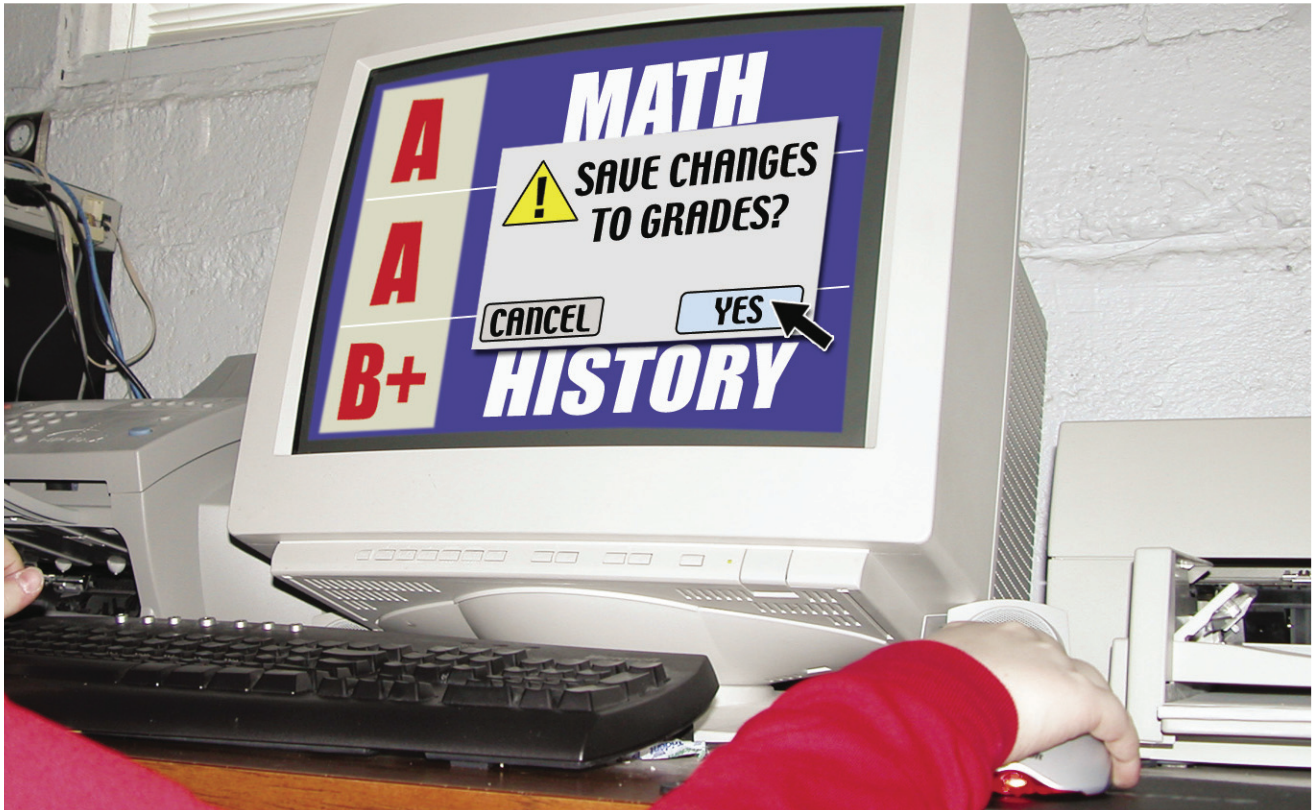


BINARY_REVOLUTION

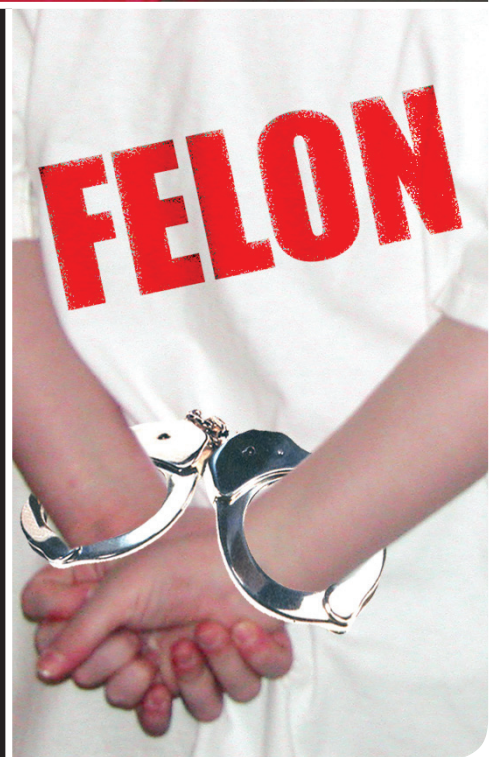
<a DDP Production>

[issue:]# /bin/rev/1.1



2003

- > Crime: Changing report card grades
- > Tool: Computer
- > Punishment: Felony charges, public scrutiny, and emotional trauma



BINARY_REVOLUTION

[a DDP production]

Binary Revolution is a magazine about technology. Specifically, we look at “underground” topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. We will also address politics as they relate to technology or digital rights.

On-topic poetry, photography, and art are welcomed as well. This magazine is what we make of it, so please send your submissions, comments, questions, and suggestions to articles@binrev.com or letters@binrev.com and help the revolution continue!

www.binrev.com

BINARY REVOLUTION is a DDP Production

The Digital DawgPound is:

StankDawg
dual_parallel
bland_inquisitor
logan5
biOs
w1nt3rmut3
Evo_Tech
nick84
Rax

/bin/rev/staff/

Editor-In-Chief: StankDawg
Layout and Design: logan5
Webmaster: bland_inquisitor

Cover Credits:

Concept: StankDawg
Design and Layout: logan5

Disclaimer: This magazine is about education. It may address topics that can be used in a negative manner, but they are only presented for the sake of knowledge and learning. We DO NOT CONDONE using any of the techniques or topics addressed in this magazine, or any of the sites mentioned in this magazine, for destructive purposes. None of the members of DDP, nor the individual authors of the articles, accept any responsibility for any damage that you may do with the information we present. You are responsible for your own actions.

Copyright: The articles included in each issue are written by a variety of authors. Each author holds the copyright to their respective articles. To reprint an article, you should contact the authors directly and get permission to use their work. In addition, the art and logos referring to “DDP”, “The Digital DawgPound”, “Binary Revolution”, and any derivation thereof are copyrights of The Digital DawgPound. If you want to use any DDP content, simply contact us and will gladly give consent under most circumstances. Simply use common courtesy and we will gladly cooperate.

Binary Revolution - © 2003 The Digital DawgPound



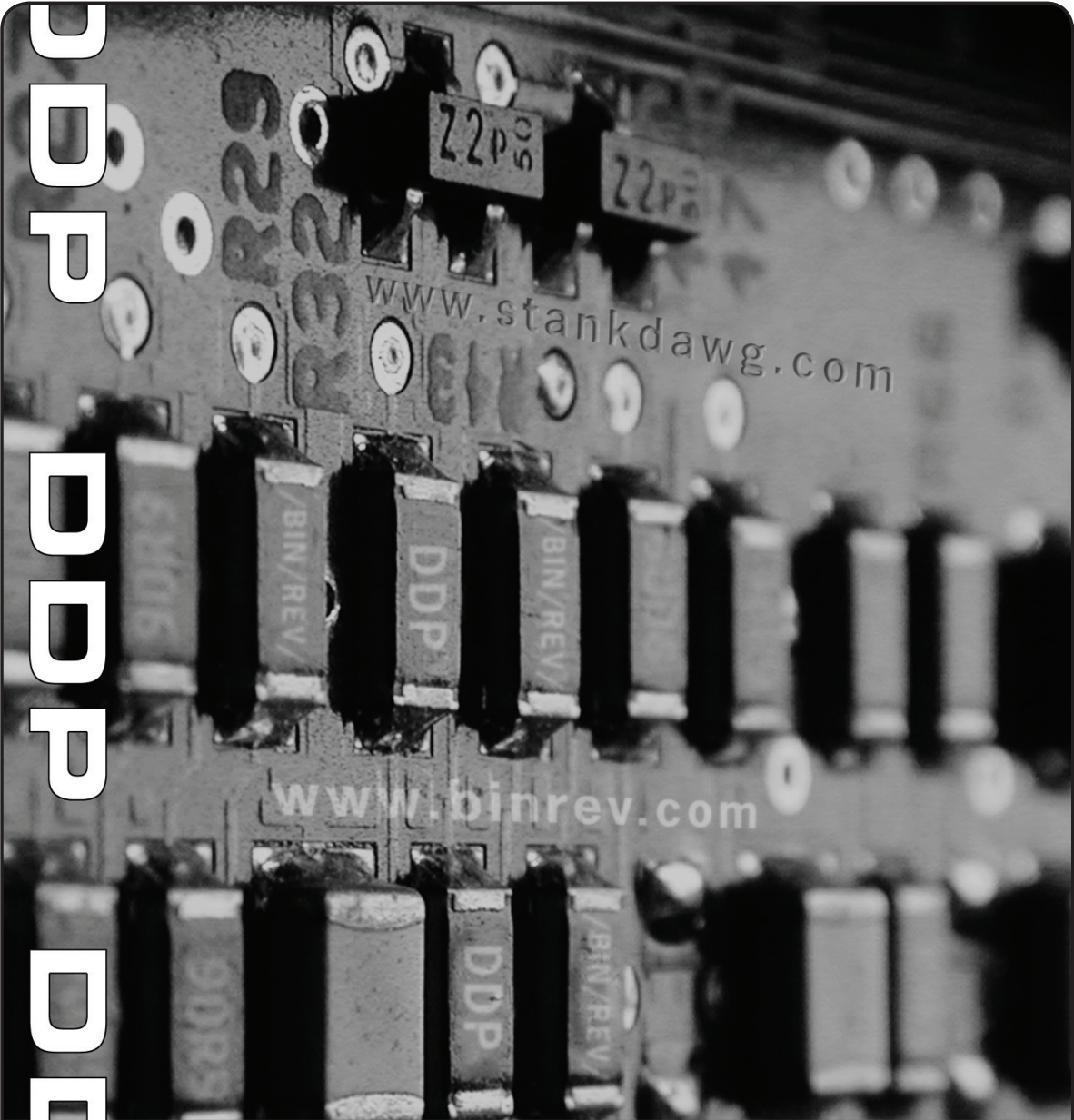
BINARY_REVOLUTION

[a DDP production]

```
ls /bin/rev/1.1/*.*
```

file:	creator:	file size:
Editorial/Introduction	system	03-04
HACKING 101— Footprinting a system	StankDawg	05-09
DoS: Tools of the Tools	bland_inquisitor	10-12
2600 secrets	nick84 & StankDawg	13-14
Letters	system	15-18
A nubies guide to ghettodriving	StankDawg	19-22
Phreaking Italy	w1nt3rmut3	23-24
Cookies: The Good, the Bad, and the Ugly	bland_inquisitor	25-27
Public TTYs: Description and Methodologies for Free Calling	dual_parallel	28-34
Your rights and why you already lost them	Evo_Tech	35-36
Perl Corner— Watching the watchers	nick84	37-39
Closing comments	system	40

DDP DDP DDP DDP DDP DDP DDP





Editorial/Introduction

What is wrong with this world? We live in an age where the most bizarre events happen. It is almost as though every episode of every bad sitcom is coming to life as the days unfold. Things that used to be considered humorous, and matters that were once considered minor are now becoming felonies! That was the motivation for the cover of this issue.

On February 12th, 2003, the Palm Beach Post reported on this bizarre incident that could easily been an episode of "Diff'rent strokes". A 6th grade student (age 11) did something that many children may have done in their lives. He changed his grades. He may have been ashamed of his grade, or felt he was graded unfairly, or any number of reasons for the action. The reasoning is not important. He simply made a bad decision based on whatever reason he had. Now this is wrong, and is something that should be punished. This is not at question! If you do not already know about his story, you might guess at the punishment for such an act. Perhaps the child was suspended from school for a few days. Perhaps he was forced to stay after school or be required to do extra homework assignments. Perhaps you feel that this is a matter that the child's parents should handle by grounding him and making him apologize for his actions. How would you react if this were your child? What would you honestly consider to be an appropriate punishment for this situation?

Helen Roberts, principal of St. Lucie West middle school had him arrested!

That is correct, I said ARRESTED! Not only was he arrested, but he was arrested with a FELONY charge against him! What felony did he commit, you ask? He committed an "offense against intellectual property". At 11 years old, the child now may have a felony on his record for changing a grade on his report card. Not only that, but principal Roberts also went the extra step of EXPELLING him from the school. How is it that we let drug dealers and murders get off with a slap on the wrist every day in the United States, but an 11 year old child cannot make a mistake? When I hear about things like this, it make me ashamed to be a human being.

You might be thinking to yourself that there must be more to the story, some other reason that such action was taken. Allow me to explain the details as they were reported by the Palm Beach Post (<http://www.palmbeachpost.com>) written by Nirvi Shah. The story goes like this: the boy (who is a minor and therefore nameless) was sitting in the lunchroom, when he came up with his diabolic plan. He told his teacher Susan Seal that he left his lunch in her classroom. When he went to the classroom, instead of retrieving his lunch, he sat down at Ms. Seals computer and changed 5 grades on his reading assignments and, of course, saved the changes. While doing this, a math teacher walked by and caught him. The boy lied, as boys sometimes do when they get caught, and was taken to the principals office to account for his transgression.

