

000AEE

the
slacker
journal

first fuckin'
free issue!

HACKERS2

summer
sequels

buddhism: WTF?

MYSFACE-IS
YOUR-SPACE

IE7 BETA2
LOL!

never pay
for wifi
access again

wireless
identity
theft



#CURRENT RESIDENT#
1600 Pennsylvania Ave
Washington, DC 20520

A man with glasses and a goatee, wearing a yellow tweed jacket, a brown hat, a patterned tie, and brown slacks, stands in a grassy field. He is holding a blue sign with the word 'ODDREE' in yellow block letters above his head with his right hand and a brown hat in front of him with his left hand. In the background, there are houses and a shed.

ODDREE

ODDREE MAGAZINE
4485 Dunganon Dr
Grove City, OH
43123

www.oddree.com

ON THE COVER

Ray is wearing:
Brown-hat Hacker
Fedora: Wal-Mart
(clearance) \$5.00

Cat Racing embroi-
dered yellow dress
shirt: Volunteers
of America \$1.99

Brown tie with
duck pattern: Ohio
Thrift \$2.49

Yellow tweed jack-
et: Ohio Thrift
\$2.99

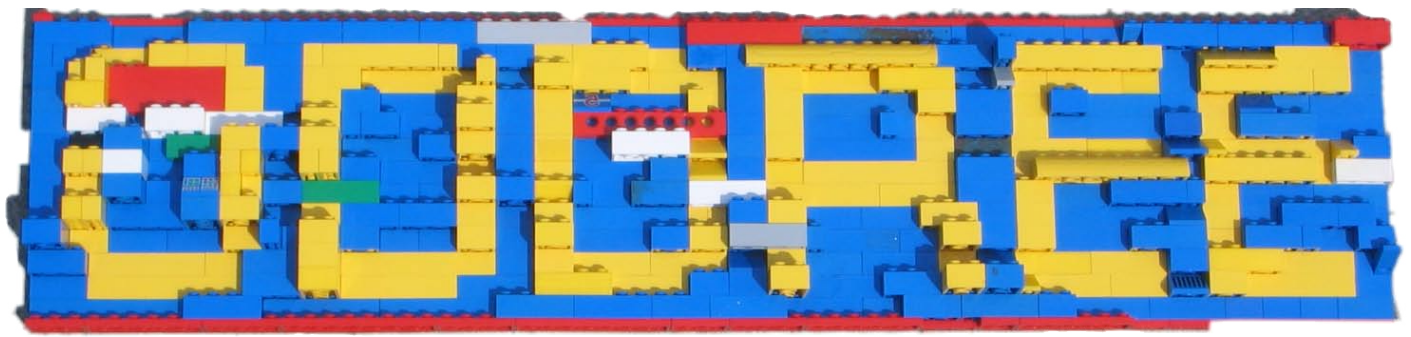
Brown slacks with
tapered legs: Ohio
Thrift \$1.99

Black Converse,
red highlights:
Factory Outlets,
Gaithersburg VA
\$34.99

Red shoe lace ac-
cessory: Payless
Shoes \$2.49

ALL PHOTOS BY:
Rotary Girl

MODEL:
Ray Dios Haque



ODDREE MAGAZINE - VOLUME #1 - ISSUE #1 - SUMMER 2006



LIST FEATURE ARTICLES

4 WIRELESS IDENTIFY THEFT

16 THIS SPACE IS YOUR SPACE

17 SUMMER SEQUELS

20 INTERNET EXPLORER STILL SUCKS

21 THE MAC ATTACK

29 BUDDHISM: WTF?

33 SUPPORT US

Comments, complaints?

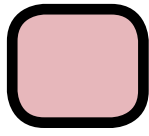
Send them to letters@odtree.com. We will be printing your feedback in issue #2.

When is issue two coming out?

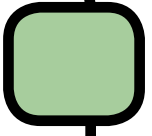
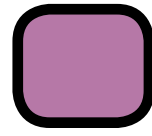
ODDREE Magazine is printed on an irregular schedule. When Ray has something to write, and time to write it, he puts it into this magazine. If you would like to see new issues sooner, you can help by sending us material to print. We figure 30 pages is just about right for a "download distribution" system.

Would you like to join our staff? You can start by writing an article for us. Send your articles to ray@odtree.com for printing consideration.

Want to help? You can donate by PayPal to: donations@odtree.com. For more info: see page 33 of this issue.



never pay for wifi again



an identity theft how-to

by Ray Dios Haque

Have you ever had your identity stolen? While teaching I once had a student tell me that someone had signed up for several credit cards using his name and social security number. This wasn't known to him until he attempted to purchase a home and was told "you have too much open credit". It seems a man in the same city had acquired nine different credit cards within a two month period. Why wasn't he aware that this had happened? Because the crook paid his bills. It's certainly a rarity in identity theft. Most thieves get the highest amount a credit card company will offer, and then load up the card as quickly as they can. This thief, however, got several cards in small amounts and then paid for the cards every month. One had to wonder if he paid the bills so that he wouldn't raise suspicion and get caught, or if he was planning on using this identity for many years to come and just didn't want a lousy credit history. I have never been a victim of identity theft. Most likely, this is because my credit is fucking terrible ... and thieves would do good to find a better social security number than mine.

While it's not likely you will be a 'transparent victim' of identity theft with your credit, it's becoming very likely that you will become victim of hijacking, man-in-the-middle attacks, and other such gags. None will argue that TCP/IP is a protocol that has out-lived it's expectations. While we gave it's latter half the appropriate name of "Internet protocol" very few expected the Internet to grow to it's present size and complexity. So it should be no surprise that when this protocol was established, it was not built with a high level security. This protocol was developed throughout the late sixties and early seventies.

"... it's becoming very likely that you will become victim of hijacking, man-in-the-middle attacks, and other such gags"



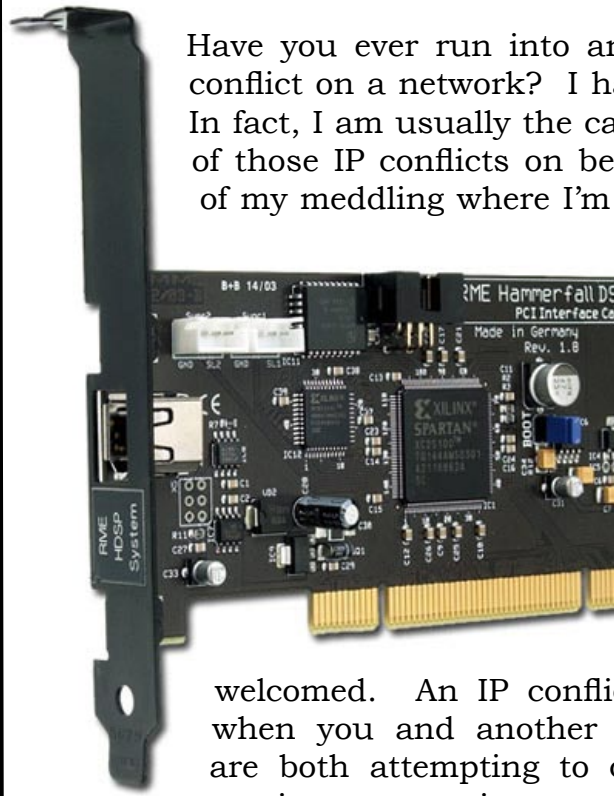
I often joke that if anyone were looking for “reason”, it could be found up at the local disco snorting cocaine and having tons of promiscuous sex. I’m kidding, of course. I don’t want any 50-something protocol engineers tracking me down for an ass kicking.

To understand this protocols weaknesses, we have to understand it’s theory of operation. We can begin with the “MAC address”. All network devices in the world have a unique MAC address. If we want to be technical about it, every “network interface” has a unique MAC address. Some network devices such as routers have several interfaces. An interface is just a receptacle such as a twisted pair Ethernet port. This address is often referred to as a physical address. We say it’s physical or “burnt in” because it’s hard coded right into the controlling circuitry of the network device.

While this MAC address is relatively short (12 characters) each character can represents a value between 0 and 16. How can a single number represent a value larger than 9? That’s the beauty of hexadecimal. We use a standard 0 through 9 system, and then extend it with letters “A” through “F”. So instead of using the number 10 to follow 9, we use the letter A. Instead of the number 11, we use the letter B. So on, and so forth. If we do the math, we can say that there are trillions of unique address possibilities with a 12 digit address.

