

Section 3

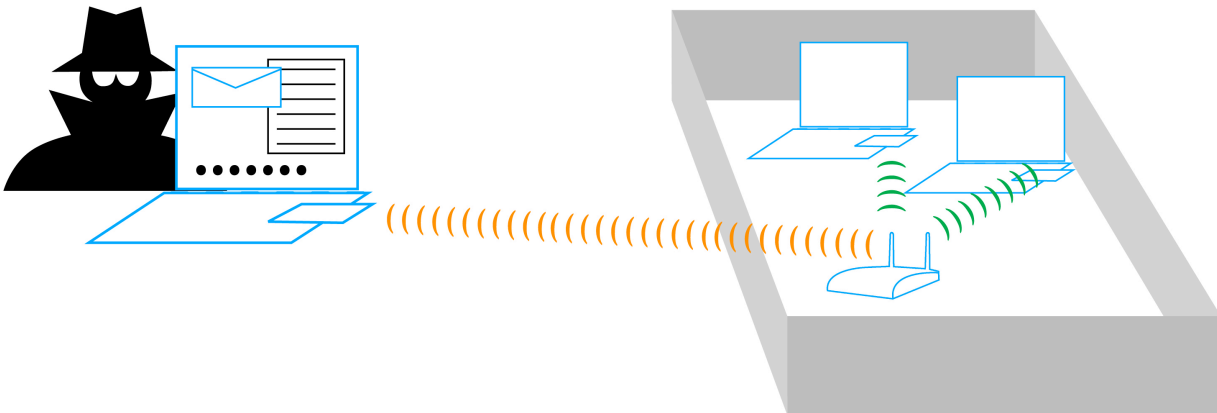
Sniffing and Capturing Data on Open Wireless Networks

Here is where we start into some of the ‘scary’ parts of a Security Assessment. We’ll capture data in a variety of formats and with different tools - both Windows and Linux - to show how vulnerable open wireless LANs can be.

We’ll capture and review Web, VoIP, E-mail, Internet Messaging, and FTP traffic showing not only the data itself, but usually the usernames and passwords associated with the traffic.

This is a great section to use when a client doesn’t think they are very vulnerable. This is also great to run at a conference, airport, or hotspot to see what other people are doing.

With all other tools included in your student kit - you’re only going to be doing these with **PERMISSION!**



Lab 3.1: Capture and Analyze Applications over 802.11



NetResident is an advanced network content monitoring program that captures, stores, analyzes, and reconstructs network events such as e-mail messages, Web pages, downloaded files, instant messages and voice conversations. NetResident uses advanced monitoring technology to capture the required data from the network, saves it to a database, reconstructs it, and displays this content in an easy-to-understand format.

While NetResident is similar to network analyzers in many respects, it focuses on high-level protocols that are used to transfer content over the Internet or LAN. With NetResident, you don't need a profound understanding of networking technologies, have to use complex packet capturing and analysis software, or dig through network packets in order to reconstruct the actual data; NetResident does all the work for you and presents only the Web pages, e-mails, instant messages, or downloaded files as requested. NetResident is used by network administrators to enforce IT policy, parents to monitor their children's communication on the Internet, and by forensic experts to gain crucial information.

Product Information

Source

Tamosoft
Professional Version
\$299.00
www.tamos.com

What you will do in this lab:

- Configure and use NetResident to 'see' network traffic on the Wireless LAN

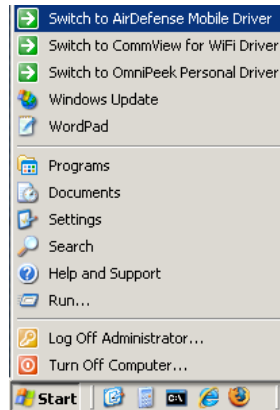
Lab Part 1 - Start a Capture in CommView

If we were using NetResident in a Wired environment, we could be watching all network traffic live. But since we'll be watching a Wireless LAN we'll need to use CommView for WiFi to first capture the packets, then replay them in NetResident.

Step 1. Load Uqibuiti SRC card




Step 2. Go to **Start** → 'Switch to CommView for Wifi Driver'.