Principal Roberts did some research and came up with the following quote from the school resource deputy: *"Whoever willfully, knowingly, and without authorization modifies data...residing or existing internal or external to a computer... for the purpose of devising or executing any scheme or artifice to defraud... is guilty of a felony of the second degree."* Ellen Mancini, an assistant state attorney in the St. Lucie County juvenile division said, "He modified data. I'd say it was a scheme to defraud". She went




on to say, "It's cheating. It's depriving other students of the fairness of the system," she said. "It's as much a fraud as anything else. Sometimes, you have to do things as an example of the authority of both the school system and the legal system". In her evaluation of the event, the 11 year child intended to defraud the school. Whose grades are these anyway? Wasn't there a saying when I was a child that said you are only depriving yourself when you cheat? Was he wrong? Yes! Does the punishment fit the crime? Of course not! I cannot believe that it is really a question, yet these people seem to be very serious about going through with it. Kids have done this for as long as there have been schools! I think saw an episode of this on "Little house on the prairie" for God's sake. It wasn't a felony then, and it isn't a felony now!

What happened to common sense in this world?

According to their webpage, St Lucie West Middle School prides itself on being "One of the Top 100 Wired Schools" in the Country by Family PC Magazine and the Princeton Review. A smiling principal Helen Roberts sits above the welcome message, with obvious pride in her accolades. Perhaps she doesn't realize that the instructor's computer was left turned on, with no password protection. In my opinion, this is something that is not typical of a "top 100 wired school". Maybe she thinks that security is not a necessity in a top "wired school". Interpreting laws is not a focus at a wired school obviously, nor is common sense. I guess she can take pride in the fact that one of her students *DID* learn a great deal about computers and applied what he learned. Unfortunately, she wants him expelled. Maybe Princeton and Family PC magazine are not the greatest judges of what constitutes a "wired school".

So how does the story end? The child was processed through the St. Lucie County jail, and then he was released to his father. Luckily, after 2 weeks of media coverage by independent media on (and off) the internet and even mainstream media including Fox News, the Florida state attorney's office decided NOT to prosecute the child as a felon. Instead, he'll be routed through a diversionary program for first time, nonviolent offenders. The boy's father made him write letters of apology, and now is working with an attorney of his own to defend his son against these ridiculous attacks. This is the very definition of triviality in our court systems. Now, because of the failure within a broken system where incompetence abounds, the boy's father must spend his hard-earned money to defend against something that should be over and done with. Even these new punishments and charges are too much, in my opinion, and more attention is needed to the case. What about the actual decision makers who are keeping this whole sitcom going for another season? Ellen Mancini (ellen@stlucieco.gov) and Helen Roberts (hroberts@stlucie.k12.fl.us) obviously do not think they are wrong. If you think that they are wrong, please let them know.

In the meantime, enjoy the myriad of articles contained in this first issue of **BINARY_REVOLUTION!** The ranting is limited to the first couple of pages, I promise. The rest of the magazine contains articles that cover technology, phreaking, hacking, digital rights, security, and everything in between. We appreciate your support, and I look forward to being around for a while, if you will have us. But now, I turn the magazine over to the members of the Digital Dawg Pound. Enjoy! 



STANKDAWG



HACKING
HACKING
HACKING



HACKING
HACKING
HACKING

This article is the first in a series of articles that address the oft-asked question, "How do I become a hacker?"

"Footprinting" A System

By: StankDawg

StankDawg@hotmail.com

Hacking is a very broad term that can refer to many things. In the context of this article, I am going to use hacking fundamentals to help you to "think outside the lines." It may sound cliché to say it, but once you get the hang of the concepts that I am teaching you, and the precise ways to accomplish each goal, you will start to understand the mindset of a hacker.

One of the things that most hackers have in common is the concept of thinking their way around things. When faced with a problem, or a situation that seems to have no options, hackers are able to make options appear. Before a hacker considers the situation closed, they make sure that all possibilities have been examined. This entails gathering all of the information about a given situation and thinking about where that information can lead them. With all of the information at hand, more options can be discovered. In a technical environment, this means "footprinting" a system to get all of the information you can about a particular environment in order to thoroughly investigate it.

Why is this step necessary? Many hackers don't know what it means to footprint a system and others simply do not see the value in it. By footprinting a system, you will get detailed information that will keep you from using inappropriate tools or methods of attack on a system. For example, in the screen shot below, you will notice that an attacker is trying to use a known exploit to break into my server. If this user had done a little bit of work beforehand and footprinted my system, they would have known that I am running an Apache web server on a machine using the Linux operating system. The exploit that they were trying to use only works in systems running specific versions of Microsoft Windows. This is obviously the work of a "script kiddie" who doesn't understand basic hacking concepts. This attacker was probably just going through a range of IP addresses using the same exploits, hoping that he gets lucky and finds one purely by accident. I wish him luck.

```
--- -- [30/Jan/2003:08:25:41 -0500] "GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 1222 "-" "-"
--- -- [30/Jan/2003:08:25:47 -0500] "GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 1222 "-" "-"
```

Screen Capture 1 - IP address blurred to protect the incompetent

To "footprint" a system, or to get a "footprint" of a system means to use logic and technological understanding to obtain all of the publicly available information about a system. Why is this important? Sun Tsu stated in his famous writing The Art of War, "...that general is skillful in attack whose opponent does not know what to defend." You



should know everything humanly possible about a system, company, and site before even touching it for the first time. By knowing all of the details about the system, you know more about your attack than your opponent knows about their defense. This puts you at an advantage.

To go about the process of gathering information, you should first start with the basics. If the company has a web presence, by all means check it out. You may even check out their competitors and see if they have already done some research and comparison work for you. I have found charts at other sites that compare that competing company to the company you are looking at, using technical data. What a great time saver that can be! As you continue your research, take notes regarding all of the different server names that you may run across. Open a text editor like notepad or something similar to copy and paste different bits of information into a text file. For example, say you notice that when you enter the "support" section of the site, the server name changes from *www.fakecompany.com* to *forums.fakecompany.com* or something similar. Make a list of all of the servers. Notice the structure and naming convention of their folders. Copy the name and address of the company, find out where it is located, and may be get a list of names of employees. You may even take it upon yourself to call the company and try to get more information over the phone. Every little bit of information has some value. Companies make a living doing data mining and data warehousing on consumers. Why not flip the script and do a little data mining on them?

Other than the obvious digging through their website, pamphlets, phone book, and other public sources of information, what else can a person do to get a better footprint of a system? Well, most of the ideas so far were more along the lines of company information. This company information, which may contain user information, can tell you a lot about the technical environment that exists. For example, if there are email addresses that are publicly listed, this could be invaluable information. Why? With the onset of single-sign-on, these may be the same usernames that are used for all access. So never dismiss this first step of information gathering as unnecessary. Once you have gotten that out of the way, you can jump into the technical part of the footprint. Now it is time to do some real digging on the technical side of things.

The very first place that a person should go is to the global domain registry. Currently, this is operated by VeriSign at <http://www.verisign-grs.com/>, although it could change to a different URL and ownership as the government tries to tinker with and extend its control over the internet. Basically, just find the global registry, wherever it may move to, and it contains the IP address and information of every web site that exists on the internet. This is also referred to as a WHOIS database or a WHOIS lookup. The result of a WHOIS search contains the name of the registrar that is responsible for giving access and/or hosting service to the site in question. You should then, in turn, go to the WHOIS lookup for the individual registrars. This second search will give you all of the contact information for the person(s) from that company who is/are responsible that site. You will be presented with phone numbers, DNS server names, and lots of information that you should also keep in your footprint. Some of this may be used for more technical research, and some may be saved for future social engineering. Be warned that while this is usually accurate for companies, it is notoriously inaccurate for rogue websites. Many users choose to give false contact information to protect their personal privacy. Another quick bit of information to get is the IP address of the system. You can use a simple command line tool called NSLOOKUP to do this on a remote system. There are many other ways to do this as well. Any software site will have several network applications



that will do IP address lookups as well as many other functions that will help form a deeper footprint. Sometimes you may have physical access to the target system but not have commandline access, nor do you have any applications that will find the IP address for you. In this case, you can use one of hundreds of tools on the web. One that comes in handy is <http://www.whatismyip.com> which will give the IP address of the system you are currently browsing from. This is particularly useful from public places where you need to footprint quickly and without drawing a lot of attention.

One final thing that I like to do when creating a basic footprint is to try and find out where the system is physically located. Sometimes the machine is not physically located at the same place as their offices or that they publish on the web site. One tool that you may use for this is called TRACEROUTE (or TRACERT) which will start from your IP address and show you the path that it takes from you to the destination. The reason for doing this is to get an idea where your packets travel on the way to the destination. Again, this step is very rarely used in practice because people do not realize the importance of the data that is presented by this simple utility. Does it leave the state or country that you are in? This makes a great deal of difference in the legality arena. Does it pass through a .MIL or .GOV domain on the way? That would make me very suspicious. Look at the screenshot below at a portion of a TRACERT to the site mentioned above. You should get in the habit of interpreting the naming conventions that you see. You can see below that while the names may seem random, you will see tell-tale signs that show that hop-9 took place in Atlanta (*.ATL5.*) and then continued on to several hops in Chicago. From Chicago, it reached what appears to be Michigan (*.LNNG.MI.*) then into Flint Michigan (*.FLNT.MI.*). Not all names are clear cut (like the last hop) but you now have any idea that this server is in, or near, Flint Michigan (In actuality, it is just across the border in Illinois).

```

C:\WINDOWS\System32\cmd.exe
  9  48 ms  49 ms  49 ms  0.so-1-0-0.TL1.ATL5.ALTER.NET [152.63.85.217]
 10  68 ms  69 ms  68 ms  0.so-6-0-0.TL1.CHI2.ALTER.NET [152.63.13.21]
 11  67 ms  69 ms  69 ms  0.so-1-0-0.XL1.CHI2.ALTER.NET [152.63.67.106]
 12  68 ms  69 ms  69 ms  0.so-7-0-0.XR1.CHI2.ALTER.NET [152.63.67.130]
 13  68 ms  69 ms  68 ms  293.ATM7-0.XR1.CHI6.ALTER.NET [152.63.65.30]
 14  66 ms  69 ms  79 ms  191.ATM9-0-0.GW1.CHI6.ALTER.NET [152.63.65.69]
 15  67 ms  69 ms  69 ms  voyager-gw.customer.alter.net [157.130.118.138]

 16  76 ms  69 ms  69 ms  498.atm6-0.rtr1.lnng.mi.voyager.net [169.207.224
.145]
 17  70 ms  79 ms  69 ms  se3-0.rtr0.flnt.mi.voyager.net [209.153.129.86]
 18  86 ms  79 ms  79 ms  winntcluster.fastdnsservers.com [209.81.157.200]

Trace complete.

```

Screen Capture 2 - Also notice that the name in the final hop tips off the OS as possibly being Windows NT

By now you have a pretty good idea of what servers are in play and the major system targets. *Notice that I still have not touched the systems directly!* I have done all of this basic level footprinting by using public means. Even now, there are more things that you can, and should do, before you take the next steps and start touching the systems directly. The next step is to identify what operating systems the systems are running as well as what applications the systems are running.



To find the operating system, it is helpful that you are familiar with operating systems in general. By knowing some of the standards and naming conventions of the operating systems, you may be more likely to recognize the system. Again, this information may also be easily garnished from the company's web site or other public records. Look for the "about" page or search through their help files to see if there are references to the technical environment that they run. But by having some general experience with different operating systems and how they look and feel, you may be able to determine, or at least make a strong guess at the operating system. Look for signs like error messages that are specific to a certain operating system. Watch the naming conventions that it uses. If you see references to directories with names like "/usr" or "/etc" then you have an idea that it is probably a UNIX system of some kind. Do not assume this to be the case, since many systems are "honeypots" that are set up to look like something else entirely just to lure you in and trap you. There are also tools online that will query a site, and based on technical responses to packet requests, give you a good idea what the site may be running. One of the best is <http://uptime.netcraft.com/up/graph/> but there are others to choose from. I could have presented this URL to you earlier, but it is important not to be dependant on these tools without understanding the principals that they are based upon.

The rest of the footprinting processes become more intrusive. From here on in, you are probably no longer viewing public information! That means that you could be breaking the law if you perform these steps on a system to which you do not have authority. For the rest of this exercise, we will assume that you have authority to the systems in question. It can be debated whether simply looking at a system is an attack or whether a portscan constitutes access. The bottom line is that you need to know the up -to-date laws for your state and country. Even if you do these things innocently, and for the sake of knowledge and understanding, YOU MAY BE BREAKING THE LAW! Do so at your own risk.

The next step of the footprint is to find out what applications the target system is running. There are many ways to do this. I have to repeat that this kind of information may also be found on the companies web page or documentation, so always check there first. They may publish .XLS files or .PDF files which tells you that they are running Microsoft Applications as well as Adobe applications. What you may find far more interesting are the proprietary programs and applications they are running and what databases they use. Usually, however, this level of technical data is kept a little bit more private. Similar to finding out the operating system, it is a good to have some experience with different types of databases and applications. Look for error messages (or success messages) that may give you a clue. Something that says "Error code: ORA4500" could indicate that they are using an Oracle database. So could a directory called "C:\ORANT" or similar naming convention. If they give you public access to their systems, try them!

One of the best ways to find very technical information about a system is also the most dangerous. It is called a portscan and it is dangerous because it will most likely get you caught, especially if you do it carelessly. There are many different portscan tools and applications out there that will allow a user to select a system by IP address (which you should have from the earlier steps of the footprint) and scan it to see what open ports it has. If the system you are scanning has an intrusion detection system (IDS) then you should be forewarned that the act of portscanning is considered "hostile" by most of these programs. Your IP address and activities will be logged and



Service	Protocol	Port
netbios-ssn	TCP	139
netbios-ssn	TCP	139
netbios-ssn	TCP	139
netbios-ssn	TCP	139
netbios-ssn	TCP	139
netbios-ssn	TCP	139
pop3	TCP	110
pop3	TCP	110
pop3	TCP	110
pop3	TCP	110
pop3	TCP	110
	TCP	25
smtp	TCP	25
	TCP	25
smtp	TCP	25
	TCP	25
	TCP	25
smtp	TCP	25
smtp	TCP	25
smtp	TCP	25
smtp	TCP	25
ftp	TCP	21
ftp	TCP	21
ftp	TCP	21

investigated by the security officer for that system! Depending on what else you do, it could be elevated to a law enforcement agency. This is one of the reasons for the motto: "NEVER HACK FROM HOME!"