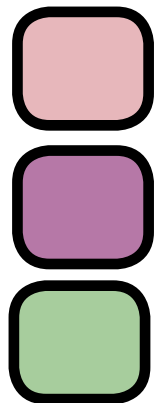
The MAC address was devised in a way that the first half (six digits) are said to represent the manufacturer, and the latter half (also six digits) represent a unique device by that manufacturer. This of course ruins the idea of the trillions of addresses. Some manufacturers will create millions of devices (such as 3-Com and Cisco) while others may only create hundreds of devices in small

batches (medical equipment). Have there been duplicate MAC addresses in the world? Surely there have been, but who cares. So long as two machines sharing the same address are not on the same physical network segment this will never be a problem. Therefore, despite a few mistakes throughout network history, we can assume that the MAC address in your network device is 100% unique, and not shared with any other device.



Have you ever run into an IP conflict on a network? I have. In fact, I am usually the cause of those IP conflicts on behalf of my meddling where I’m not

welcomed. An IP conflict is when you and another host are both attempting to communicate as unique participants on a network, yet you both hold the same network address. This network address or “IP address” was likely loaned from a DHCP (Dynamic Host Configuration Protocol) server, but could have also been statically configured by an administrator. The question at hand here is, “how did you know there were two of us – if we have the same address?”. To detect an accidental conflict such as this we rely on the MAC address.



ZERO COOL IS BACK



HE COULD USE SOME HELP HACKING THE PLANET.



Play **HACKERS** and you can help Dade Murphy and his friends hack the planet from the comfort of your living room.

Grab trash files. Hide floppy disks in men's rooms. Make traffic lights change colors and cause horrible, catastrophic automobile accidents.

You can even meet up with Kate Libby and go on a hot date. All in stellar color graphics.



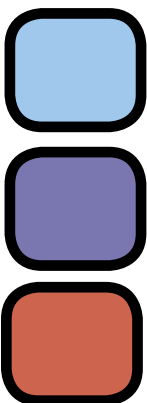
Here's an analogy. One day you get a call from a credit agency. They ask for you by name, and when you identify yourself as that person, the agency tells you that you own nearly ten thousand dollars in back taxes and credit card debt. You are floored by this news, because you have received a refund on your taxes for the past several years, and you only own one credit card with a very low limit. The agency then goes on to ask you if you moved from Texas to avoid this debt. Never having lived in Texas, you insist this is a case of mistaken identity. How will the credit agency determine that you are not the deadbeat in question? They will compare your social security numbers. In the end you find that this person was just some poor loser who happened to have the same name that you do.

In the story, we saw that a unique number was needed to identify you as a unique individual. We can use the MAC address in the same way on a network. A good question here might be, "who is aware that there is a conflict?". Without slipping too far off topic, let's compare some network devices which are quite different and yet all serve the same purpose which is to connect several computers together over a "network".

The Hub - Hubs (rarely used these days) are very cheap to produce and simple to understand. They are flat rectangular devices with anywhere from eight to a hundred connections on the front for network devices. Hubs are at this point considered completely obsolete. Why? Whatever traffic is sent into a hub is then retransmitted to all other connected devices. This is an awful idea,

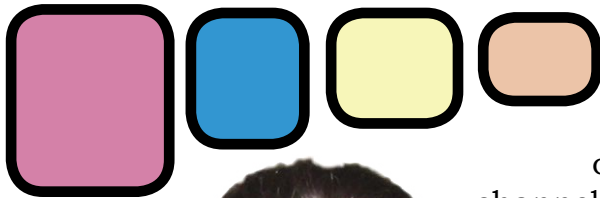
because you end up getting other folks network traffic handed to you ... and congestion builds up quickly. All traffic is sent to all ports with no distinction of 'what belongs where', even if it's complete gibberish. This has caused quite a bit of grief for network administrators worldwide which reminds me of a story.

Years ago, network administrators banned together and declared that large networks were huge miserable failures when connected via hubs, and they weren't going to stand for it. In fact, in mid-summer of 1997, six administrators in Silicone Valley went on a drunken rampage murdering "2E" engineers at a local electronics plant that manufactured hubs. No one can explain why this death toll was represented hexadecimally. Some theorize that the reporter of the story was an engineer himself and was making a statement with the obscurely recorded number. Yet, most readers of the local gazette guessed that "2E" was a mis-print, and that only two engineers were murdered in all. For this reason, it is said that only 1A citizens sent flowers and cards to the victims families.

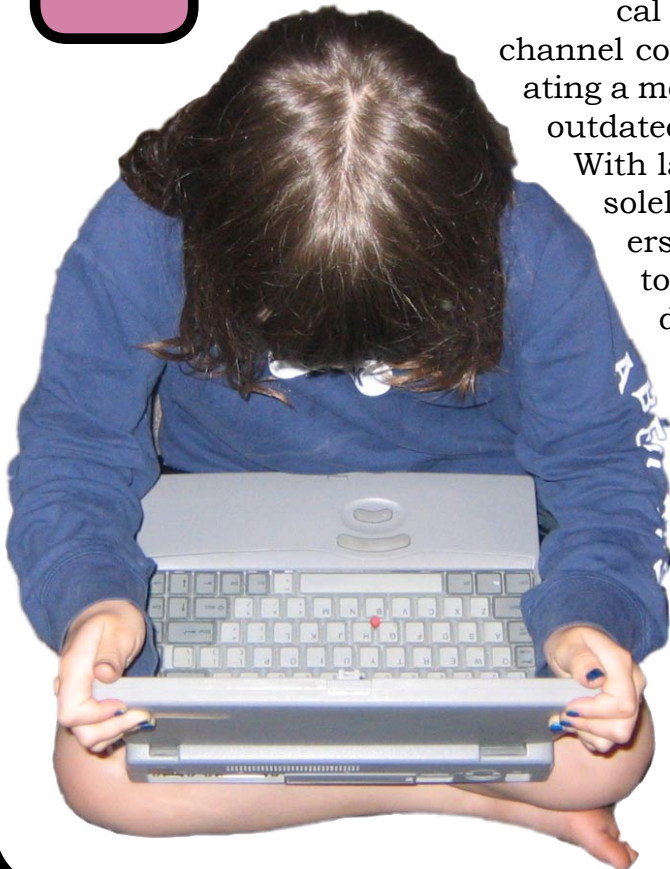


The modern Switch – Switches sound a lot like hubs when explained. They too are flat and rectangular with lots of little ports for connecting devices. What makes them different is how they act. Switches will only transmit packets between hosts when it makes sense to. If two parties connected through a switch have a long conversation involving thousands of packet transfers, no one else connected to that switch has to hear it.

For this to work properly, switches require some ability to identify the hosts as unique participants. They identify hosts using their MAC address. Now what if two devices were to connect to this switch having the same MAC address? Most likely the switch would see this as either a horrible routing mistake involving hubs, a mathematical impossibility, or some jerk performing a case of stolen identity. In any case, traffic would likely cease to flow between these devices.



The Access Point – AP's transmit their signals to and from wireless network cards using the open airwaves (radio transmissions). Because we share the open air, and there are no physical connections to speak of, data flows over that channel constantly colliding with other signals and creating a mess. In comparison, AP's seem a lot like those outdated hubs that we thought we were done with. With lack of physical connections, AP's have to rely solely on the MAC address to identify unique users. This means that to differentiate between to users with the same MAC address would be difficult if not impossible.



By now you are asking yourself, “how do I become another user on a network -how do I steal their identity?”. But wait ... the first question you should ask is, “why should I want to become someone else?”. That’s easy. Imagine you have just checked into a fine hotel. Myself, I stay in Motel 6’s all over the United States. While they have no ‘frequent guest’ points program, they do have HBO, occasional fresh linen, and real working showers (but hot water is often optional).

In these hotels you may be offered a plethora of no cost services such as a free breakfast and bath soap (which according to the wrapper may also be used as shampoo). Despite the wonderful hospitality of this fine establishment you are still expected to pay a high dollar amount for Internet Access. I'll bet in a busy motel, at least one person has paid for this service. How about we assume the identity of that paying customer. It would be as simple as stealing their identity ... by stealing their MAC address!