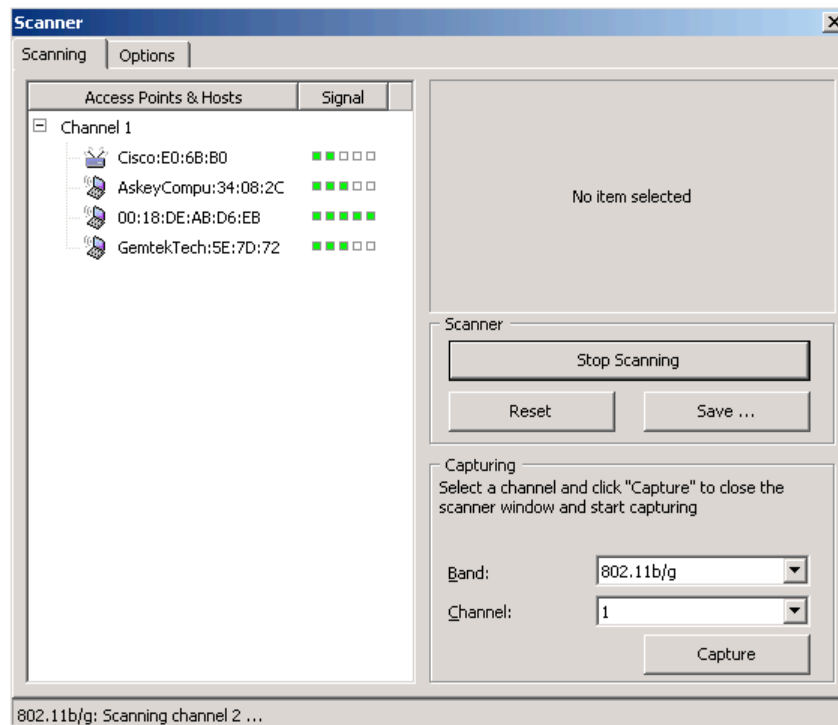


Step 3. Launch **CommView for WiFi**. Start → Wireless Tools → CommView for Wifi



Step 4. Start a Capture with the capture button. 

Step 5. Select **Scan** to start **CommView for WiFi** scanning channels for available 802.11 traffic.




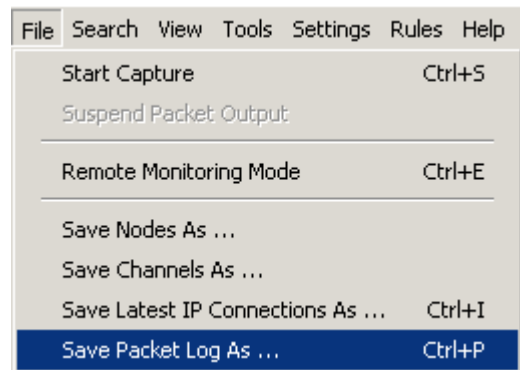
- Step 6. Select the **channel for the classroom AP** then **click Capture**.

Lab Part 2 - Use your Nokia N800 to connect to view a web page, start a WvoIP call, and googletalk to IM.

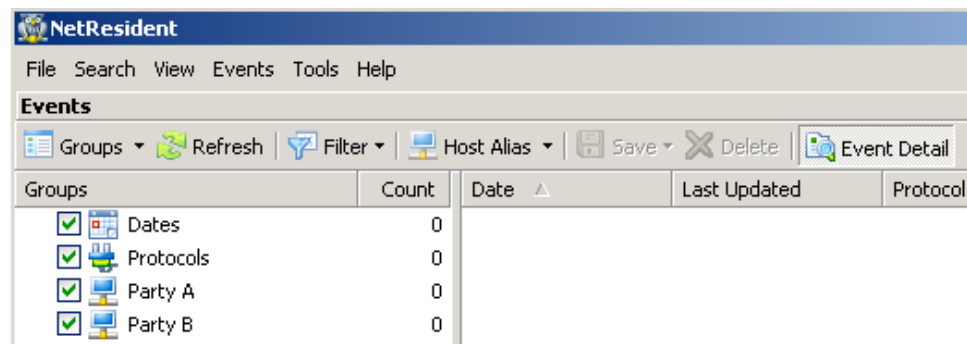
- Step 1. While you are capturing on a selected channel connect your Nokia N800 to the classroom AP and view a website.
- Step 2. Start a Gizmo call on your Nokia to the student sitting next to you.
- Step 3. Open a googletalk IM chat on the Nokia N800 to a student sitting next to you.

Lab Part 3 - Stop the CommView capture and view the application traffic in NetResident

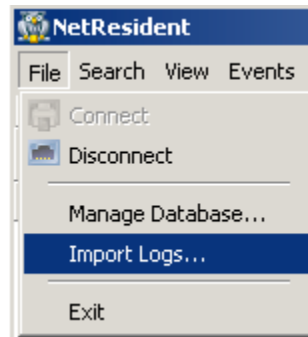
- Step 1. After a while, say 10 minutes, **stop the capture** 
- Step 2. Now save the capture as a log file.