The portscan will tell you all of the open ports on the machine. If the system has multiple machines, which is highly likely, you should portscan all of the ones that you know. By analyzing the results from a portscan, you can tell what ports it has open. You may recognize certain ports as being used by certain apps. The screen shot to the left was taken from a limited portscan. You can see what services they are running and by connecting to some of them, you may discover what applications they are using. Better portscan and network analysis tools will give you similar information and much, much more. Two of the best commercial packages for hardcore footprinting and

security risk analysis are NetRecon from Symantec, and LANGuard from GFI. There are literally hundreds of free and open source equivalents as well. I highly recommend you do this from a different location if you are not previously authorized to do this! If you do a portscan using your laptop from a library, coffee house, or university, then it will be much more difficult to track the alleged attack back to you.

This is another reason for the great interest in wireless hacking. With open wireless networks, you can get an almost totally anonymous connection that can be untraceable if you know what you are doing. Another great tool if you have physical access to the system is <http://scan.sygate.com/> which is a portscanner and other tools, all of which have a web interface. Once again this is useful if you are in a public place trying to find information on a public system. This could also be useful if you are inside the company you are researching. Depending on how serious you are about this investigation, you might even consider working for the company part-time if you do not already. This will give you limited access to insider information and give you physical access to their systems.

This may seem like a long process, but as you get better at it and get the hang of it, you will get faster. But speed is not necessarily important, which is why note-taking is emphasized so much. Taking good notes is a must and also allows you the luxury of stopping and continuing later. This does not all have to be done in one sitting! In actuality, it may be better to spread out the time between visits to prevent patterns in the logs that may get you detected more easily. You will notice that in almost all of your hacking endeavors, this fundamental process will come up over and over again, or at least some parts of this process. Get good at doing it and it will become second nature to you. The most important thing is that you understand the importance of it, and realize that even though it may sound cliché, knowledge truly is power.



DENIAL OF SERVICE ATTACKS

Tools of the Tools

By: bland_inquisitor (bland_inquisitor@hotmail.com) of the Digital Dawg Pound

DISCLAIMER:

All of the information contained in this article is for **INFORMATIONAL PURPOSES ONLY!!** I do not approve of DoS attacks used for the sake of mindless violence; I think that in this form they are the direct opposite of hacking. If you manage to use this information illegally, it's your problem not mine.

OVERVIEW:

We've all heard their names: Teardrop, Fraggle, Smurf, Bonk, and many more. DoS attacks are small, nasty, readily available, and take zero technical proficiency to use. This is a bad combination for everyone. EBay, ZDNet, CNN, and countless other systems have fallen victim to this type of criminal activity. DoS attacks cost corporations millions of dollars every year in lost productivity. In this article I hope to show the basic theories behind how a DoS attacks are possible, explain some of the generic DoS scripts out there, and show how DoS attacks have evolved into more precise and lethal tools of destruction.

TYPES OF DoS ATTACKS:

Bandwidth Consumption-

The least personal, and most easily detected, type of DoS attack is based on bandwidth consumption. How it happens, is that the attacker will eat up all the available bandwidth on the victim's system. There are 2 possible ways this can take place.

- I. If the attacker has more available bandwidth than the target, he can simply flood it by being able to receive more information than he needs to send. (Ever heard the term "ping flood?")
- II. Some DoS attacks, as we will see later, can be amplified by using the combined resources of another network. By doing this, an attacker can flood even the largest networks with relative ease.

If a criminal is going to DoS someone, they will most likely execute it from a system they have already "Owned," however, it is not uncommon for an attacker to deny service from their personal internet connection using a spoofed IP address. The frustrating part of this type of attack is the fact that it is based on a fundamental flaw in TCP/IP architecture: the substandard way in which systems handles SYN requests.

Resource Theft-

What if an attacker feels the need to DoS someone but doesn't have either an Owned system to send from, or a network connection capable of overpowering the target? Never fear, someone's already thought of that. A resource theft attack overutilizes access that the criminal already has to a computer to hang or crash it by using all the available memory or overtaxing the CPU. For example, an attacker could spawn multiple executions of freecell on a computer, therefore using all of the available system memory. This would result in a computer not allowing any more processes to be run, and denying service to legitimate users.



Flawed Programming-

There are other types of attacks that make full use of programming oversights. The Pentium f00f attack allows someone to crash any x86 environment by executing the bogus instruction 0xf00fc7c8 because of a flaw in Pentium microprocessor programming. We know that it is possible to execute commands in a bufferoverflow situation, and this type of attack is based on that principle. For those who may not be familiar with the term "buffer overflow," it is a condition that allows for code to be run (usually as root) by putting a greater number of characters than allowed for into a variable. The most common occurrence of this is when a program inserts data into a buffer without checking its size.

DNS Cache Poisoning-

It is also possible to alter a router so that it redirects all incoming traffic to an unintended location, either through the attacker's system, or into a non-existent one. DNS attacks or "cache poisoning," occurs when a DNS server is tricked into resolving an unintended location. An example of cache poisoning would be if someone redirected all the traffic intended to go to www.stankdawg.com to www.disney.com therefore denying service to www.stankdawg.com. Also, it is possible to redirect traffic to a non-existent network or "black hole." An example of this would be sending all incoming traffic meant for www.oldschoolphreak.com to be sent to an arbitrary address, essentially erasing www.oldschoolphreak.com from the internet. This could go undiscovered for days, until the host notices their hits went from 5000 to 0!

A LOOK AT CANNED DoS ATTACKS:Smurf-

Smurf is a self-amplifying attack that uses directed broadcasts to crash a network. There are 3 players in this scenario: the criminal, the amplifying network, and the victim system. What happens is that an ICMP ECHO packet is spoofed to appear as though it were sent from the victim's system to the amplifying system's broadcast address. Here's where the shiznit hits the fan. Every box on the amplifying system that is configured to respond to a broadcast ping request will respond to the victim system, thereby flooding it with responses, and shutting it down. To keep your system out of the amplification business, simply disable directed broadcasting at your border router. To keep from getting "Smurfed," limit incoming ICMP and UDP at your router to only those systems that need it. If you find your system on the business end of a DoS attack, get with the amplification system, and use a tool like MCI's "dostracker" to trace the attack to its source.

Fraggle-

Fraggle, a variant of Smurf, is a DoS mechanism that uses bogus UDP packets, to port 7 (the echo port), as opposed to Smurf's ICMP. The advantage over Smurf, if you want to call it that, is that if a box on the amplification system is not configured to respond to UDP, it will send back an error message that will consume bandwidth.

DDoS ATTACKS:

In February of 2000, the long theorized DDoS attacks came. EBay fell, then CNN.com, then 5 other major systems and a myriad of minor ones came grinding to a halt. DDoS attacks require more forethought than DoS attacks, but that doesn't make them any harder to accomplish, or any less common. The difficulty is in Owning the systems themselves!

There are 2 parts to most DDoS scripts, the client (used by the criminal), and the servers (placed on unwitting or already Owned systems). An attacker will place the server software on as many computers as possible, making them his "zombies." Then, when the attacker feels the time is right, the zombies will execute the attack command, using their resources, and IP addresses, to shut the victim system down.




The first DDoS attack mechanism was written for *nix systems by "Mixer." The "Tribe Flood Network" offered all the standard DoS attacks, and sported a TCPbound root shell. After TFN was shown to be effective, the look-alikes hit the scene, all attempting to offer better features while simplifying the process even farther. Trinoo and Stacheldraht are 2 major players in the post-TFN market. Of the 2, Stacheldraht is the most stable and lethal of the DDoS programs. Offering ICMP, UDP, SYN, and smurf-style attacks, encrypted telnet sessions between client and server, and the ability to blind network-based intrusion detection software, Stacheldraht is the leanest, meanest way to hose a network almost anonymously.

LOCAL ATTACKS:

There are a number of local attacks, but they are not very popular. Also, they are all but outdated. These examples are more aptly defined as "exploits," but I mention them here because they can lead to a DoS situation, even though they are distant cousins. On NT 4.0, there is a way to fill %systemdrive% by exploiting disk quota functionality. In Linux kernel 2.2.0, a local attacker could use the munmap () function call used by ldd to overwrite key areas of the kernel memory, causing a kernel panic.

In closing, remember that the key word in "denial of service" is DENIAL! It's not always a matter of using brute force to shut someone down. Almost always, the most effective attacks are also the stealthiest. If you want to learn more about DoS attacks, try them out on YOUR OWN system. Learn safely, and have phun!

SHOUTS:

StankDawg, who for all the editing is hereby officially promoted to co-author, dual_parallel, and everybody at www.stankdawg.com and www.oldschoolphreak.com. 

0101



-----*

* 2600 Secrets - by: nick84 & StankDawg @ DDP(www.stankdawg.com) *

-----*

Recently 2600 has been including a number of secret / hidden messages on certain pages within each issue, which this article aims to outline. Be forewarned that there may be "spoilers" here that you may not want to know in case you insist on finding them all on your own. This list starts with the first issue of year 2000.

~~~~~

Page 33 - Each issue page 33 will not be listed as such, as the number 33 will be cleverly disguised in various ways. In issue 19.4 the editors of 2600 wrote the following comical reply about it: "we get more mail on this than any other subject by far. And yet, everyone who writes in seems to know what page number they're talking about even though they claim the page information is faulty! It defies all logic".

Previous Page 33's

-----

- 17.1 - Date listed as "spring 0" instead of "Spring 2000" (\*NOTE\*: this issue had several different page anomalies similar to the ongoing page 33 fun. This was the first issue that the phenomenon started and appears to be a running joke that there is an existence of a "Y2K bug" still lingering in the 2600 computer system right up to this day.)
- 17.2 - Date listed as "Summer 19100" instead of "Summer 2000"
- 17.3 - Date listed as "Fall 0" instead of "Fall 2000"
- 17.4 - Date (Winter 2000-2001) covered with a black (censor?) bar
- 18.1 - Omission of date "Spring 2001"
- 18.2 - Mirror Image
- 18.3 - Replaced "Fall 2001" and "Page 33" with their respective rot-13 translations of "Snyy 2001" and "Cntr 33".
- 18.4 - Omission of the date "Winter 2001-2002" and the word "Page"
- 19.1 - Unknown hieroglyphics, possibly Wingdings font
- 19.2 - XXX & III
- 19.3 - 33 dots/periods
- 19.4 - Upside-down top right of page.

~~~~~

Index Page - The index page usually contains a hidden phrase/message, or picture:

Previous hidden content on the Index Page

- 17.1 - ???
 - 17.2 - ???
 - 17.3 - ???
 - 17.4 - "Ya Basta" beneath the word May (Ya Basta = "practical anarchism")
 - 18.1 - ???
 - 18.2 - ???
 - 18.3 - the word "rebuild" in the bottom center
 - 18.4 - ???
 - 19.1 - ???
 - 19.2 - the word "think" above the word "comprehensive" in line 2
 - 19.3 - IP address 166.112.200.202 [citizencorps.gov] under the word "monitoring"
 - 19.4 - "Kevin is now free" (above "positivity")
- ~~~~~



Front Cover - Covers have been known to contain hidden words/meanings/Significance:
Previous unexplained or hidden content on the Covers

-
- 17.1 - A silhouette of 3 people in a movie theatre. The 3 people look strikingly similar to Bugs Bunny, Darth Vader, and Mickey Mouse. It is a protest over the lawsuits against 2600 by the MPAA. At the bottom is a picture of a VCR with the buttons labeled with the words "awareness" "unity" and "power". The DVD logo has the word "tyranny" in it and there is a "REJECT" button next to it.
 - 17.2 - Although it was not known at the time of publication, these were scenes from the documentary film "Freedom Downtime" about Kevin Mitnick and the film being made about him.
 - 17.3 - A handcuffed individual wearing an H2K shirt with the phrase "VOTE NADER" seemingly tattooed on his arm. His hand holds a Motorola cel-phone with the number "3479379686" and the time "8:06" on it. The number was actually the decimal representation of the 2600.com website at that time. It has since changed.
 - 17.4 - The BellSouth building at night with the Batman symbol in the sky behind it.
 - 18.1 - A courthouse with the saying "Equal justice under law" is guarded by police officers in riot gear. A "Save WBAI" bumper sticker is on the steps. WBAI is the station in New York that broadcasts "Off The Hook". The scene poses the question: How can there be equal justice under the law, if the law is no longer accessible to the people?
 - 18.2 - The 2600 van in front of the Ford building with the name of the building altered to say "Ford Really Sucks" as a protest against Ford and other companies threatening legal action against sites that register names using the company's name a negative manner. Reflected on the windshield are IP address ranges that are owned by Ford.
 - 18.3 - Picture of Dmitry Sklyarov superimposed against the New York City skyline. The picture was taken before September 11. IF you hold the book at an angle so that the light bounces off of it just right, you can see a peace sign formed on the glossy paper just below the 2600 logo in the open sky.
 - 18.4 - In the background is a road sign reading, "Do Not Enter - Except Authorized Vehicles". The foreground quotes a statute that demonstrates how liberal and vague that laws can be written so that they infringe on our civil rights so badly that we might as well not take any actions at all at the risk of breaking some poorly worded law.
 - 19.1 - Several hidden words from the top down including: Cyber Crime Treaty, Infinite Justice, WTO, RIAA, Code Yellow, CARP, FCC, C(B/D?)DTPA, CH(???),DNA, MPAA, USA Patriot, Axis Of Evil, DMCA.
 - 19.2 - Map of open/closed wireless networks in Manhattan, New York City.
 - 19.3 - Picture in front of the White House. The jar labeled Tips is named after a controversial Orwellian like program in the United States. The jar contains social security cards, a US passport, a phone bill, a copy of 2600 issue 19.1, 2 diskettes labeled "evidence", a roll of film, and a plane ticket. Being placed in the jar is the US constitution which symbolizes the loss of our civil rights, particularly privacy, to programs like this.
 - 19.4 - Believed to be the face of Emmanuel Goldstein from 1984 on the Blinken lights project building.