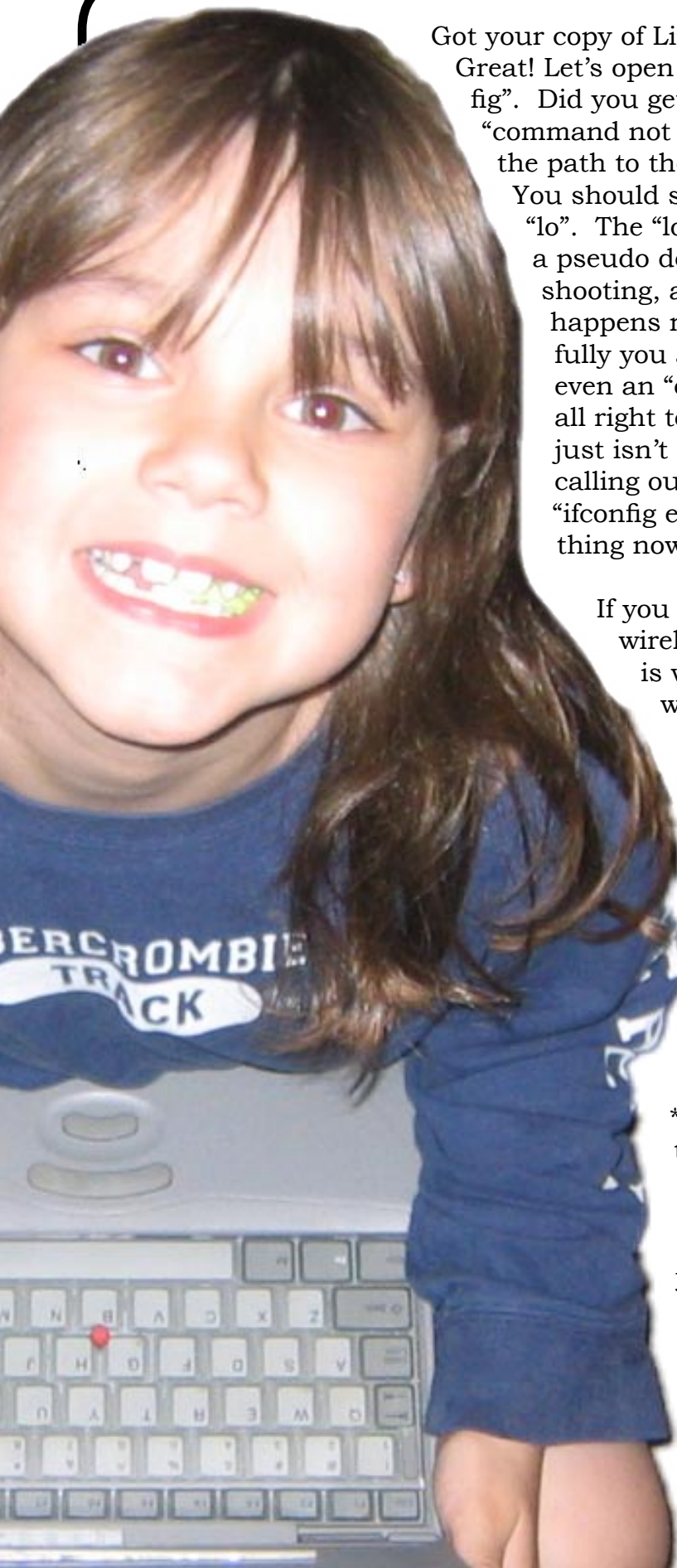
Before stealing someones identity, consider the paying alternative. Just how much are they trying to squeeze out of you for this paid access? I have often bought access from McDonald's. Most McDonald's restaurants throughout the United States offer WiFi services for \$2.95 and the connection lasts several hours. The downside of this service is you generally have to pay with a credit card. I have attempted to order a "connection coupon" from the service counter, but the employees usually have no idea what you are talking about and are probably unaware that they even offer this service. Coffee shops are also known for WiFi access, although those commercial joints like Starbucks will get you for a couple bucks an hour. Consider locating a public library or book store. These often give away free access.

If you're too cheap to buy it, or you are just attracted to the idea of electronic identity theft we will now explore how to pull it off. To proceed with this activity you will need a WiFi card, a "pay to play" hot spot, and a very "special" operating system. Our best advice, is to get some

flavor of Linux. Why Linux? We have a few theories.

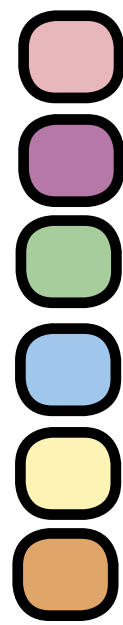
Early operating systems such as UNIX were very loose in dealing with hardware. Many UNIX variants such as Linux had this same "looseness" which allows for the quick changing of network properties. Modern operating systems such as Windows XP may allow hardware properties to be changed, but it will likely require a fair bit of hacking, rebooting, and heavy drinking. While several utilities have been written over the years for Windows to allow spoofing of your IP and MAC addresses, they all seem to suck big donkey dicks. Again, our advice is to get a copy of Linux, and come over to the "other side". If you are new to Linux, we recommend Ubuntu Linux. The installation process is very smooth, and adding software packages to it is a real snap! Plus, free updates. Something that is becoming a rarity even with open source Linux distributions.





Got your copy of Linux installed and ready to roll? Great! Let's open up a terminal and run "ifconfig". Did you get a response? You may have got a "command not found error". If so, try including the path to the program with "/sbin/ifconfig".

You should see at least one device, even if it's "lo". The "lo" is short for "loopback". This is a pseudo device which is useful for troubleshooting, and for talking to yourself (which happens more often than you think). Hopefully you also see an "eth0" and maybe even an "eth1". If you see nothing, that's all right too. Maybe your network device just isn't configured yet. You might also try calling out the network device by name with "ifconfig eth0" or "ifconfig eth1". See something now?



If you have a wired network device and also a wireless one, you will want to know which is which. Try running "iwconfig" and see what you come up with. The "iwconfig" command will tell you "no wireless extensions" for wired cards, and will display properties for your wireless one. So now we have that figured out. Let's refer to your wireless device from here on out as "ethX".

I have found a few interesting characteristics of how "pay to play" access points operate.

- * They will transmit traffic to and from anyone.
- * Once you have paid for access, they will transmit traffic between you and other stations.
- * If you attempt to transmit to other stations before paying, they will obscure your traffic.

When I say "they obscure your traffic", I mean to say that they cripple any attempts you make to identify other parties on the network. When you want to speak to a new host on a network, you go looking for them by IP address.

So I might open a terminal window and type "ping 192.168.1.1". Once you have honed your senses, and have a great sense of timing you may notice a brief bit of lag while waiting for that first successful reply. Why? Because in that short moment, you went onto the network and said "hi, I am looking for 192.168.1.1, if you are this person ... let me know ... my name is 00:A1:B2:C3:D4:E5". We call this process "ARP". For that matter, we call the entire protocol ARP (Address Resolution Protocol). And if that isn't simple enough for you, the command to demonstrate this protocol is also called "arp". Want to give it a shot?

From a terminal, type "arp -a". This says "I want to see my ARP entries". You should see a list showing you IP addresses (or sometimes host names) on one side, and MAC addresses on the other. If you got nothing back, ping some one and try it again. Now ... if you wait between 2 and 5 minutes and run "arp -a" again, they will be gone. Why? ARP is a dynamic system. While you can record away ARP entries statically, nobody does. So we only hold onto these MAC addresses for a short while. Even though it's permanently burnt into the hardware and will NEVER change, we want to allow for some unlikely (yet still possible) events. Those are: Someone quickly changes out the physical network card in a PC and then uses the same MAC address. Or - a machine was loaning an IP address (using DHCP), they lose it, and then they pick up another.

Again, neither of these events are likely to happen at all, let alone "soon", and so if you ask me I think this whole system is silly.

Getting back to our goal here - the access point should talk to you. It needs to talk to you, so it can sell you it's services. You should not need to speak to any other users on the network. In fact, by doing so you could only be up to trouble. So when you go onto the network and ask "who is this 192.168.1.11" (where 192.168.1.11 is some random host on the network) the access point will answer back with "oh, I think you meant for that to come to me". It will then offer a useless answer, or an invalid one. In other words it's saying "pay no attention to them kid, I'm the guy you need to speak to". In my early experiments, I was pretty frustrated with this game. I knew that to impersonate one of those paying users, I would need their MAC address.

VIEW ASKEW TRIVIA GAME

[by grant brunner]

**ten tough questions for view askew experts
[answers next issue]**

- 1. What actor almost played the character Jay in Mallrats instead of Jason Mewes?**
- 2. What news paper did Jennifer Schwalbach work for when she met Kevin Smith?**
- 3. What group of religious zealots protested the release of Dogma?**
- 4. What role was Kevin Smith originally going to play in Clerks?**
- 5. Out of the seven movies that Kevin Smith has written/directed (as of 2006), which film is not part of the "Jersey Saga"?**
- 6. Out of the six episodes of the Clerks cartoon show that were made, which two aired on ABC?**
- 7. Out of the non-Kevin Smith films produced by View Askew, which one was made by Bryan Johnson?**
- 8. What character in Dogma was originally written for Jason Lee?**
- 9. In Clerks, how many roles are played by Walter Flanagan?**
- 10. Which film written/directed by Kevin Smith has Brian O'Halloran not appeared in?**

And I knew that every time I tried to inquire about it, the damned access point screwed it up. So what can we do? We can become the access point!

Lo and behold, the secret to making this work, is to become the access point. You will need his MAC address, but this will be easy because he offers it up to you. Remember, he needs to get you to the point where you pay. So start by pinging the access point. We will leave out the part where you open your laptop, connect to the access point, and wait for an address to be loaned. Let's assume you have done all that, and you can talk to that access point. Get into a terminal, and see what your address is (you can use `"/sbin/ifconfig"`). Now we need the



address of the access point. So do a `"netstat -rn"`. Check the address in the bottom row of the second column. That is your access point. Ping it with `"ping <ip address of access point>"`.