~~~~~  
So go back and dig up your old issues of 2600 and see if you missed any of these little hidden secrets. I am sure they are not done yet!







# cin>>feedback

email your questions or comments to: [letters@binrev.com](mailto:letters@binrev.com)

## Comment:

"I've been interested in hacking since I was 9. I started with VB v3(I think) making AOL progs and trying to find someone who knew hacking me to take me under my wing. I talked to a few of them, same response from all of them: READ. Well, I couldn't understand what I was reading. Now I'm turning 17 and I get it a little more, however I'm still searching for that proverbial master to teach me to snap a fly out of his hand. I've been socially engineering since I was in middle school. In 8th grade I was the first one to send messages over the network via DOS prompt and make music. I did it all blind, not knowing what I was typing would do anything. Then with a new computer system in play, I was the first one to bypass security, warez games onto them, and at the end of the year, flood the system with a virus of my friends creation that fills the computer with random files of random suffix (.exe, .cfg, .wiz, .hlp, etc) so they couldn't find file and delete them at once. Eventually this filled every computer in the school with SHIT files and ate memory when the computer started. Then I fucked with the .bas files in the server and it went down. I don't know how long it took them to clean what I did, I never went back. This again, all without knowing what I was doing. I socially engineer every chance I have. All over my high school I watch security, bullshit teachers and administration. I really try without knowing what I'm doing. However, I still want to phreak and hack. I still haven't figured out \*NIX systems, I don't even know where to begin or how to install the fucking thing. I think I've found some accurate redbox readme's from PISS. Maybe. I'm going to go to Radio Shack and look around at the shit there. I need though, source. It seems like it's a giant community of underground social engineers using the art of phreaking/hacking to make their lives easier. I want in, badly. However I can't sort the 1970's articles from what's new. I can't find anything that's up-to-date with HOW TO and INTRODUCTION stamped on them. I want to find a leg in the door or at least some kind of newbie site. I very badly want to start phreaking since it seems the easiest to get into overall.

If you think you can help at all, please. I'm tired of this pretty school shit and engineering my way onto Wal-Mart PA systems. I want to get serious, I want to have a red box with me and be able to make a call when I want. I want to gator clip my way onto a phone line and make calls. Shit, I want to be able to get where I want. If you can help at all, thanks. And I'll register if I need to reply, which I hope I will."

-jp

## Response:

*Well, we welcome anyone here who wants to learn. I hope you do register and visit frequently. what people told you is true. You have to read a LOT, but here you can read and interact and get responses to specific questions. There are already tons of threads that will teach you a lot.*

*There are a couple of things that you mention that I think I should address. If you want to learn and experience real hacking, you need to first define what hacking is to you. I seriously think you should read our FAQ and read the very top of the Main Page. These are the things that we emphasize here.*

*You will find very little help with creating and distributing viruses. If that is your interest, you can find that information elsewhere on the web. While I am not totally opposed to it, I prefer to focus on more productive and positive things than destruction.*

*Red boxing doesn't work anymore. People can debate that if they want, but I believe it. "Gator-clipping" or beige boxing does.*

*As far as timeliness of information, listen to RFA (which you do), read the 'zines (many linked from here, just look for them), and visit the forums frequently. Our Articles page is up-to-date and I am in the process of putting dates on that page just for validity.*

*Most people work or go to school and hacking is a hobby. Unfortunately, you might not find a full-time "mentor" simply because of the time issues. Instead, you have found a whole forum full of mentors.*

*StankDawg*

## Question:

I was playing with my router and came across and option for a DMZ host. it didn't give to much of a description of what it was except that you can set an ip address for it... now if I set an IP for this would that open up my network?

Twirlz

## Answer:

*The DMZ is for some online games or media streaming that doesn't work to well behind a firewall. I know that some live QuickTime Server streams don't like firewalls too well, so you'd have to place your machine in the DMZ to get the stream properly.*

*Quoteth I from my Belkin router manual: \*ahem\* "Please note that when a computer is placed in the*



DMZ it is not protected by the firewall and is open to hacker attacks. Use this feature only when needed."

Huh. There's that "H" word again.....

All the machines on my network (except my server) get a dynamic IP address from the virtual DHCP server in the router. On my router, you assign the internal IP address of the machine you want in the DMZ and then activate the DMZ feature. It still uses the IP address that is issued by the router but turns off all the protection features of the firewall.

Logan5

**Question:**

How do nukers work and what are 'packets'. How would one make a nuker with Delphi?

D-AcE

**Answer:**

Wow! OK, I'll answer this one...

**PACKETS:**

A packet is the method of transportation of data over the internet. When you send an email for example, it gets wrapped up by your system into a "packet" that contains 3 parts.

Part 1 is the header record. It contains a few things, most important of which are the destination address, and the originating address. It also contains the packet number to keep similar packets together.

Part 2 is the data (sometimes called "payload") record. This is the actual data that is being transmitted. This would be your email text with formatting (or forum post, downloaded web pages, any kind of data...). If there is too much data to fit in one packet, it is split into multiple packets. Each individual packet has a header record which keeps all the parts together.

Part 3 is the footer record. It basically contains the EOF (end of file) marker for the packet. It also contains error checking to make sure the packet is intact upon arrival. If one packet is damaged, the entire message doesn't have to be resent, only the damaged packet needs to be resent.

That is a very basic explanation. There are specific sizes for each packet segment and explanations for them all over the web. Just understand how they work for now.

**NUKERS:**

As far as I know, this is a slang term for DoS (Denial of Service) tools. They send out multiple packets to a specific site. They can take various forms, but they all work similarly. They manipulate the packet to do a couple of different things.

1) They simply send out millions of tiny packets with

little or no data hoping to overload (or NUKE) the target router/system.

2) They send out packets with intentionally damaged records so that the system has to try and recover the bad data causing a huge amount of stress on the target router/system.

3) DDoS (Distributed Denial of Service) use either/ both of these methods but they reside on multiple attacking machines. Instead of 1 machine attacking (which 99.99999% of the time is not powerful enough to take out entire routers anymore) they use multiple machines to all attack at the same time, synchronizing their attacks and NUKING the router/system in question.

IP Spoofing is usually a topic here, which is the concept of tricking the header record of a packet to reflect a FAKE originating address so that the attack is not traced back to the attacker. This makes it difficult to defend against, but easy to route away from (use another/backup router that is not being attacked to maintain availability while the attack is analyzed and traced).

**HOW TO MAKE A NUKER WITH DELPHI:**

Don't. You will get arrested. Almost all DoS attacks are traced and found. Header records and logs will always show traces of your attack. They are largely ineffective now anyway.

HTH! further reading...

<http://www.howstuffworks.com/router.htm>

<http://www.howstuffworks.com/question525.htm>

<http://www.howstuffworks.com/firewall.htm>

StankDawg

**Question:**

I want to switch to Linux, but I don't know anything about it. So before I use a lot of money on an operating system I don't know, I would like to find a free version of it, but where can I find it?

Cr4X

**Answer:**

You can download almost any Linux distro for free. <http://linuxiso.org> If you don't have a CD burner a lot of places will burn CD's and sell 'em for a few bucks. You could also find your local LUG (Linux user group) here ... <http://www.linux.org/groups/index.html> ... and drop than an email. I'm sure someone has an old set of CD's they can let you borrow/have.

BoBB

**Question:**

Help, does anyone know the basics behind finding info out all the way up to taking over websites? Basic or hard, or even places that has EASY to read info, I can't stress that enough? Cheers...

-Insu



**Answer:**

*There is no easy trick to hacking websites. That is a myth. You have to understand the website and their structure and look for weaknesses. It is a case-by-case basis. If it were easy enough to have a set of instructions, then everyone would be doing it.*

*There was a phase during the early years of the web where many sites (mostly pr0n sites) would use the same hashing algorithm to authenticate users. Or they used a simple nonencrypted database to store users and passwords. In these cases, hackers wrote tools to do simple lookups or even ADDS to the database to allow access. This was an app you would download and it would work on those sites that used that SPECIFIC type of database or algorithm.*

*Obviously, the pr0n companies put a stop to this quickly. Now most sites are different or use more secured systems so that there are no "magic" tools to hack any web site. You may get extremely lucky and find some moron who is running an old setup that these may still work on, but that is doubtful. If you want in, you will have to find a backdoor and it will only work on that particular system in most cases.*

*For one sample of basics, try my article on basic directory transversal at <http://www.stankdawg.com/articles/>*

*StankDawg*

**Question:**

*I'm trying to find a music ripper to rip some old tapes of mine, but all I can find is CD rippers. ...would a CD ripper work if I was ripping a tape? ...also, after you get done recording is your wav suppose to sound all choppy or will the mp3 conversion fix that? because if not then I have a 1 gig wav file!!! if not what would I be doing wrong. I've been playing with audacity and I don't know what I would be doing wrong.*

*Twirlz*

**Answer:**

*OK. A .wav file is about 1 MB for every 10 seconds of audio. I think the reason your wav is choppy is because a gig of audio is a lot to ask of any system. trying to pre-cache that much raw data is going to give your box a hernia. try splitting your wav into more processor-friendly chunks and see if the quality is a little closer to what you want. Failing that, just convert the whole thing into mp3, that should reduce the size dramatically, and also the strain on your computer. If the conversion makes the quality better, it would be the size reduction's effect on the file. Also, there are good ways and bad ways to transfer a tape to your comp. The worst way is to hold a shitty mic up to the speaker on your boom box. The best way is to run an audio cable out of your stereo and into the line in jack on your soundcard.*

*bland\_inquisitor*

**Comment:**

*I keep notes on things I've been reading or working on. I think so would you, if possible I'd like to get a copy of what you've gathered over time on CD or paper. It would be a big help since I see you've been in the scene for awhile. Only looking to widen the horizon, if you now what I mean. I have good intension and don't mean no harm. I'm not a cop or anything affiliated with one. Just a guy that likes hax0r and wants to learn more. What I really want to read about more then anything is on Linux. I'm done with the books I just want some thing raw. Get back to me if you can, if not well delete peace.*

*Metadox*

**Response:**

*We keep a huge resource of information in the Digital Dawg House at [www.stankdawg.com/forums](http://www.stankdawg.com/forums) as well as an archive of all DDP member articles at [www.stankdawg.com/articles](http://www.stankdawg.com/articles) that are available to anyone. Our forums are a great, searchable source for information. If you cannot find what you need, feel free to post question in the forums, where we do our best to find an answer.*

*StankDawg*

**Comment:**

*hello there,  
I was inquiring about joining. Well, I would just like to meet other hackers that i can discuss things about. I am located in Tokyo, Japan. I noticed you mention your group is international and was wondering if you had any contacts in Japan I could meet? I have been programming since I was 11 and have had a great love for computers (and exploiting them. Finding out how they really work) since that time. I am getting into assembly, disassembling, and cracking but could really use some guidance. Well, let me know the good word.*

*Izzy*

**Response:**

*You don't have to join DDP proper to hang out at the site and in the forums. Yes, DDP has members from around the world, but we also have forum members from all over the world as well. There are regular hits in my logs from Japan so someone is visiting from Japan besides you. By all means join the forums and introduce yourself and you will not only meet others from across the world, but possibly meet other hackers in Japan as well. We love hearing the world perspective on hacking!*

*StankDawg*

**Question:**

*Ok, so I'm reading all this stuff about beige boxing and some articles explain some stuff differently than others. I opened up this box on the side of a (uh...my) house and there were like these*



four screw lookin' things

[0] [0]

[0] [0]

Kind like that, and there were some white colored wires in there too. Is this what I'm lookin' for?

Jeremy Renault

**Answer:**

Sounds like you have an older 4-post protector outside your house, in lieu of a TNI - Telephone Network Interface. The wires may not be red and green. Just take the alligator clips from your beige box and touch them to the posts until you get dial tone (feel free to check the voltage with a DMM if you're uncomfortable).

dual\_parallel

**Question:**

I want to set up a personal website totally disattached from my biz website. I'm faced with two options of where to host it. I REALLY want to host it myself here at home, since I have a G4 running OS X Server and it's more than up to the task. I'm really itchin' to do it that way, for the experience and leaning process, but I deally I'd like to register a new domain name. My problem is that my ISP does not allow hosting sites on a residential account nor do they have the option for using a static IP address with a residential account. I can use a DNS alias to point to the web server, so that's not really an issue. If I want a static IP address and having a "legal" server, I'd have to bump up to a Business Class account which is over \$100 a month, and I'd have to pay a monthly fee for the static IP address.

I \*could\* just set the site up on my server at home and hope that <my ISP> doesn't notice a spike of bandwidth usage coming from my account. But with my luck, they would pick up on it and it and shut me down....site, account and all. I could also set up a second hosting account with the hosting company where by biz site is hosted...that's only \$100 a year. But that means I don't get to play with my server.

So, can anyone give me an idea how much traffic there would have to be before <my ISP> picked up on anything? Does anyone else host their own site on an ISP account that they're not supposed to? Just curious on anyone's experiences in a similar situation.

logan5

**Answer:**

logan5, I have had 2 websites on my home server. I use **dyndns.org** to handle the name deal, since i don't have a static IP.

I was running both of the websites, (**digitalrights.org** and **animeshift.mine.nu**) from my home server. **digitalrights.org** brings in (on a good day) between 300 and 800 hits a day. I can almost say for sure they will not notice the bandwidth spike. do you run p2p? p2p is

the biggest bandwidth hog ever. you'll transfer MUCH more data if you are running p2p than you will just running a web server.

I use <Cable ISP name> as my provider. They have never said a word about it. and it clearly states "No server of ANY kind" in the TOS: I say go for it. worst they can do is kick you off.

Bi0s

**Question:**

I would like to start writing articles for the Digital DawgPound. I am wondering if I can submit them some where. Do u know where?

Rogue Operator

**Answer:**

Well, what a great, timely question this is! With the onset of our official DDP zine, we now open the doors for article submissions. This first issue was filled with articles by DDP members alone. We have written for many different 'zines in the past from 2600, to outbreak, to radical future, to frequency. With the onset of our new zine that you see before you, we now find ourselves in the position of accepting article submissions. Send any article submissions to [articles@binrev.com](mailto:articles@binrev.com) and we will get back to you ASAP with information on using your article. If we cannot use it for whatever reason (such as a full issue already committed) we may know someone else who can use it before it gets outdated and put you in touch with them.

StankDawg

**If you have questions or comments for the letters page, post them in the forums at <http://www.stankdawg.com/forums> or email us at [letters@binrev.com](mailto:letters@binrev.com) and maybe you will see your name here next issue!**

StankDawg



A NUBIE'S GUIDE TO:

# GHETTODRIVING

By: [StankDawg@hotmail.com](mailto:StankDawg@hotmail.com)

## INTRODUCTION:

Back in the early days of hacking, we had a term called "Wardialing" which referred to the act of dialing large sequences of phone numbers with a modem with the hopes of finding an open modem on the other line. If a modem picked up, you would then see what kind of access you had on the other end, and try to access the computer on the other end. Now, a new form of the same style of attack has appeared. It is called "Wardriving".

Wardriving is the act of driving around in a car, with a wireless access card, and looking for open wireless networks. Wardriving has a subset known as "Ghettodriving". Ghettodriving is a term first coined by dual\_parallel of the Digital DawgPound (DDP) and quickly adopted by the rest of us. It refers specifically to a very quick and inexpensive version of wardriving. Basically, "we of the ghetto" cannot always afford the most expensive laptops, wireless cards, and antennas (which is very important in increasing the range of your scanning). Ghettodriving is about making due with what you have. This is a guide to how to get out and about and ghettodriving with a low initial cost as quickly and easily as possible.

## STEP 1: HARDWARE

Ok, first of all, you need a laptop. It does not have to be a powerful system! You can find a used laptop for 500 bucks and it will most likely work. All it needs is a way to pick up wireless signals. That can be through PCMCIA cards or USB adapters. If you really want to get technical, you could actually use a full sized desktop and monitor if you really wanted to lug it out into your car. This would require a special power setup to maintain power to such a large machine, and basically drives up the price. This defeats the purpose of ghettodriving. It will also make it more obvious to you and get you busted easier.

In addition to a cheap laptop, you will need a device to pick up the wireless signals. Most commonly, this will be a wireless PCMCIA card. Generally, most cards are supported by the latest versions of the software (see "STEP 2" below) but you can always check it out on the web before you purchase one. If you are using Windows XP, which is what this guide is mostly geared towards, you have a better chance of the card working since generic drivers for Windows XP are available.

Another possibility is to use a USB wireless adapter from your USB device. I have tried this and it does work. The benefit is that older laptops may not have PCMCIA slots. You also simply may not want to purchase a PCMCIA card for whatever reason. I had a USB adapter for my home network, and I used it for ghettodriving until I was able to purchase a PCMCIA card. The obvious drawback here is that you have this bulky USB cable and adapter hanging off of the side of your laptop. It is not a big deal to get started, or if you are truly driving and not moving or picking the laptop, but eventually, you will want to stop somewhere and use the laptop and the extra piece of hardware will annoy the hell out of you. Especially if you get out of the car and begin "warwalking".



GPS (Global Position System) devices are a luxury that Ghettdrivers can forego. These devices will add extra information to your Ghettdriving. Specifically, they can add latitude and longitude readings for each wireless network you find. This is helpful to pinpoint the exact location of networks that you pick up. Usually, you will know your own scans and save them with well chosen filenames to make them recognizable. When you start sharing your information with others (see STEP 5), they may need more precise information.

Antennas are another optional step, but these are generally unused by ghettdrivers. They are sometimes expensive, and the point of ghettdriving is to keep the cost down. You can find many places on the web to research how to make your own antenna, but it will require some time and knowledge. A better alternative for the ghettdriver with a budget would be to purchase one of the models of PCMCIA cards that has an opening for an external antenna built onto the edge of the card. Both Orinoco and Cisco make models like this with many more companies following suit.

## **STEP 2: SOFTWARE**

Again, since this is geared for nubies, I am going to focus on the Windows XP environment. The software of choice for Windows XP is called “Network Stumbler” or “NetStumbler” for short. Always download the latest version to assure support for the greatest number of cards. Also, do not worry if your card is listed under the unsupported list. As I said earlier, Windows XP and NetStumbler provide generic drivers that may detect your card just fine even if it is not listed as a supported card.

There are also good clients for Linux. The most notable is “Kismet”. If you are familiar with Linux, this might be the best way to go since Linux also has a few more tools and utilities for cracking. If you do not want to commit your entire laptop to Linux, you can also try the Knoppix distribution, which boots and runs entirely from the CD.

Also, since ghettdriving is about making due with what you have, I would be remiss to mention what do to if your card is not supported by NetStumbler or Kismet. Since Windows XP wireless networking is set to always listen for WAPs anyway, you may simply need the client application software that came with your wireless card. With this installed and running, you can simply use the built-in Windows XP wireless support to find wireless networks. There are other packages like aphopper that may work in a pinch as well. It is not as friendly as having a dedicated app like NetStumbler, but it will work, and that is the bottom line.

NetStumbler installation is straightforward. Once you install the software, you simply start the application and it will begin “sniffing” for Access Points. As you move around, and come in and out of range of wireless network, NetStumbler will detect and notify you of the network. At this point, you are up and running, but it is important that you understand a few more things before you go further.

## **STEP 3: UNDERSTAND HOW IT WORKS**

Wireless Access Points, or WAPs (or even simply APs) work on radio frequencies using basic radio wave technology. It is not much different than the way that your car radio works. Radio stations send out an extremely strong signal that gets picked up by your car radio (thus the need for an antenna). This is the same way that wireless networking works, only on a smaller scale. The radio station has a set frequency that you dial in on your radio tuner and it is sent out from an enormous broadcasting tower. A Wireless Access Point sends out a constant signal at a set frequency. The only real difference is that 802.11 has a much smaller range.

Since you know that the WAP is shouting out its availability all the time, just like a radio station, common sense tells you that you must be able to dial into that frequency, just like a



radio station. You got it exactly! That is the fundamental principal in Wardriving. The programs mentioned in the software section above are simply listening devices that are tuning in to the 802.11 frequency and waiting for that signal (or station) to come in. When you come within the vicinity of an Access Point, it lets you know.

The software will indicate to you when it has found a wireless network shouting its availability. Since you have a wireless card, and they have a wireless access point, you can now become a user on their network. There are a few more details and or restrictions as explained below, but in the simplest form, and in a basic insecure (and very common) setup, you will have full access to the network!

#### STEP 4: ACCESS!

What does that mean? Well, there are some factors that can establish and/or limit what access you do have, but generally, you will have a lot of access to that network. When a typical home user sets up their home network, they are doing it for the purpose of having easy and convenient access to the internet. A typical business will set up their wireless network to be both easy to maintain and easy to access for its employees. To that end, they usually leave the access point wide open so that when they set up computers in their home or business, they can easily set it up and be off and running. Their laziness is our gain.



When you drive or walk into the wireless network range, you are no different than a computer sitting in their office. Most of these networks have DHCP turned on and anyone connecting to the network gets a generic DHCP address assigned to their computer for routing purposes. With that address, you are now a node in their network. If they have internet access turned on, which they almost always do, you have the ability to sit in their parking lot and surf the web or check your email on their bandwidth.

There is an exception to this rule. There always is. In the example I just walked you through; we made a lot of assumptions on availability. These assumptions are true in more than 50% of networks that I have found. Sometimes, however, you will find that the person has turned on WEP (Wired Equivalent Privacy) encryption. WEP encryption requires that all client systems on a network know the WEP key to gain access to the network. Think of it as a long password. For Ghattodriving purposes, WEP enabled networks mean that you shouldn't even bother with that network. There are software packages that will attempt to crack WEP encryption, but Ghattodrivers are usually just looking for quick access. If WEP is enabled, it is easier to simply find another wireless network without WEP turned on and use it instead.

There is another reason that Ghattodrivers don't usually bother with WEP enabled networks. It is a legal issue. While it is currently legal to locate and acknowledge the existence of wireless networks, it is **ILLEGAL** to **ACCESS ANY NETWORK WITHOUT PERMISSION!** Even if WEP is turned off, it is still illegal to access a network, wireless or otherwise, without permission. Frankly, in most circumstances, it is near impossible to be discovered, but this is not in any way, shape, or form insinuating that you break the law! It is just pointing out a matter of fact. If someone goes to the effort of implementing encryption (and possibly other forms of authentication), they obviously are **NOT** giving you permission to access their network. This being the case, Ghattodrivers choose to skip them. Even though most Ghattodrivers feel that it is harmless to piggyback on someone else's bandwidth to do a web search for information or to do a quick check of an email account, they will not generally force

their way into a system. It is a grey area that borders a very illegal border, so each person must draw their own lines and set their own limits on how far they will go. The legal line is crossed upon actual access of the network.

Also, just for informational purposes, once you are on a network, you may be curious as to how the network is set up or who the network belongs to (so you can thank them). Since you are another perfectly established node on that network, you can use network tools just like any other network client. Utilities like LANGUARD and AIROPEEK can be wonderful for researching the network. You might come up with many other creative ways to use your newfound access, but again BE CAREFUL. You may be doing something that, while it can be harmless, may technically be illegal.




## STEP 5: RESULTS

As you Ghettdrive, your results are maintained onscreen until you close the program. Once a network has been found, you can save the information to a file which you can access later. Maybe you take a trip to Disneyworld once per year. Each time you go back, you now know the locations of places to access the internet without starting all over again. Or you can share the file with a friend who is going also. You may have the need to jump online and lookup prices for something from the parking lot of a store before your purchase. You may want to check for an email from friends regarding where they want to meet you in the park. The uses are endless!

You can also upload the results of your Ghettdriving to many different sites online. Instead of giving a list of these sites, you will be better off to simply go online and search for sites that you prefer, perhaps something local. Sharing with a few friends is useful, but can you imagine sharing information with the whole world? Not only will your friend know where to go, but now, so will anyone else who wants to visit Disneyworld! People can get online before buying tickets and make sure the reseller is legitimate and not a con artist. Publicly releasing information will actually raise the consciousness of society. I'll bet some of you reading this never realized that hacking can produce such awareness and contribute to the betterment of society on such a grand scale. Maybe hackers aren't so bad after all!

## CONCLUSION:

In summary, this is one of the most fun things to do since Wardialing. Finding places to get internet access in such strange places as parking lots and highways is an amazing feeling. If you understand how it works, and know where they lines are, you can safely, and legally, explore the world on a whole new level. You will never look at your neighborhood the same again! 







# phreakin' italy!



By: w1nt3rmut3

**A** fairly universal topic, phreaking. The phone system here is very different than the one in the states, well at least in Rome. The pay phones are run by basically the same company, Puntotel. The big diff is that 99.9% of the phones are used by cards, not coins. Coin ones are very rare. The cards come in multiple sizes, ranging from 2.50 euros, to 10 and higher. They are also all the same exact type, except some take just cards, and some take cards and coin. They also have a lot of features, besides talking. They allow for SMS, email, and fax. emails run for about 20 cents, and the SMS is, I believe 10 cents, but I cant use it, b/c it can be only used to message European cellies. A normal call would go like this:

- 1) pop the card in
- 2) pick up the receiver
- 3) dial the city code your in (06 for Rome)
- 4) dial the number

That's for intra-Rome. Its akin to 10 digit dialing in the states. then, you press the fat OK button. The other funny thing is that it doesn't dial until you are done typing in the number. Its sorta like dial tone emulation on some pay phones, where it waits for the whole number then dials. One big difference between Italy and the states is that numbers can be of any length.

USA: 1 + NPA + xxx + xxxx

Rome: 06 + whatever length you have



photo by w1nt3rmut3

Its sorta like a step-by-step, taking in the digits as it comes. Oh, and in case your wondering the dial tone is totally different. Its a beeping, about a second long, and a second of silence.



## **ODDITIES:**

### *4-digits*

You have heard numbers on the radio like dial star something on your Joe Blow cell phone provider for requests on some Clear Channel station. They have something similar here, but for the land lines. Rome is a big tourist attraction, not to mention a big ass city, so you either turn to public transportation (a whole other file) or taxi. The taxis make it simple. Dialing 3750 or other 4 digit numbers give you instant access to a taxi company, or perhaps other companies, simplifying the extortion of your money.



### *Permanent Marker*

Something I have noticed on a lot of payphones is 3 digit numbers written on the sides. At first I thought this was isolated, but I looked around, and they're everywhere. My guess is there is some way to call the phones, but I have yet to figure that out.

### *Long-Distance Dialing*

I have been known to make long distance calls, and i need some help in saving some money, so I use 101's for that in the states, but

you gotta go for the cards here in Rome. Stumbling upon a phone shop, they offered me 100 minutes to the states for 5 euros. What a deal. After making some calls, I soon find out that the card has gone from 80 minutes, to 30 minutes. WTF? Thought it was just a glitch. But after buying more, I start to get only 30 minutes, not even a "100" to begin with. My guess is the company that produces them, Vectone, either knew I was coming, or the such proliferation of the cards forced their value down, and in turn killed the minutes. I did find the 800 number busy 50% of the time. BTW, u wanna the number?