Now that you have touched base, you have quietly recorded away that access points MAC address. Now do a `"arp -a"` and write it down. If you are using an x-windows terminal, I would recommend highlighting this with your mouse and copying it. Now we will become that access point. And following these next steps should be done very carefully.

"Lo and behold, the secret to making this work is to become the access point"

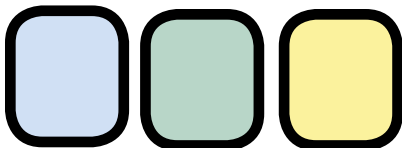
To continue, it would be easier to become root. So run a `"su -"` and type the root password when prompted to. Don't know your root password? Did you never set one? Ubuntu Linux attempts to do everything without using root, so to fix that you would have to run `"sudo passwd root"`. After setting a password, the `"su -"` command should work just fine. Got root? Good ... let's continue.

First we must take your network card offline. We don't want to kill it completely, or unload the driver. We just want to put it to sleep for a while. So do a `"ifconfig ethX down"`. Why did we do this? If we change either your MAC address, or your IP address we will create an instantaneous conflict of sorts. This would confuse other network participants and also possibly expose our evil plan. Next, we will change your MAC address.

To change your MAC address, run “ifconfig ethX hw ether <MAC address of access point>”. Did that fail? If so, try “ifconfig ethX lladdr ether <MAC address of access point>”. Did that fail too? If you are told that your device is in use, you should run “ifconfig ethX down” again and try to change the MAC. If it’s complaining that your command is bogus, you should run “man ifconfig” and see how you are supposed to do this. Some distributions do this part differently.

Now we will take the access points IP address. This should be easy. We will run “ifconfig ethX <IP address of access point>”. Now we can reactivate the card and begin to have some fun. So run “ifconfig ethX up”. You are the access point. Because all of these signals float through the airwaves, there will be no repercussions of what we have done. Traffic that was meant to go to the access point will get there, and it will get to you also. The point of all this is to get paying users to speak to us ... so we can steal THEIR identity.

One might ask “if we are assuming the identity of the access point, why can’t we surf the Internet now?”. There is a problem we have here involving routing. Typically, you send traffic to the access point, and he routes it to the next stop.



Because we “are the access point”, if we try to route traffic, we end up routing it to ourself. This of course either creates a nasty loop, or the traffic just dies. Either way, we are only going to stay with this identity temporarily.

To become one of those paying users, we need to see who they are. How can you

identify a paying user? They will be generating some network activity. To browse to a website, the user would be generating DNS requests (to turn ‘www.oddree.com’ into an IP address) and regular old HTTP requests (for standard web page transfers). Just like Neo, we need to “see the code”. This can be done using an age old network monitoring tool, tcpdump. To start it up (still as root) do a “tcpdump -i ethX”. You should get a moments pause, and then the garbage will start to roll in. I have only ever been on one network when I saw absolutely nothing. That was the San Diego International Airport (in San Diego, of course). I was there between midnight and seven in the morning as were some other poor traveling suckers stuck between flights. But missing, was a single paying WiFi customer. May you never experience a network this quiet, or have to sleep in a McDonald’s booth while anti-terrorist airport messages ring through your head every 4 ½ minutes. Anyhow, if you really see nothing, you might have picked the wrong network device.

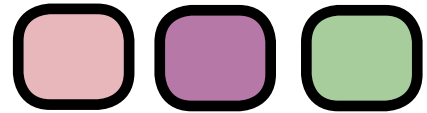
Now what are we watching for? Look for DNS traffic and HTTP traffic which will be clearly labeled. I generally let the screen fill up and then do a “Ctrl+C” to stop the flow of information. Look for a paying customer, and then take note of their IP address. We will become them next. You should ping them now, just to be sure that they are in your ARP table. Don’t be surprised if you have several entries when we look. To have a peek, run “arp -a”. Did we get them? If not, we can repeat the tcpdump trick and try this again. Sometimes hosts are physically a little too far away from us to get away with these tricks. If you have a MAC address and an IP address of your paying buddy, put it to use the same way we did with the access point.

“ifconfig ethX down”

“ifconfig ethX hw ether <paying users MAC address>”

“ifconfig ethX <paying users IP address>”

“ifconfig ethX up”



Now, you have become that paying customer. Want to test it? You’ve earned it. Open up a web browser and try to bring up a web page. Perhaps after some hesitation, it should load just fine. You may wonder what is happening on the network right now. You may not care. We’ll explain anyway. When you make a request to the access point to bring up a web page, that paying customer may see the request and say “hey, I didn’t say that!”. And when the web request is processed, and content starts coming back, they will say, “I didn’t ask for this shit!”. So can we get away with this secretly? No. Will the paying customer be aware of what is going on? Not bloody likely. I was once performing this very trick in an airport when I got that weird feeling that I was being watched. When I turned around I saw that two balding travelers had been watching me hack away in a terminal. I was a little worried that I might have been busted, because I never underestimate the knowledge of prying eyes. When they turned back around I heard one guy say to the other, “Hmph! It’s a laptop!”. No, they weren’t complete idiots. My laptop looks like a cross between a homemade explosive device, and a toilet seat.



Now that you are borrowing a paying users access, you may wonder “how long will this last”? That all depends on when they paid. Hotels usually make you buy access for 12 to 24 hours at a time while coffee shops and the like sell it in two hour increments. If you are especially polite or kind, you might wait for your paying user to finish up their work and leave. Now you can assume their identity and not cause anyone a single lick of grief. To me this is like sitting down as someone is leaving a restaurant and finishing their food. Yes, it’s wrong. But they were going to throw that food away, and you’re hungry! It’s recycling, right?

Lastly, I wouldn’t be doing this magazine justice if I didn’t mention the security considerations. While you are running around pretending to be paying customers ... they continue to be themselves. If that person had the knowledge, and the motivation, they could now monitor all of your traffic pretty easily. In other words, they could sniff your passwords, watch what websites you visit, and record your instant messaging conversations. Are you frightened yet? No? Me neither. I’m a risk taker. And if anyone got into my mail, or read my IM conversations they would be pretty bored and disappointed.

We have officially trained you in stealing access from “pay to play” access points. While most magazines would slip a disclaimer in here, we will not. But if you get into trouble, don’t come crying to us. None of this is legal, and you know it. Hack on, folks.

[Ray Dios Haque]





this space is your space

[Grant Brunner]

I have written about the Internet phenom that is MySpace before, but I think that it deserves to be written about again. Before I go off on my tangent, let me just note that I think that MySpace is utterly ridiculous. Not only MySpace, but the entire concept behind a system of a community of public profiles used for “networking” (id est, dating) is out-landish. As some of you might know, I’m a big fan of the Internet, but I think some things are sacred. I’m not going to go out looking for a girlfriend (Or just a good time, for that matter) on the web. If I want a gal-pal, I’ll go out and meet one at a social gathering. I find the concept of “hooking up” through a website to be myopic and out-and-out silly”. What, I ask you, would you do if you go on a date with a girl (Or guy... Whatever you please), and they have the most annoying personality that you have ever been privy to in the entire world?

I find MySpace and other “networking” sites to be akin to an annoying friend that wants to set you up on a blind date. Your friend will tell you all of the wonderful features about this person, and so will anyone’s MySpace profile. By the end of the love-fest for the blind-date-to-be, you’re practically in love with this person. What a lucky break, you think. Why hasn’t this gem been scooped up yet? I’ll tell you why... **BECAUSE HE OR SHE NEEDS MYSPACE TO GET A DATE!** Don’t you think that if someone is desirable, that person would be out getting some tail? I do, and it’s my article, so hang with me.

Aside from this obvious flaw in the equation of love, MySpace works well enough. Many people are a part of the community, and for some reason that is unknown to me, they love

it. A good friend of mine is a part of the community, and he thrives in it. This is a man that has been through undoubtedly hours of me rambling on about all of the flaws in MySpace. He has even agreed with many-arant of mine, yet he was still drawn to it like Pam Anderson is drawn to untalented musicians. I have asked him why he uses it, and the only answer he has given me is “People that I know use it.” Really, that is a good enough reason to use something? I suppose if it was themed, and it drew in people of similar interests, it would make sense to me. But it just a site where people from every different background that you can think of meet to post “funny” pictures in their friend’s comments, make some of the ugliest layouts I have ever seen, and stream (1990s style) Copyrighted music on top of my of the tunes coming out of my media player.

COOL NEW PEOPLE?