800-969-572 (yes, that's 6 digits)

PIN: 9912 723 6971

Good luck using that in the states.

### *Closing Arguments*

So, its all good here in Rome, except for the long distance. If anyone can figure out the 3 digit numbers on the phones, or run into one of my PLA stickers, (bright green), drop me a line at: [w1nt3rmut3@binrev.com](mailto:w1nt3rmut3@binrev.com)

See ya! ☺





“Turn that (computer) off... That cookie shit scares me.” -- Tony Soprano

**THE** cookie. Those little crumbs of code that allow sites to get to know you a little better have been elevated to almost legendary status by the media and the tech-savvy community. I hope here to shed some light on the subject; to tell you what they are, how they work, their limitations, how to get rid of them, and how attackers can use them to “get to know you a little better.”

*Disclaimer: This is information, not a license to harm someone. If you do, it's your bad.*

**WHAT THEY ARE AND HOW THEY WORK**

Perhaps it is best to start with what cookies aren't, as this seems to be the biggest point of contention. The first thing to realize here is that cookies are not programs. They CAN NOT sit on your box and record everything you do. Cookies are text files, and they have all the limitations of being a text file. Cookies DO NOT gather information about every web page you visit, because only a program can do that. Cookies are sent from a web server to your machine, and can be accessed by that server on future visits. Here is a cookie on my machine (that I have modified because it contains data that I don't want to share with the class).

member\_id

xxxxxx

[www.stankdawg.com/](http://www.stankdawg.com/)

123454365

123456

23456789

3456789000

12343432123

\*

pass\_hash

a-bunch-of-data-that-is-a-hash-of-my-password-at-this-website

[www.stankdawg.com/](http://www.stankdawg.com/)

123454365

123456

23456789

3456789000

12343432123

\*

The format of a cookie is the “name-value” pair. A variable is named, and an identifier is associated with it.



The first pair is member\_id. When I visit www.stankdawg.com the server sees that my member\_id is back, then that information can be stored server-side to show how many times I have been to this page, when I am most likely to visit, and so on.

The second pair is the site name; and the longer identifier, which is also unique, would most likely be used if I didn't have a member\_id. However, it is good for the Webmaster to keep in mind that since the cookie rests on my computer, I have the ability to monkey around with it. Basic hacker spidey sense would say, "Hmm, if I change my member\_id to 1, I might could log on as the admin, who would most likely be the first user to register." This leads me to another use of the long identifier. This particular Webmaster uses my longer, and harder to guess, identifier to authenticate me with the member\_id in the cookie at the server level to make sure nobody gets up to any shenanigans on the sly.

The third pair is pass\_hash. This is a Godsend for lazy asses like me. The pass\_hash pair stores, well, a hash of the password I have set on this site so I don't have to type it in every time I want to see what's going on at the forum.

This cookie is about the mid-range of sophistication; the most basic is just something like: **User: 53442758345621 www.oldschoolphreak.com** (this page doesn't use cookies, I'm just pimping a site).

There is a direct correlation I would like to draw here; the more "high-tech" a site is, the more information will be stored in the cookie. Any site that allows you to customize options will most likely store all those preferences in a cookie on your box. It's only fair; after all, if someone's going to let me tool around with their site, I'll shoulder the 100b burden.

### **COOKIE ABUSE**

The information stored in a cookie is pretty much innocuous when it pertains to simple site customization, but it's not necessarily information that you want everybody to get his or her grubby little mitts on. Some of the cookies you play host to are the only source of verification used on a particular site. It makes sense; servers can't always rely on an IP, because most people are on a dynamic system. So what would happen if someone were to get a hold of your amazon.com or eBay cookie? It's the most basic and overlooked form of identity theft out there.

Locally, stealing someone's cookies is about as hard as taking candy from a baby. The kind folks at Microsoft were benevolent enough to use C:\windows\cookies as the cookie jar for Internet Explorer. The same is true in a "remote" situation for people sharing root on a LAN or WLAN with you. Weather or not you're supposed to be on their network is another issue... It's a matter of jacking packets and looking for the almighty cuid= line, then replacing the boring old cuid in your cookie with the far superior one you have just borrowed. Bada Bing, you're now som one else.

There are several ways to get the cookies of Joe InternetUser, but the one I want to talk about is by far the most interesting.

### **THE PEACEFIRE EXPLOIT**

Click a link, and you're the prom queen of the Internet. Scary huh? The URL script is



located at [www.peacefire.org/security/iecookies](http://www.peacefire.org/security/iecookies) Go read the page for what it does, it's pretty damn cool. IFRAME it in an HTML-based e-mail, and it's a nightmare. Yes, there's a patch [www.microsoft.com/technet/security/bulletin/fq00-009.asp](http://www.microsoft.com/technet/security/bulletin/fq00-009.asp) , but it's still fascinating to see that kind of thing in action.

**COOKIES GONE WILD**

Companies like doubleclick perpetrate the most lethal, most insidious, most devastating form of cookie abuse there is. They have violated rule #1 in the bland\_inquisitor handbook. They mistook ability for authority. And on top of that, they seek to make a quick buck at the expense of our privacy. Here's the basic idea. What if a group of independent web servers used an ad company to place a generic cookie on your box that would "help" the members target advertising geared toward your personal browsing and shopping habits? This is dangerously close to something bad. The members place a "clear gif" on their page that links to the ad agency. When you access that picture, the ad company places or reads their cookie on your machine. They then match the refer ring site with your cuid, then add this information to their database. It's still ostensibly anonymous, but if you buy anything from a doubleclick member, they can match your cookie with the shipping information. At this point, they have you. All your browsed pages, all your online purchases, everything that you have done that is within the scope of the sites being doubleclick partners.


This is a direct quote from the doubleclick privacy policy:  
**"No personal information is used by DoubleClick to deliver Internet ads.**

DoubleClick does not use your name, address, email address, or phone number to deliver Internet ads. DoubleClick does use information about your browser and Web surfing to determine which ads to show your browser."

FUCKING NATURALLY they wouldn't use your name and address for delivering INTERNET ads, they say NOTHING about selling your name and address to telemarketers and junk mail purveyors. Item 4 of their privacy policy states:

**"DoubleClick encourages all companies with which we do business to engage in fair information practices."**

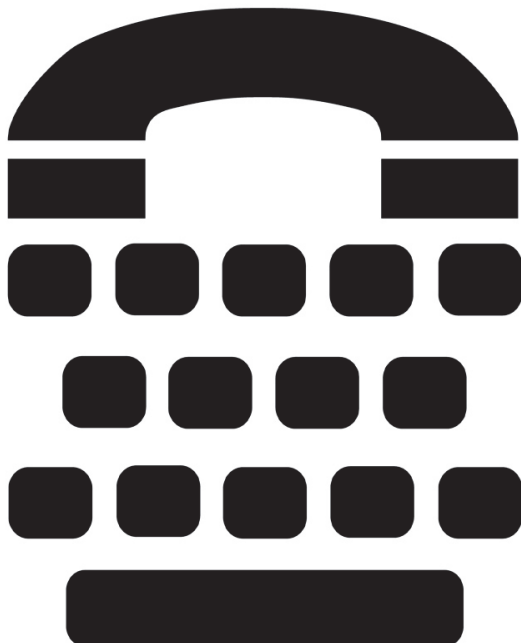
There is no penalty associated with "encouraged." Remember that.

Ranting aside, I hope that I have taught you something. As always, good security practices, and good implementation of those practices, can go a long way to keep you happy on the internet. 

**SHOUTS:** StankDawg, the DDP, dual\_parallel, and gratz to logan5



```
// Public TTYs: Description and Methodologies for Free Calling  
//  
// by dual_parallel  
//  
// http://www.oldschoolphreak.com
```



### Introduction

With the advent of widespread electronic connectivity, one might think that the deaf, hard-of-hearing and speech impaired (hereon called deaf) have unfettered access to limitless communication. Email, text and instant messaging are convenient, but access is not always possible regardless of disability. This is where public TTYs fill an important gap in accessibility.

TTY stands for TeleTYpewriter, or sometimes Text Typewriter. Teletypewriters are devices that enable the sending of text messages using modulation and have been used by hams for decades. TTYs formed the basis of the technology that is now the modern Telecommunication Device for the Deaf, or TDD. By convention, deaf TDD users call the devices TTYs.

The creation of the TTY began in 1964 when a deaf physicist named Robert H. Weitbrecht, with the help of others, decided that deaf people should be able to use the telecommunications system as easily as a hearing person. (The full story of the TTY's creation is told in Harry G. Lang's book, A Phone of Our Own.) This creation of a few men almost 40 years ago is still an important part of accessible telecommunications.

This article will address publicly available TTYs; legislation regarding their placement, the basis of their technology, and methods for making relay calls at no cost.

---

### Legislation

Enacted July 26, 1990, the Americans with Disabilities Act (ADA) protects the civil rights of the disabled. The four main titles of the ADA (Title I - Employment, Title II - Municipal Services, Title III - Public and Commercial Locations, and Title IV - Telecommunications) mention the use of



TTYs. The requirements of Titles II and III, which concern most public locations, can be summarized by the following:

- Newly built venues with four or more public pay phones, one being an interior phone, must have a TTY on site
- Existing facilities that are adding pay telephones to bring the total on site to four with one interior phone must have a TTY

Other regulations can be met with the inclusion of a shelf and power outlet at pay phones or courtesy TTYs.

Title IV, Telecommunications, creates the Telecommunications Relay Service (TRS) that exists in every state and is available 24 hours a day. Funding for TRS is normally collected as a surcharge listed as a "Telecommunications Relay Service Surcharge" on Local Exchange Carrier (LEC) phone bills. These charges pay for toll-free relay numbers and relay operators, or Communications Assistants (CA) as they are officially called.

---

### Technology

Public TTYs usually consist of Fortress or Millenium pay phones with an enclosed, motorized drawer mounted underneath the phone housing. When the TTY encounters TTY tones from a dialed number, the drawer will open to reveal a ruggedized keyboard and a one-line LED display. A red LED adorns the front of the drawer, which responds to data transfer, ringing and voice during conventional calls. Courtesy TTYs are usually acoustically coupled TDDs.

The basis of TTY technology is the Weitbrecht modem. The Weitbrecht modem uses Frequency Shift Keying (FSK) modulation and the Baudot code character set to transmit data at a rate of 45.5 baud (bps). Frequency Shift Keying is the use of two analog waves at different frequencies to represent ones and zeros. The Weitbrecht modem uses 1400 Hz for the mark (1) and 1800 Hz for the space (0). So as the TTY user types a message, the TTY converts the entered characters, using the Baudot code set (see Table 1), into the buzz-like beeping that can readily be heard.

Other standards for TTY communication exist, like Bell 103 and Turbo Code. Bell 103 transmits at 300 bps and uses the ASCII character set. Turbo Code transmits at 110 bps and, more importantly, transmits data as fast as the user can type and allows for conversation interruption like voice calls. Turbo Code is implemented in all Ultratec, Inc. TTYs, the most commonly encountered public TTY.



Table 1: Baudot Code

| Binary | Hex | LTRS         | FIGS  |
|--------|-----|--------------|-------|
| =====  | === | =====        | ===== |
| 00011  | 03  | A            | -     |
| 11001  | 19  | B            | ?     |
| 01110  | 0E  | C            | :     |
| 01001  | 09  | D            | \$    |
| 00001  | 01  | E            | 3     |
| 01101  | 0D  | F            | !     |
| 11010  | 1A  | G            | &     |
| 10100  | 14  | H            | #     |
| 00110  | 06  | I            | 8     |
| 01011  | 0B  | J            | BELL  |
| 01111  | 0F  | K            | (     |
| 10010  | 12  | L            | )     |
| 11100  | 1C  | M            | .     |
| 01100  | 0C  | N            | ,     |
| 11000  | 18  | O            | 9     |
| 10110  | 16  | P            | 0     |
| 10111  | 17  | Q            | 1     |
| 01010  | 0A  | R            | 4     |
| 00101  | 05  | S            | '     |
| 10000  | 10  | T            | 5     |
| 00111  | 07  | U            | 7     |
| 11110  | 1E  | V            | ;     |
| 10011  | 13  | W            | 2     |
| 11101  | 1D  | X            | /     |
| 10101  | 15  | Y            | 6     |
| 10001  | 11  | Z            | "     |
| 01000  | 08  | CR           | CR    |
| 00010  | 02  | LF           | LF    |
| 00100  | 04  | SP           | SP    |
| 11111  | 1F  | LTRS         | LTRS  |
| 11011  | 1B  | FIGS         | FIGS  |
| 00000  | 00  | ===unused=== |       |

---

Methodologies

The following methodologies will teach the reader how to make free toll or local calls from a public TTY. No matter what the circumstance, relinquish the use of any public TTY to any deaf person who wishes to use it.





The first method for making free calls with a TTY is to simply ask. Courtesy TTYs are widely available and people are generally more than happy to let a hearing person use one. The TTY will more than likely be an acoustically coupled TDD and the probability of making toll calls is low.

The second method concerns pay phone TTYs and is slightly more involved. There are a few prerequisites to make these calls: access to a TTY pay phone, a toll-free TTY relay number, a way to op divert, an ANI number and the number you are calling. General knowledge of IntereXchange Carrier (IXC) switching may be helpful. A tone dialer will not be mentioned because it is assumed the reader carries one at all times.

Now, TTY pay phones can be found at malls, airports, universities and other areas meeting ADA requirements (see Appendix A). TTY relay numbers for the 50 states and more can be found at:

[http://data.club.cc.cmu.edu/~red\\_trek/relay.html](http://data.club.cc.cmu.edu/~red_trek/relay.html)

There are many ways to op divert to toll-free numbers and many texts written about it. Published ANI numbers are also plentiful - a little research will go a long way. Regarding the number you are calling, DO NOT call a number associated with you. With info in hand, here is the method for making the call:

1. Op divert to an ANI number. If the ANI number does not read back the number of the pay phone, you have ANI fail and you can continue.
2. Op divert to a toll-free relay number.
3. The CA will ask for the number you are calling from. Enter a random, but realistic number.
4. You will then be asked for the number you are dialing and the call will be completed.