The odd part of this whole situation is that I rarely hear anyone besides myself complain about MySpace. Can I really be the only one that hates MySpace with a passion? I doubt it. So, my fine Oddree readers, I have something to ask of you. If you would, please write to me about how you feel about MySpace. Feedback is your (and my) best weapon. You get to tell me your side of the story, and I get to pick your argument apart in my next article. So if you have the stones to write me, I might just print your letter. So it would be best if you didn’t say anything you wouldn’t want me to have the last word on.

Grant Brunner is a writer and a budding film maker. If you would like to hear more from him, you can read his website (bassguy.tk), and listen to his podcast (twr.bassguy.tk). If you would like to contact Grant, you can write to him at grantbrunner@gmail.com.

SUMMER MOVIE PREVIEW 2006

It's time for another summer filled with blockbuster films featuring worn out super-villains and their complex psychological daddy issues.

Just kidding! You won't see any of that shit this year. The summer of 2006 promises the return of heroes that you probably thought would never return to the screen. I'll bet you thought Hollywood was afraid to gamble away millions on a film that only the nerd minority would run out to see. You thought wrong.

.....

HACKERS2

AKA "Joey's Wrath". Since the last film, "Joey" has assumed his original alias of "Ultra Laser" and left the group of hackers that included Zero Cool, Acid Burn, Cereal Killer, and the others. Joey having felt he was never respected by his cohorts goes on to consult with Eugene ("The Plague") who is now serving a 10 year prison term for his crimes in that took place in the first film. Eugene teaches Joey through a series of coded letters and secret notes passed by prison guards. As Joey's power grows equal to that of Eugene, he leaves the city and travels high into the mountains of a far off land.



- We have compiled a short list of the hottest films this summer. Every
- year has its fair share of sequels.
- But this is the year that we will see
- the return of Zero Cool, Ferris Buel-
- ler, and Doc Holliday and even Marty
- McFly.

- Get in line. Buy those fifteen dollar
- movie tickets. Grab your eight dollar
- popcorn (with complementary but-
- ter-like sauce) and prepare for the
- best fucking summer in your whole
- miserable life.

There, he disciplines his body in a martial art which modern weapons cannot easily feat.

Jonny Lee Miller returns to reprise his role of Dade Murphy ("Zero Cool"). In this film, Dade battles alcoholism and a crystal meth addiction while trying to maintain his relationship to his girlfriend "Acid Burn". Angelina Jolie chose not to reprise her role in this sequel, and was replaced by the lesser known Justin Bateman (of Family Ties fame). Acid Burn has problems of her own as she discovers the attraction she has always had with hacker

Sneakers2

AKA “Sneak-Eyes” The luck has run out for the band of hacker’s-for-hire that we remember from the first film. An angry “Cosmos” has set out to destroy our heroes and successfully plants a bomb in their van, killing everyone in it except for Martin Bishops girlfriend, Liz (played by Mary McDonnell). When asked why all the original characters were killed in the opening credits of this film, the director replied as follows. “We really wanted the original cast back. But, Robert Redford’s face is callapsing, Dan Akroyd said he was too busy, Sidney Pointier told us to ‘eat shit’, and that River Phoenix kid thinks he’s too good to return our calls”.

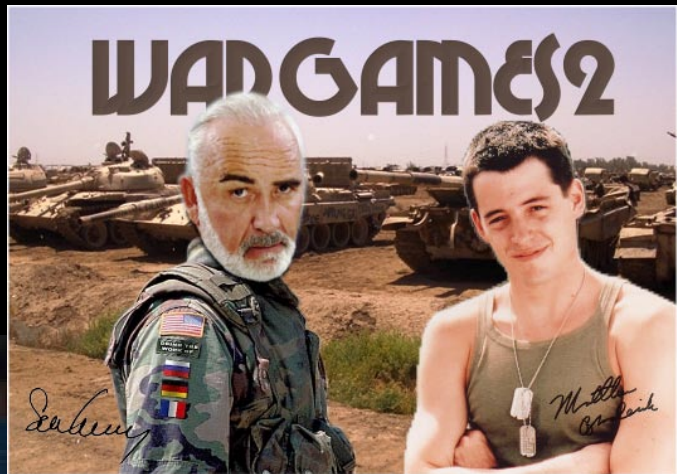
.....



In this sequel (only by name) produced by the LifeTime television network (for theaters) Liz vows revenge for her boyfriend and hacker buddies. Liz seeks out arch enemy Cosmos (now played by Ving Rhames) and using only an old Brisbane Portable computer (and a series of oversized floppy disks) is able to infiltrate Cosmos’s crime network. Cameos include Mr. T, and Jaquine Phoenix (who claims he only visited the set to take care of business involving harassment of his de-

WarGames2

Mathew Broderick reprises his role as “Ferris Bueller” in this never before attempted switch of a character between films. Replacing the nerdy David Lightman character, Ferris brings a cool-factor to this excellent modern day war epidemic. We join Ferris in his life many years after the first film took place and learn that he joined the military immediately after high school. The films many flashbacks reveal that his time in the military has been a “non-stop parade of shenanigans with his humorless commanders”. But now living in Iraq, Ferris is called upon by his commander (played by Sean Connery) to end the war



by “hacking the terrorists”. Ferris and his military friends fight to destroy the terrorists by infiltrating their networks and deleting all their important documents and bookmarks. Will Ferris win against the evil terrorists? Who the hell are the terrorists? Where the fuck is Bin Laden?

SWORDFISH 2

AKA "Sushi Date, The" - What ever happened to super hacker Stanley? How are things going with his daughter? Is the evil Gabriel Shear still lurking in the shadows after his daring getaway at the end of the first film? In Swordfish II, these questions will go unanswered.

Movie exec's decided that the timing wasn't right for a "hacker movie" and so instead they focused on creating the ultimate romantic comedy. Says director Rob Reiner, "the chemistry between Hugh Jackman and Michelle Pfeiffer in the first film was incredible. When asked if they would come back and reprise their roles, they were both delighted". When recently interviewed about his part in this film Hugh Jackman commented, "they had me signed on to do a sequel, and I refused

to do another fucking romantic comedy ... so I guess the studios win this round". Asked how she related to her character in this film Halle Berry replied, "at one point in the film she [Ginger Knowles] gets really drunk and runs over some guy with her car (laughs)".

In Swordfish II, most of the film takes place between 5:00PM and 2:00AM the following morning. We will follow the pair as they meet at Stanley's posh apartment, listen to music, and later take a cab to a fine sushi restaurant. The two have little in common, but they just can't get enough of each other. While Halle Berry does not go topless in the sequel, Hugh Jackman does. As Reiner explains "this is a chick flick ... if you want to see boobs you will have to wait for the DVD to see the beach scene we cut where I make a cameo ... bare chested [sic]".



See you
at the
movies?

[Ray Dios Haque]

INTERNET EXPLORER STILL SUCKS

This issue, we review 'IE 7 BETA 2' in one lousy page - [RDH]

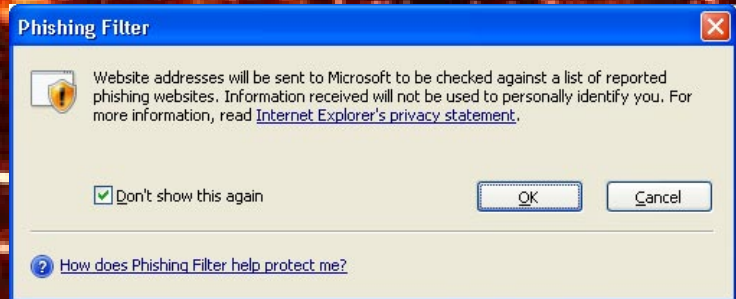
1



We've seen this Google box in Mozilla Firefox for ages now. Should we be impressed that Microsoft finally got around to "adopting it"? What's with that little magnifying glass? That was stolen directly from Apples "Tiger" OS! As usual, no points for originality here.

3

An all new "Phishing Filter" will keep you from sending your bank information to Nigerians. Or at least that's the idea. We were harassed by an annoying message that kept telling us "this website cannot be checked for Phishing". False alarms are always a great way to make people feel safer and more secure in their browsing experience.

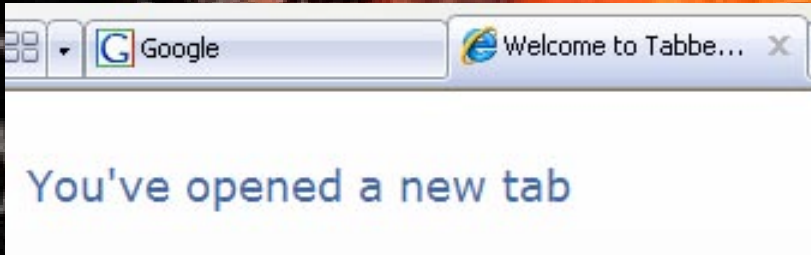


Internet Explorer has always seemed pretty quick. Until now. It's running from the time you log into Windows, so it should be pretty fast to open up. But IE7 is sluggish.