Note the number read back from the ANI number. There is a good chance it will read back the NPA of the IXC regional center and then seven zeros. To increase your chances of call completion, enter a number from that NPA.

The third method deals with telcos that use 711 relay service. Dialing 711 from a pay phone, or a subscriber line for a courtesy TTY, will automatically dial a relay op. From here, three things could happen. At a courtesy TTY you will be able



to make local calls like method one. Next, at a pay phone, the relay op could ask for the method of payment and no call will be made. Last and best, is that no ANI will be passed and the call will be completed similar to the second method. The final calling method involves TTY relay, but it utilizes public computers instead of telephones.

Publicly available computers are abundant; libraries, broadband company kiosks, demonstration computers, etc. And making a nationwide relay call is as simple as using a Java-enabled browser. AT&T Relay Service, found at <http://www.relay.att.com/national/relay.html> is a free, browser-based relay service provided by AT&T. Currently, only Windows operating systems are officially supported, with browser support limited to Netscape 4.7 and later and Internet Explorer 5.0 and later. Conversations are encrypted and can be printed for later perusal. Using the service is straight-forward: enter the number to be dialed, click Connect and you will be greeted by an AT&T CA.

Some pitfalls you may encounter include called party confusion from talking to a relay op and subsequent disconnection. Another obvious drawback is the relay op not believing you and not connecting the call. Other than that, these methodologies are effective.

---

Conclusion

Where hackers may seem preoccupied with breaking security, it may be easy to say that phreaks are only concerned with making free telephone calls. This is not the case. Computer security is just another fulfilling challenge that knowledge-hungry hackers cannot resist. Cost-free calling is a product of exploration - finding new and different ways to use telecommunications technology.

The technology of TTYs may seem basic, but their history, importance and current technological development make omission of TTYs in a phreak's repertoire folly. There are many advancements left to explore, like TTY printers, Voice Carry Over (VCO) and telephone captioning. Enjoy the technology of TTYs with the true spirit of a hacker.

---

Appendix A - Concerning Public TTY Locations

Unfortunately my LEC, Qwest, does not maintain a database



of TTY pay phone locations. Not to preach, but the Qwest Special Needs Center (400 Tijeras Ave. NW; Albuquerque, NM 87102; 800-223-3131) should be ashamed that something as simple as a list of TTY pay phones does not exist. I will concede that one Qwest employee said he would pass on the idea of a TTY database to his superiors. Until that time, I have taken it upon myself to compile of list of pay phone and courtesy TTYs in my local calling area. I will be sending this list to Qwest.

-----

Albuquerque International Sunport  
Qwest Millenium / Ultratec PPT1  
505-245-9092

Albuquerque International Sunport  
Gate A3  
Qwest Millenium / Ultratec PPT1  
505-245-9111

Coronado Center  
Louisiana & Menaul  
2500 telephone set / Ultratec Minicom IV  
505-872-8161

Cottonwood Mall  
10000 Coors Blvd. Bypass NW  
Qwest Millenium / Ultratec TTY  
505-898-9804  
(Inoperable!)

TVI Montoya Campus  
Wiley Hall  
Qwest Fortress / Ultratec PP2M240  
505-299-9750

Winrock Mall  
I40 & Louisiana  
Qwest Millenium / Ultratec PP2M120  
505-883-9403



Appendix B - TTY Abbreviations

ABT - about  
ASAP - as soon as possible  
ASST - assistant  
BIZ - business  
BLDG - building  
BYE - good bye  
CD/CLD/CUD - could  
CUL - See you later.  
CUZ - because  
DO-DO - What to do?  
DOC/DR - doctor  
EDU - education  
FIGS - figures  
GA - go ahead  
GA SK - about to hang up  
HD/HLD - hold  
ILY - I love you.  
IMPT - important  
LTRS - letters  
MSG/MSGE - message  
MISC - miscellaneous  
MTG - meeting  
NBR/NU - number  
OFC - office  
OIC - Oh, I see.  
OPR - operator  
PPL - people  
PLS/PLZ - please  
PRO - professional  
Q/QQ - question  
R - are  
SEE-SEE - Let's wait and see.  
SERV/SVC - service  
SD/SHD/SHUD - should  
SK - stop keying  
SKSK - hanging up  
THKS/THX - thanks  
THRU - through  
TMR/TMW/TOM - tomorrow  
U - you  
UR - your  
URS - yours  
WUD - would



# YOUR RIGHTS

and Why You  
Have Already  
Lost Them

BY: EVO\_TECH OF DDP

Most of us have already heard the story of Mike Maginnis, but please read through it one more time, if just to refresh your memory. And no, this article is not on Mr. Maginnis or on the USA Patriot Act.

Everyone remembers the story of Mike Maginnis, right? Well, the following information is what I have gathered from *www.2600.com*'s articles on this case. Apparently Mr. Maginnis was an IT professional that enjoyed photography in his spare time. A local of Denver Colorado, Mr. Maginnis mostly photographed the local skylines and parks. Mr. Maginnis was in the city one day taking pictures of the Adams Mark Hotel on Court Place, and the surrounding parks and buildings. He took a few photos, and headed back to his car.

This is where a Denver Police officer confronted him. He was asked to surrender his camera, and Mr. Maginnis refused, as he saw that he had done nothing wrong. The Denver police office then pushed him to the ground and arrested him.

He was taken to Denver District 1 police station on Decatur Street. He was made to wait in a room alone for several hours when finally, a secret service agent entered the room. The agent introduced himself as special agent "Willse". The agent began telling Mr. Maginnis that his suspicious activities made him a threat to national security, and that he would be tried as a terrorist under the USA Patriot Act. The agent told Mr. Maginnis that he had been taking those photos in order to analyze the security of the vice president and cause "terror and mayhem".

Mr. Maginnis denied all of these charges, as he was not guilty of them. At this point, the agent apparently became irritated, and began to call Mr. Maginnis a "Rag-Head collaborator" and a "dirty pinko faggot". After approximately an hour of interrogation, Mr. Maginnis was finally allowed his phone call. Instead of phoning his lawyer, he called the Denver Post. This was immediately over heard by the police clerk, and the line was cut off. Then Mr. Maginnis was placed into a holding cell. Several hours later, he was released.

Mr. Maginnis was told that he would not be receiving his Nikon F2 camera back, as it was being held for evidence. Maginnis never received any arrest papers upon his release. Mr. Maginnis quickly contacted his lawyer, who contacted the Denver police, who completely deny ever having him in custody, or any one looking like him.

Now, this is a bit frightening, is it not? The behavior of the Denver police and secret service is inexcusable. This mans rights were violated, and no one will be held accountable for it. It is being entirely denied, and Mr. Maginnis can provide no hard proof of the events. However, with the amount of hate e-mails and phone calls he and his parents are receiving, one would wonder why he would place himself in this position, if the events were untrue.

And now, how does this relate to you? Well, consider this. Many people in the country right now, including most of you reading this, feel a need for change on the government's level. This is a great thing to think, and I believe every one should follow through with their ideas and pursue what they feel is right. But be warned, don't think or do anything TOO revolutionary.

You see, everything has "shifted" so to speak, and not many really see it. You see the attempts by all to be suddenly "patriotic". After September 11th, you couldn't swing a dead cat without hitting an American flag. Which is really great, don't get me wrong. However, where was the patriotism of the American people BEFORE that September? Where were their flags then? This type of so-called "patriotism" doesn't feel sincere.

But, I digress. Now that this new and (in my opinion) largely artificial patriotism has emerged, the worst thing you can be accused of is being "un-patriotic" or a terrorist. Many public officials were quick to throw this new "horrible" label onto those in the hacker world. People will also now go along with nearly anything their government says, so long as they slap words like 'patriot', "anti-terrorism" or "homeland security" in front of whatever they want.

In all honesty, this scares the hell out of me. And it should do the same to you. This new popular



attitude gives the government nearly free range to bend and nearly break the constitution and bill of rights, wherever they see fit. Mr. Maginnis is a perfect example of this. He was placed under arrest, had his person and personal goods searched and seized, and all in the interest of "homeland security". All the man did was to take a few pictures. And his rights were quickly stripped from him.

Now, think if you started to make your attempts to change some things in your government. You begin to stage demonstrations. You begin to contact government officials. Now, in most cases, the government will largely ignore you, so long as they don't feel threatened by your movements. But let us suppose for a moment that they did begin to feel a bit threatened. Imagine how quickly they would bear down on you. And now, thanks to the new "patriotism" felt by nearly the entire country, you don't even have your rights left to protect you, or your family.

The simple act of speaking out against your government and its doings is pivotal to what it is that we believe in as a country. Free speech is one of our most prized rights as a nation. However, with the current opinions as they are across the nation, if you are not labeled as "anti- American" or "un-patriotic" by the news media, you will be by the people themselves. Free speech is gone.

And when your rights start to be violated, even if the people want to, they will not be of any help to you, as they will be too afraid of falling to a similar fate to you, and those like you. The fear of being "unpatriotic" has been put into the American people. Therefore, they will slowly become afraid of exercising those rights. Free speech is no longer an option.

And if you aren't using your rights, then why do you really need your rights?

You see, humans by nature feel a need for comfort. This comfort can very easily be seen in your "typical" American. This comfort has become something most of us tend to hold dear to our hearts. This comfort zone is the main reason why very few Americans will go any further than simply talking about their ideals and complaining about their government within the confines of their own homes.

When you step up, and begin to speak out for what you believe in, you are placing your comfort zone at

Amendment I.\*  
Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

risk. The people who believe you to be "un-American" can ridicule you, prank call your home, and fill your mailbox with endless hate mail. And this is their right, and not the issue at hand.

Once you take that next step and begin acting on your ideas, it becomes very easy for you to be labeled with the titles and descriptions I have listed before. Once the people have thus branded you, and you become "annoying" enough for the government to take notice, no one will be coming to your aid when your rights begin being violated.

Once you take that next step and begin acting on your ideas, it becomes very easy for you to be labeled with the titles and descriptions I have listed before. Once the people

Why? Because to do so, your fellow Americans would have to be willing to place their comfort zones at risk. Once again, people have become too comfortable where they are and with the way things are going. To shake this up is a completely foreign idea to them. They have already given up their rights that are slipping away from you as you fight to assert them.

No one wants to be on the receiving end of the type of treatment Mr. Maginnis was put to. And as stories and accounts of similar treatments come out, more and more Americans will become unwilling to speak out. They are unwilling to do whatever it is that their very hearts tell them is right. They are unwilling to stand up to those that they, themselves, put into office. This is where the fear plays in. No American wants to be treated this way, so they become afraid of getting treated this way, and all attempt to avoid obtaining the label of "un-American".

Because the people of this country have become "comfortable", and unwilling to disturb that comfort, we have almost willingly given up our rights. Because most Americans lack the drive or motivation to fight for what it is they know to be right, the government has no cause to hear our voices when we speak out. For they know that most are unwilling to take the steps necessary to bring about change.

Change is not easily brought about. Especially when you have those in power who are more than happy with the way things are going right now. They will work against you, and as they have these labels and titles they can publicly assign to you, and thus get the backing of those "patriotic" Americans, the government can make it even more difficult to change.



# PEARL CORNER

## WATCHING THE WATCHERS

Being the webmaster of a site ([rootsecure.net](http://www.rootsecure.net)) which receives a reasonable amount of hits daily, I decided to try and find out some more information about who my visitors were. Therefore I wrote a simple little script to go over my log files every month or so and give me all the hostnames for the IP addresses found in my logs. This led me to discover a number of hits from \*.mil, and \*.gov domains which proved to be particularly interesting. I discovered I have everyone visiting my site from FNMOC, NCSC, NIPR, SPAWAR, NASA, DOD, DERA, FNMOC, NCSC to the Swedish Armed Forces. (see [http://www.rootsecure.net/content/temp/agencies\\_on\\_rootsecure.net.txt](http://www.rootsecure.net/content/temp/agencies_on_rootsecure.net.txt) for details.

This obviously warranted further attention, which it was duly given in the form of a Perl script capable of going through an Apache log file, picnicking out the IP addresses, resolving them to hostnames, checking if they are \*.mil or \*.gov, and picking out the raw log lines for those hits.

Upon last running this script I discovered the following interesting facts:

- \* Department Of Veterans Affairs is looking for 802.11b sniffers on Google.
- \* Idaho National Engineering Laboratory is looking for info on spoofing "HTTP referrer".
- \* Swedish Armed Forces are using Linux.
- \* DOD are interested in wartyping.

Previous runs of the script have shown the following:

- \* Australian Department Of Defence is looking at "802.11b auditing" on Yahoo.
- \* Defence Evaluation and Research Agency (DERA) is looking for "phpBB exploit" and "vnc exploit" on Google, using Linux machines.
- \* Space and Naval Warfare Systems Command (SPAWAR) is looking on Earthlink for: "EMSEC" (Emissions Security Countermeasures).
- \* DOD is interested in "net send exploits" on Yahoo.
- \* Air Force Logistics Command is looking at "wireless keyboard hacking" on Yahoo
- \* National Institute of Standards and Technology is interested in "Uncertainty principle untenable" on Yahoo.

In addition to the above hits I received a nice email from an Air Force employee thanking me for the information on wartyping.com stating he was conducting a risk analysis on a wireless keyboards.