It doesn't get any better when you start heading out to your favorite web sites. Side by side with Mozilla Firefox, it's not even half as fast. Perhaps it will be quicker when it's built into "Windows Vista". Or perhaps not. We're sticking with Firefox.

2

Microsoft has finally implemented Tabbed Browsing. Just about five years behind the rest of the world. We're bothered that the "close" button for the tab- is on the tab itself. If you're going to steal someone's feature: do it right.



4

There's nothing I like more than reading a page full of text which has been displayed with "font smoothing". Now, everything you read will be fuzzy and smooth at the edges. Not only does this eat a huge chunk of resources, it's horrible to look at. Yeah, you can turn it off. But why the fuck is it on?

Those buttons that you have grown familiar with over the past 15 years were changed, and shuffled around. I guess it looks "new-er". But there is nothing better about them. It looks to me like a pathetic attempt to be stylish. Mission failed.

5



6





THE MAC

ATTACK

PATCHING ORINOCO DRIVERS ON UBUNTU OR DEBIAN LINUX

So, you wanna' take out that laptop and do a little wardriving, eh? All of your friends are running around using Netstumbler with Windows on their laptops, and you would like to show them a thing or two with what you can do in Linux. There's just one problem. You have put Linux on your laptop. Your wireless card is detected and runs just fine, but you can't seem to 'sniff' for networks. Perhaps you're running Unbuntu on an iBook (which will use Orinoco drivers for the Airport card). Your card doesn't seem to

want to cooperate with utilities like Kismet! **You are not alone.** The fine people that have worked over the years to develop Orinoco drivers on Linux discovered that the only way to stabilize and improve upon their code was to remove "RFMON" support. "RFMON" is short for "Radio Frequency MONitor". You need this ability to put your card into a listening state where it will simply open it's ears and report back everything it finds. Adding the support back is difficult, so we have decided to walk you through the process one step at a time.

For this article, we performed a clean installation of Ubuntu Linux 5.10 (Breezy Badger) onto an iBook (Ray's iBook to be exact). At the time of writing, 5.10 was the latest and greatest stable release. Yet, Dapper Drake (currently in BETA) is just around the corner. Therefore, we will make some notes throughout the article for those who are on the "cutting edge" of technology, or reading this in the future. Incidentally, if you are living in the future, please come visit me and let me know what people think of this issue. Having feedback in advance of the magazines release is nice.

First, we want to become root. We could just use 'sudo' for everything which would allow us to run just one thing as root, and then return to our standard user priveleges. But we would also like to show you how to enable the root account. In Ubuntu the root account is disabled for login purposes. Try becoming root as we did below.

```
ray@hax0r:~$ su -  
Password:  
su: Authentication failure  
Sorry.
```

Well that wasn't very successful. Was your luck about the same? What we will do next is enable the root account by giving it a password. Since we can't yet log in as root, we will use 'sudo' for this job.

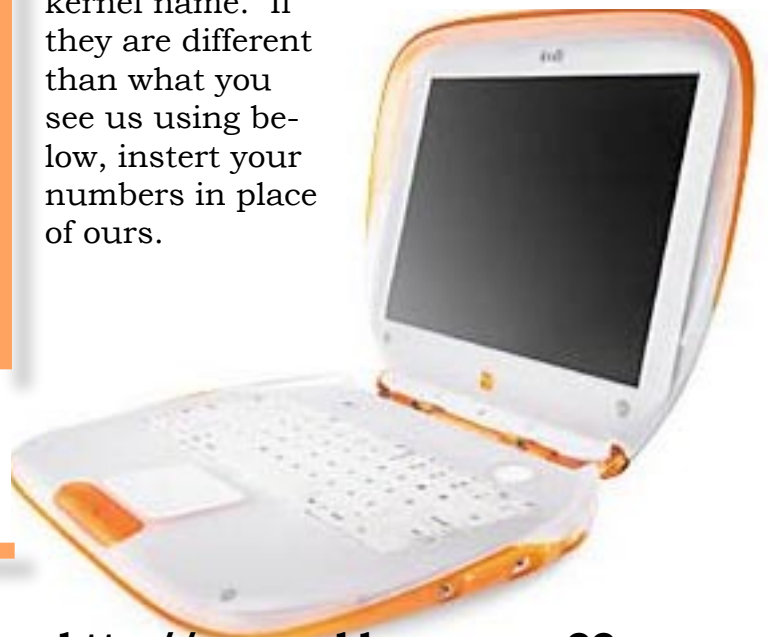
```
ray@hax0r:~$ sudo passwd root  
Password:  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully
```

Note that it first asked for the current password, yet root doesn't seem to have one. I typically enter the password of the user account I am using right now (which was probably created during installation). Next you will enter your new root password twice (for confirmation). Now you can become root when you need to. But let's keep on with using 'sudo' to get a couple more things done.

As part of a standard installation of Ubuntu you don't get the packages you will need to build software. You will have to add these yourself. Some of the things we will need are:

- * Linux kernel source code (specific to the installed kernel)
- * Linux headers (also specific to the installed kernel)
- * Essential tools for building software (make, automake, autoconf, etc)
- * A compiler that will created binaries such as GCC v3.4

Because some of what you will need is specific to the kernel you have installed, you should look at your kernel details before continuing. At your terminal prompt, run 'uname -a'. Note the numbers that follow the kernel name. If they are different than what you see us using below, instert your numbers in place of ours.



We are going to use “apt get” to install everything we need in one big step. Take note that we are not listing every single package you will need. Because “apt-get” has a “smart” processing feature, it should tell you that you will also need several other packages to support what you have chosen. When prompted about packages to be installed, say “Yes”. Also note that we are installing this to an iBook (a Mac) so we need to install the “powerpc” headers in addition to the standard headers package. If you are not running a Mac, leave out the “powerpc” headers package.

```
ray@hax0r:~$ sudo apt-get install linux-source-2.6.12 linux-headers-2.6.12-9
linux-headers-2.6.12-9-powerpc build-essential gcc-3.4
```

After some copying from your CD (or downloading from the net) you should be ready to compile some source code. So now we need to go fetch that code.

You have a couple of choices when you download this source code. You can get it with patches but in unpatched form (this allows you to patch it yourself), you can get it without patches in original form (and download the patches separately) or you can get the code with the patches included AND all ready applied. This is the route we recommend. Use the URL's below to obtain the driver.

Patched Orinoco Drivers Page:

<http://www.kismetwireless.net/download.shtml#orinoco1326>

Direct Download Link:

<http://www.kismetwireless.net/code/orinoco-0.13-26-r1.tar.gz>

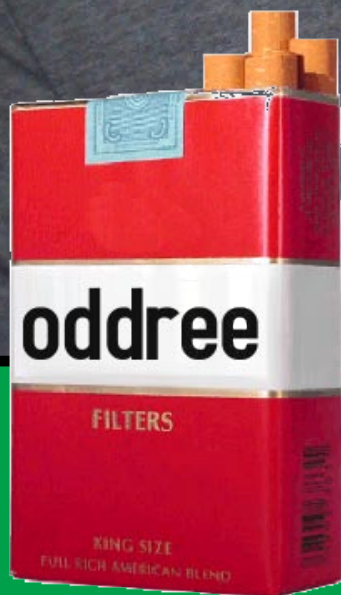
We'll assume that you downloaded that tar.gz file to your Desktop since that's where Mozilla Firefox would have put it. So go ahead and open up a Terminal window and try this ...

```
ray@hax0r:~$ cd Desktop/
ray@hax0r:~/Desktop$ ls
orinoco-0.13-26-r1.tar.gz
ray@hax0r:~/Desktop$ tar -xzf orinoco-0.13-26-r1.tar.gz
ray@hax0r:~/Desktop$ cd /orinoco-0.13-26/
ray@hax0r:~/Desktop/orinoco-0.13-26$ make
```

Now watch in amusement as your driver is built before your very eyes. This shouldn't take too long. Even on old shitty hardware like mine this took a little under a minute. Don't expect to be congratulated or anything. As usual, if you did a job well done you just won't have any error messages to read.



-Smoking! ROFL!-



oddree cigarette company (c) 2006

```
* SurgeonGeneral has joined #oddree
<SurgeonGeneral> heh
<SurgeonGeneral> omg cigarettes are bad for u they
might give you cancer an pregnant wemon shoudnt
smoke either
* SurgeonGeneral has quit IRC (Quit: warnd!)
```


Next we need to make a quick backup of our present drivers because they work. In the event that this new driver causes problems (which is pretty likely) we can always revert back to the “known good ones”. Note that in the example below we trimmed down our prompt so that the commands you need to enter are easier to read.

Our goal is to get into the directory where the wireless modules are stored, create a new directory, and copy the drivers into it. This will be our fail safe.

```
ray@hax0r:~/Desktop/orinoco-0.13-26$ cd /lib/modules/2.6.12-9-powerpc/kernel/
drivers/net/wireless/
ray@hax0r:$ sudo mkdir backup
ray@hax0r:$ sudo cp orinoco*.ko airport.ko hermes.ko ./backup
```

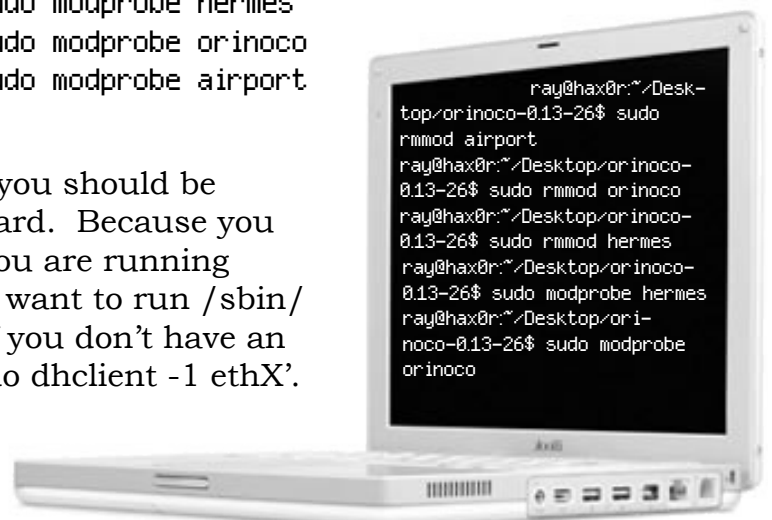
Now that the backup is taken care of, let’s go ahead and copy the new drivers into that directory we just left. We will be replacing all the files we just made a backup of. Note that the second and third lines below are all on one line when you enter them.

```
ray@hax0r:$ cd ~/Desktop/orinoco-0.13-26
ray@hax0r:~/Desktop/orinoco-0.13-26$ sudo cp airport.ko hermes.ko orinoco*.ko
/lib/modules/2.6.12-9-powerpc/kernel/drivers/net/wireless
```

Great! We are ready to put our replacement drivers into use and see if they’re working. In this next step we will drop the current drivers out of use (this will sever your network connection). Then we will use ‘modprobe’ to put the new ones to use. We could also use ‘insmod’ to accomplish this task, but modprobe is better at reporting errors and telling you if something is not going to work as expected.

```
ray@hax0r:~/Desktop/orinoco-0.13-26$ sudo rmmod airport
ray@hax0r:~/Desktop/orinoco-0.13-26$ sudo rmmod orinoco
ray@hax0r:~/Desktop/orinoco-0.13-26$ sudo rmmod hermes
ray@hax0r:~/Desktop/orinoco-0.13-26$ sudo modprobe hermes
ray@hax0r:~/Desktop/orinoco-0.13-26$ sudo modprobe orinoco
ray@hax0r:~/Desktop/orinoco-0.13-26$ sudo modprobe airport
```

If all went well with your modprobes, you should be back in business with your wireless card. Because you dropped the network card entireley, you are running without an address again. You might want to run /sbin/ifconfig and check your IP address. If you don’t have an address, you can obtain one with ‘sudo dhclient -1 ethX’.



Installing Kismet

Now that you have your Mac ready to sniff some packets, let's continue on and install the best damned Linux/UNIX based wireless utility that there is: Kismet. If you're running Ubuntu or some other Debian variant, installation is pretty easy. But first, we need to open up a couple of software repositories.

The short explanation: By default you are only ready to install from a reliable set of standard packages. We need to "unlock" the ability to install some packages that aren't real well tested or even useful to the average Joe (like Kismet). To do this, we will need to edit your "sources.list". We're going to use 'vi', a terminal based editor which is probably older than you. It's not user friendly, so if you would rather use some GUI based editor you are welcome to it.

```
ray@hax0r:~/Desktop/orinoco-0.13-26$ su -  
Password:  
root@hax0r:~# cd /etc/apt/  
root@hax0r:/etc/apt# ls  
apt.conf.d  secring.gpg  sources.list  
trustdb.gpg  trusted.gpg  trusted.gpg  
root@hax0r:/etc/apt# vi sources.list
```

Once we have the file opened up, we want to locate these two lines:

```
# deb http://us.archive.ubuntu.com/ubuntu breezy universe  
# deb-src http://us.archive.ubuntu.com/ubuntu breezy universe
```

Remove the '#' symbols before the 'deb', and save the file. Next we will update your packaging system so it is aware of the new repository.

```
root@hax0r:/etc/apt# apt-get update
```

You're going to see some files getting downloaded and updated. Eventually things will come to a halt and you're read to install Kismet. At the prompt, do the following.

```
root@hax0r:~# apt-get install kismet
```

It should tell you that you need a few other packages (libraries) to use Kismet. If it stops and wants a response, just say "yes" and strike the enter key. It should indicate that the package is being downloaded, unpacked, and configured. Once it comes to a halt, kismet is installed.

Now the slightly tricky part. We need to configure Kismet for the WiFi card you are using. We're going to assume that it's an Airport card using the Orinoco driver.

We need to edit the /etc/kismet/kismet.conf file. We'll use 'vi'.

```
root@hax0r:~# vi /etc/kismet/kismet.conf
```



Now find this line that reads 'suid=' and put a valid username after the '=' sign. A valid user is someone on the system who is not root, and who is not a system user. In other words, use the username of the person you are right now. Ours looks like this:

```
# User to setid to (should be your
normal user)
suiduser=ray
```

Next we need to identify the 'source' for Kismet. This is the most important line in this file. We want to tell it what type of card we are using, what it's 'eth' name is (for a Mac, it should be eth1, where eth0 is the internal wired ethernet device), and lastly a 'nickname' for this device. We used 'Kismet'.

```
source=orinoco,eth1,kismet
```

You are so ready to go. You should save your changes to this file, and quit. Now, if you are still root you should drop back to an average user (yourself). Then run Kismet. Notice we are running it with 'sudo'. They don't want you running Kismet as root for security purposes. But you will find running it as an average user will likely present error messages. So just do it like this ...

```
root@hax0r:~# exit
ray@hax0r:~/$ sudo kismet
```

Now you're running Kismet! Congrats. If you have any problems using it, you should RTFM. Be warned though, when you exit Kismet your WiFi driver will probably be trashed. So keep reading ...

Resetting Your WiFi Driver

When you exit Kismet you may notice a short disclaimer which politely explains that your WiFi card may have been rendered useless. And if you are trying to go about your day surfing porn and downloading your torrents ... but can't ... then we told you so!

Sure, rebooting would fix the problem. But that would get old real quick. What you really need to do is to 'drop' the driver and reload it. We have found that building a script is a nice way to accomplish this task. Open up your favorite text editor (like 'vi') and enter the following:

```
#!/bin/bash
rmmod airport
rmmod orinoco
rmmod hermes
modprobe hermes
modprobe orinoco
modprobe airport
```

Now save the file. Before we can run this script, we need to set it to executable. Here's what we did:

```
ray@hax0r:~$ su -
Password:
root@hax0r:~# vi /bin/resetwifi
root@hax0r:~# chmod 755 /bin/resetwifi
```

Notice we put our script into the /bin directory. We had to be root to put it there. And guess what ... because of what it performs you need to be root to run it! You can use sudo.

```
root@hax0r:~# resetwifi
```

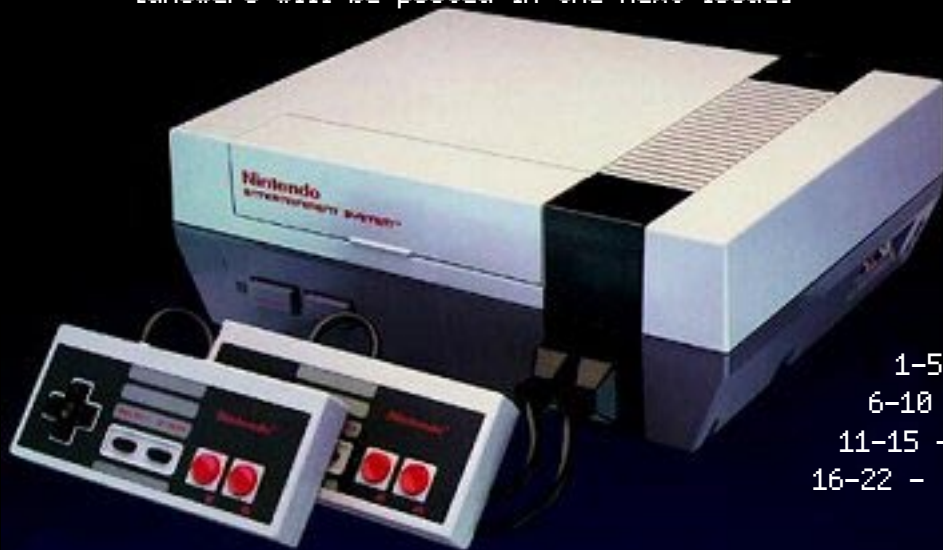
Problems? Get help:
<http://www.oddree.com/forums>

[Ray Dios Haque]



NAME THE LAME GAME

[answers will be posted in the next issue]



How many of these shitty old NES games do you recognize?