I certainly think its nice to see the US Government finally taking such a visible interest in security for a change. To be able to run the Perl script that will search your logs for such hits you first need access to a box with a working copy of Perl (pre-installed on most \*.nix and downloadable for Windows at <http://www.activestate.com/Products/Download/Download.plex?id=ActivePerl>) then:

1. Copy / paste the script from this article to a new file such as ip\_resolver.pl.
2. Put your log file in the same directory and name it log.txt
3. Goto the directory containing your log/the Perl script and execute the command:  
perl ip\_resolver.pl
4. The script may pause while it reads in the logs, then it will start running through them displaying the results on the console.
5. Then when finished it will save a file "hostnames\_out.htm". This contains all the hits colour (yes that's how I spell colour) coded: green for \*.edu, blue for com/net/org, red for mil/gov and black for anything else. At the bottom of this HTML file you will find all the gov/mil hits separately listed along with all the raw log data lines relating to them.

The script also has an additional option, which allows you to tell it to start reading the log file at a particular line. To use this option simply execute:

```
perl ip_resolver.pl linenummer
```

In an age of increased government powers watch the watchers.

[http://www.eff.org/Censorship/Terrorism\\_militias](http://www.eff.org/Censorship/Terrorism_militias)

Interesting hits can be mailed to [nick84@rootsecure.net](mailto:nick84@rootsecure.net)

**nick84**  0101



```
#!/usr/bin/perl -w
# Note: Some lines have been wrapped for readability
# names of the input log file / output hostnames file
#
-----
$log_in_file = "log.txt";
$html_results_file="hostnames_out.htm";
#-----
#=====
# run parts of the program
&get_hostnames;
&html;
&save_html_page;
#=====
# template for displaying hostnames
sub html {
$html_page = <<__READ_HTML__
<html>
<head>
<meta http-equiv="Content-Language" content="en-gb">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Hostnames</title>
</head>
<body>

<table border="0" cellpadding="0" cellspacing="0"
style="border-collapse: collapse" bordercolor="#111111" width="100%">
<tr>
<td width="100%" bgcolor="#000000" height="50">&nbsp;&nbsp;&nbsp;</td>
</tr>
<tr>
<td width="100%">
<pre>
$all_hn_ip
</pre>
</td>
</tr>
<tr>
<td width="100%" bgcolor="#000000" height="50">&nbsp;&nbsp;&nbsp;</td>
</tr>
</table>
</body>
</html>
__READ_HTML__
} ### end sub html
#=====
sub get_hostnames {
# read in the raw log file to @data
open(DAT, $log_in_file) || die("Error log file must be \"\$log_in_file\"");
@data=<DAT>;
close(DAT);
# initialise a variable to strip new line characters from a string
use vars qw/$NLT/; $NLT = qr/(?:\r|\n|\t)/;
# prevent un-initialised errors
$all_ip='';
$all_hn_ip='';
$all_sp_ip='';
$hn_ip='';
$sp_hn_ip='';
$sp_lines='';
# if a line number was entered on the command line e.g. perl ip_resolver.pl
# 1724 start resolving ips from this point on
if ($ARGV[0]) { $in_line_from=$ARGV[0]; }
else { $in_line_from = 0; }
foreach $line (@data) {
$line_no++;
if ($line_no >= $in_line_from) {
```





```

if ($line) {
$line =~ s/$NLT//g;
($ip)=split(/\ /,$line);
# if ip is a number in the format ***.***.***.*** then
if ($ip =~ m!(\d+)\.(\d+)\.(\d+)\.(\d+)!) {
# if the ip has allready been resolved then skip this part
unless ($all_ip =~ /$ip/){
$all_ip = $all_ip . "$ip ";
$hostname = '';
# resolve the actual ip address
$hostname =
(gethostbyaddr(pack('C4', $1, $2, $3, $4), 2))[0];
$hostname = $hostname || 'no reverse DNS';
# get the length of the hostname to line up the columns
$ocharno = length ($hostname);
if ($ocharno > 50) { $charno=1; }

else { $charno = 50-$ocharno; }
# add this ammount of space characters to make up the
# rest of the line untill the start of the ip address
$addspace = " " x $charno;
print $hostname . $addspace . $ip . "\n";
# use various colours for the various hostnames
$line_start = '<font color="#000000">'; $line_end =
'</font>';
if ($hostname =~ /edu/i){ $line_start =
'<font color="#008000">'; }
if ($hostname =~ /(com|net|org)/i){ $line_start =
'<font color="#0000FF">'; }
if ($hostname =~ /(gov|mil)/i){ $line_start =
'<font color="#FF0000">'; }
# compile the finished hostname / ip line complete with
# font colour
$hn_ip = $line_start . $hostname . $addspace . $ip .
$line_end . "\n";
# add this line to the rest
$all_hn_ip = $all_hn_ip . $hn_ip;
# if the hostname is a special one (gov/mil) then add
# it to a special store of its own to be displayed at
# the top of the page and also add the coresponding raw
# log lines to a special store
if ($hostname =~ /(gov|mil)/i){ $sp_hn_ip = $sp_hn_ip .
$hn_ip; $addunderline = "-" x $ocharno; $sp_lines =
$sp_lines . "\n$hostname\n$addunderline\n"; $all_sp_ip
= $all_sp_ip . "$ip "; }
}
# if we have a special ip then store the log lines for it
if ($all_sp_ip =~ /$ip/){
$sp_lines = $sp_lines . " " . $line . "\n";
}
}
}
}
# if there are special hostnames present then sort out the line spacing
if ($sp_hn_ip) { $all_hn_ip = $all_hn_ip . "\n" .
"====*.GOV / *.MIL=====\n\n"
. $sp_hn_ip . $sp_lines; }
} ### end sub get_hostnames
#=====
sub save_html_page {
# save the finished html page to a file ready for viewing
open(DAT,">$html_results_file") || die("Error ensure this script has write
permissions \"$html_results_file\"");
print DAT "$html_page";
close(DAT);
}
#=====

```





# /\* comments \*/

**<http://www.binrev.com/>**

The official website of Binary Revolution Magazine - source for news relating to the publication of /bin/rev/, as well as information on how to make submissions.

**<http://www.stankdawg.com/>**

The home of it all. Keep up with all DDP activities here.

**<http://www.oldschoolphreak.com/>**

Home of Radio Freek America (RFA). The official online radio show of the DDP. Starring dual\_parallel and a cast others.

**<http://www.digitalrights.org/>**

Yes, you DO have rights! You must visit this site to see how your rights are being taken away by our government on a daily basis. Formed by DDP member Bi0s.

**<http://www.rootsecure.net/>**

Security news, updated daily. True unbiased reports from one of our worldwide correspondents. Created, written, and maintained by DDP member nick84.

**<http://www.port7alliance.com/>**

Home of a great online 'zine called Radical Future. Contains contributions from DDP members as well as P7A allies.

**<http://www.outbreakzine.tk/>**

Home of Outbreak, a monthly online 'zine containing more DDP contributions. From technical, to humor, this zine covers it all.

**<http://www.2600.com/>**

Come on, they started it all. Several DDP members have been published in 2600 and we strive to achieve their level of recognition. This magazine emulates their format.

**<http://www.phrack.org/>**

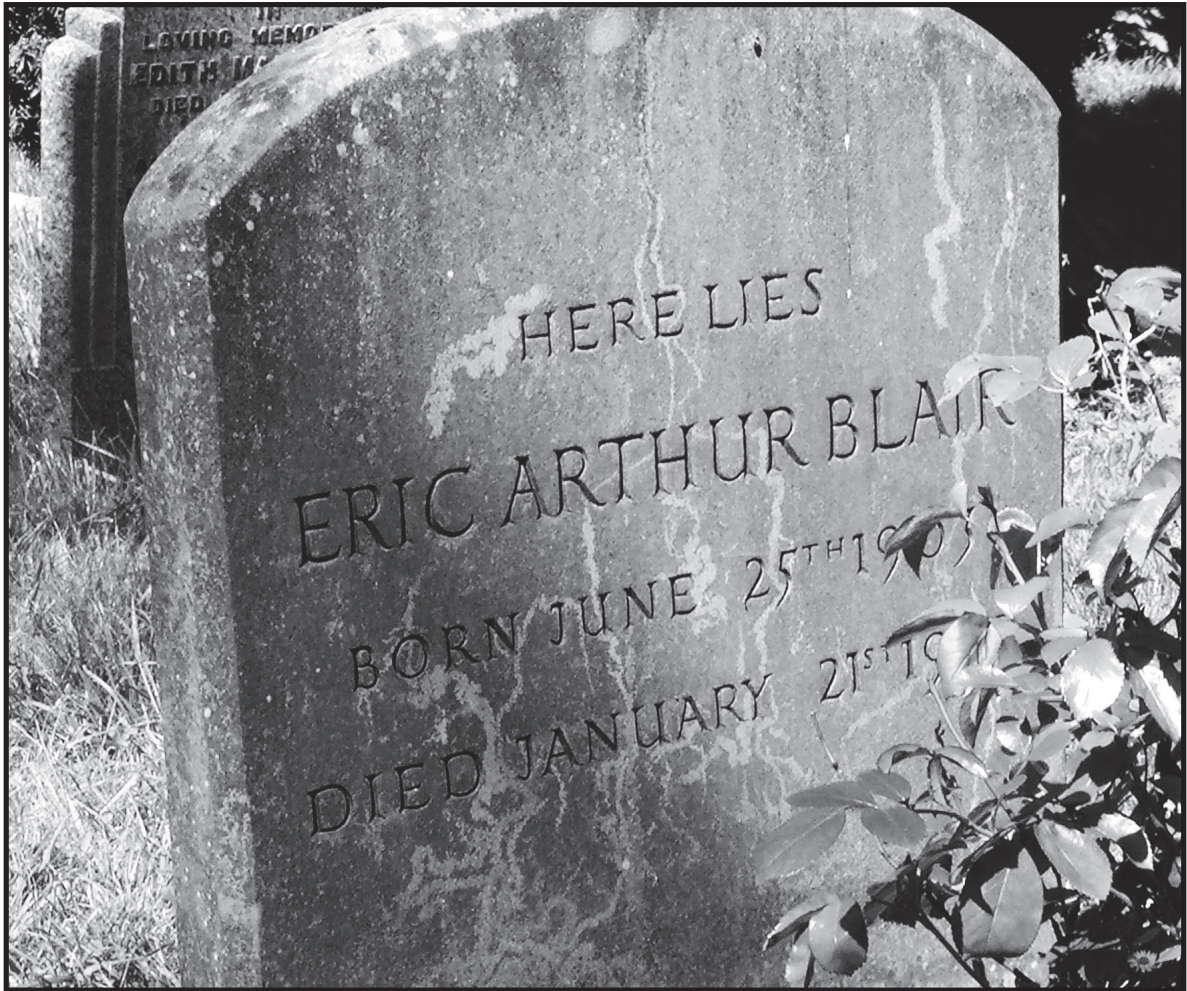
Another inspirational 'zine for technical information. We hope to achieve similar technical credibility.

## **THANKS:**

As the editor of this fine magazine that you just finished reading, I must thank all of the members of the Digital DawgPound. Without them, I would be just another geek on the internet, pissing people off. But with them, I am another geek on the internet pissing off a much wider audience than I could ever reach alone. Of course, I am kidding, but I do appreciate all of their contributions and support. Not only our members deserve thanks, but also our regular visitors and listeners, or as I like to think of them...friends. This product came about thanks to their support and encouragement as well. Please send your comments, flames, questions, and answers to the forums at **<http://www.stankdawg.com/forums/>** or feel free to email me directly at **[stankdawg@stankdawg.com](mailto:stankdawg@stankdawg.com)** with anything at all.

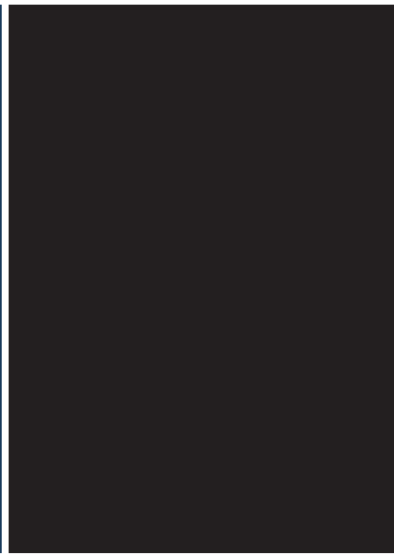
Until next issue... keep on hacking!





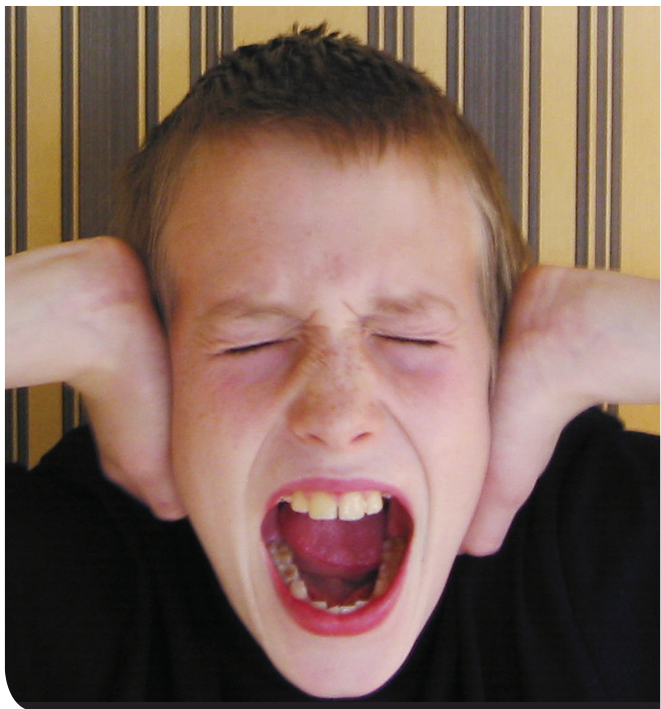
---

Big Brother ~~is~~ watching.  
WAS



# 1983

- > Crime: Changing report card grades
- > Tools: Pen & Paper
- > Punishment: Parental admonishment and school suspension



A DDP Production

www.binrev.com