- 1-5 - Perhaps this was before your time.
- 6-10 - Did you waste your youth outdoors?
- 11-15 - Nice work. You're a real nerd.
- 16-22 - I guess we should have made it harder.

BUDDHISM: WTF?

LESSON #1 - by [Ray Dios Haque]

Would you like to know a bit about Buddhism without reading a few college textbooks? Me too. Unfortunately, I took the route of college textbooks. Why? Many of the books I have picked up on Buddhism really seemed to insult the intelligence of the “western” reader.

They all had a lot of very nice color photographs, and many had the story of “the Buddha”. But not one book that I could find truly conveyed what Buddhism is all about. Of course, most of my book shopping happens at the half priced book stores which aren’t always known for their quality selections. I was however lucky enough to stumble onto a very good book while visiting the University Of Oregon in their student library (which by the way, is an AWESOME library).

With all that I have learned I have set out to tell our readers all about Buddhism. We’ll give you a little each issue. Incidentally, I have been studying Buddhism for months, and I still consider myself a novice. If you would like to join in and correct me on a few things, send us mail and hop into our forums on oddree.com/forums. I might be able to answer questions that you have, I might not.

Is Buddhism a religion? Many Buddhists say no. We generally recognize religions as the worship of a God (or Gods), the following of a set of teachings, and some sense of faith. In Buddhism, there is no “God”. The Buddha was quite clear about this. In some of his writings he speaks of conversations with his student monks (the “Bhikkhu’s”). One of those monks challenged the Buddha with questions about God. Buddha pretty much challenged the idea of God with the question of “what is the beginning of God?”. In other words, “if God made all of us, who made God?”. Belief in a God is reliant upon faith. Having such faith is challenging, and is quite admirable.

It is also important to note that the Buddha believed in respecting other religions (or any belief structure which promotes a healthy and peaceful relationship to others).

There is also no sense of “faith” in Buddhism. Faith in a higher power is considered “wrong view”. The Buddha felt that belief in God and life after death only fed the desire to beat death with “self preservation”, and kept man from relying on himself to solve life’s problems. When things are going wrong, we might be angry with God. Others might feel at ease, as “this is the plan that God has created for me”. Such views might keep a person from making intelligent decisions about their loved ones, their careers, etc. An arrogant young monk once challenged the Buddha with a series of questions on whether the universe was infinite or not, and if it were not infinite ... what was outside of it? The Buddha sat quietly and didn’t answer. To give an answer would indicate that he knew that answer, and that it was worth knowing. He later approached the monk said to him that he never discussed such things because none of that would lead to ones happiness (and therefore was not really worth knowing).

Another hot topic in religion is the concept of a soul. Buddhists do not believe in the concept of a soul. The Buddha taught that even the sense of “self” is false. This is quite a tough concept to grasp, but we’ll give it a shot.

In Western society we tend to go with the age old saying “I think, therefore I am”. In Buddhism, there is no such belief.

In Buddhism, there is no such belief. You think, because you are a conscious sentient being. Your actions are driven by your mind. And your mind is just another organ for feeling and sensing things. This mind is controlled by your consciousness. So do you think is it our consciousness that is our soul? If so, than perhaps you are more of a Buddhist than you thought. According to Buddhist thought, this consciousness is a collective energy that is transferable at the end of your life. If you are able to meditate at the end of your life, you may have some control over where this energy goes next. But will you be a human in the next life? That all depends on what you did in this life. One important thing to note is that you should be thankful that you were born a human being. As a human, you have great control over how you will live your life. Wild animals spend their entire lives hunting for food, caring for their young, and avoiding the prey that stalk them.

One of the toughest concepts for a Westerner like myself to understand is that of reincarnation. When someone is experiencing a run of bad luck you might hear them say "was it something I did in a previous life?". This is the essence of karma. The word "karma" translates to simply "perform an action". This is a neutral word (not good, not bad). If you are said to have done something good than you have increased your karma. Bad deeds definitely give you a fill of negative karma. The Buddhists believe that your actions in this lifetime will directly dictate the life that you will take on next. If you harm creatures and cause suffering all of your life, you can expect to return as an insect or an animal that lives in suffering.

We often balk at this concept of reincarnation because we don't think it is possible that we were once another human, or a creature running through the forest. But keep in mind that Buddhists only feel that your energy (for lack of a better word) was passed to this life. It is highly unlikely that you would remember a previous life. More likely, you may feel 'imprints' of that former life. Buddhists feel that those imprints guide your personality.

Are you a Buddhist? Do you think you'd ever want to be one? It is said that if you are attempting to live your life by the Buddhist way, than you are a Buddhist. There is no church to attend. No club to join. You just have to practice "the dharma". Dharma simply means "the teachings". There are many lessons that the Buddha left behind for us to follow. Namely, the "Four Noble Truths". Because we are attempting to divvy this out in small doses, our next article in issue #2 will focus solely on the Four Noble Truths.

If you would like to learn more, may we recommend: What the Buddha Taught. This book is available from Amazon.com for a modest price. It's extremely easy to read and if you read the reviews for this book, you will find it's very well received.

Would you like to discuss Buddhism with our readers? Check out the forums at ODDREE.com.

[Ray Dios Haque]

Garden Arrangement & Photos: Rotary Girl

ACRONYM HELL

Across

2. The original and still widely used system for domain name resolution.
5. Loan IP addresses, default gateway, subnet mask, more.
6. You send email with it.
8. Microsofts moronic method of making up your own IP addresses.
10. A company that provides network services.
11. Grab mail from a server, store it locally.
13. Now you can shop online semi-safely.
14. One packet, one time, many voluntary receivers.
15. A new and security driven file system built for Windows NT.
17. The "next generation" addressing and routing protocol.
18. Using several disk drives in tandem with one another for performance or fault tolerance.
19. You connect to these in coffee shops.
21. Thicker optic cable, carries several signals.
22. An increasingly poor choice in wireless network encryption methods.
24. Common for "a network card".
26. A primitive network protocol involving "workgroups" developed by IBM.
29. More secure than telnet.
30. Runs on port 3389.

Down

1. Translates a domain name to an IP address.
3. You can read your mail, but leave it on the server.
4. Microsofts Active Directory uses this..
7. A term for the standard telephone system.
9. Protocol for chatting on DalNet - LOL!
10. Used for voice over IP, and not much else anymore.
12. Those little cards you put in the side of your laptop.
13. Your browser speaks it.
16. Good shielding, costs a bit much (Ethernet).
17. Think 'ping'.
18. An old username and password management protocol traditionally for dial-up connections.
20. Knowing an IP address, and needing a physical one.
23. Irritation or interference generally caused by electrical motors.
25. Remember newsgroups? Me too.
27. A push, twist, and lock on network connector (obsolete).
28. Microsofts protocol for file and printer sharing.

SEND US YOUR MONEY

We employ children.

We live off of Ramen Noodles (not Top Ramen either).

We spend countless hours writing and assembling this fucking magazine.

All for you.

The least you could do is give us a dollar or two of your booze money.

HOW TO HELP

Donate by PayPal to: donations@oddree.com

- 1 - Give a copy of this magazine to everyone you know. If everyone who read this magazine gave us a dollar, we would have like ... ten dollars.
- 2 - Give us a dollar. Most magazines cost you between five and ten bucks, and they suck. Here is one worth reading and it's free. Is a dollar donation too much to ask? You could even give us TWO dollars and we will schedule a party at ODDREE HQ, complete with a cake and disposable party hats (you will not be invited).
- 3 - Buy our merchandise. We have a screening setup, and access to some quality shirts. When you buy one of our shirts, a couple dollars is donated to the magazine. See the website for details.
- 4 - Read this magazine to the elderly. We're not sure how this will help us financially, and old people will likely be confused by the content. But it just seems like a nice thing to do.

WHERE DOES IT ALL GO?

While most charity organizations dwindle your money away on starving children, we will invest your money in our worthy cause. The following will be funded by you:

- (1) Domain and Hosting expenses. We keep these low by taking volunteers to help mirror our magazine. But we still pay to keep our main site up.
- (2) Editing expenses. At present, we are working with materials that were either given to us, or cost us very little. We will use your funds in part to purchase equipment and/or software.
- (3) Rewarding the staff, and readers. If we can possibly afford it, we would like to run promotional contests and perhaps even pay a small amount to our authors.