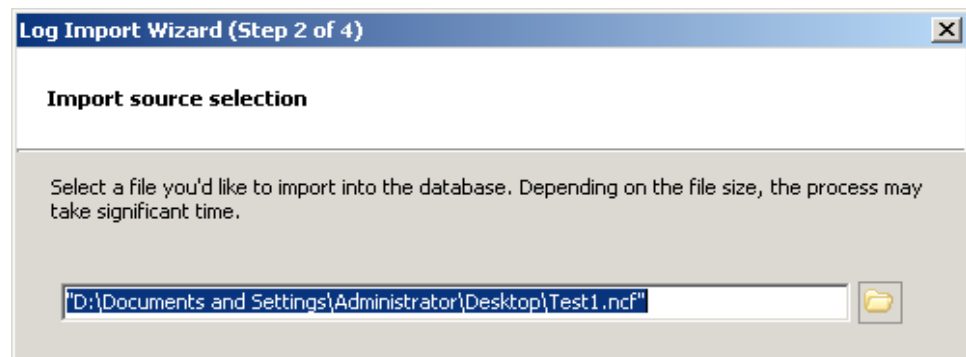
- Step 3. Save the capture file to your desktop to make it easy to find. Give it a name.
- Step 4. **Close CommView for WiFi.**
- Step 5. **Open NetResident. Start → Network Analysis → NetResident**



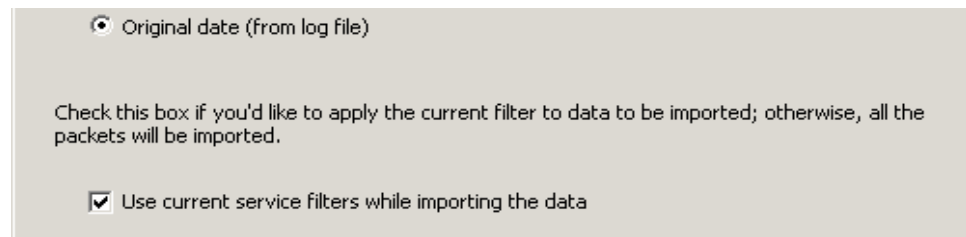
- Step 6. We will now Open the log file we created with CommView for WiFi - and allow **NetResident** to 'replay' the packets into different data streams.



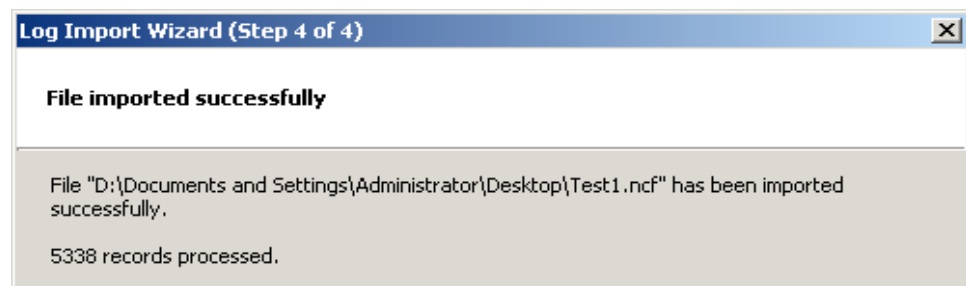
- Step 7. This will start the Log Import Wizard.



- Step 8. Browse to your log file.



- Step 9. Click **Next** to accept defaults.



- Step 10. Click **Finish** to complete the wizard.
- Step 11. This will now open a Capture File.

Groups	Count	Date	Last Updated	Protocol	Party A	Port A	Party B	Port B	Description
Dates	1	5/8/2007 2:09:...	5/8/2007 2:09:14 ...	Web	[10.0.0.138]	1576	[72.14.253.103]	443	SSL session with https://72.14.253.103
Protocols	2	5/8/2007 2:09:...	5/8/2007 2:09:15 ...	Web	[10.0.0.138]	1578	[209.85.139.18]	443	SSL session with https://209.85.139.18
Party A	2	5/8/2007 2:09:...	5/8/2007 2:09:15 ...	Web	[10.0.0.138]	1582	[72.14.253.103]	443	SSL session with https://72.14.253.103
Party B	5	5/8/2007 2:09:...	5/8/2007 2:09:18 ...	Web	[10.0.0.138]	1580	[209.85.139.18]	443	SSL session with https://209.85.139.18
		5/8/2007 2:09:...	5/8/2007 2:09:25 ...	Web	[10.0.0.138]	1603	[209.85.139.18]	80	mail.google.com:GET /mail/?auth=DQA...
		5/8/2007 2:09:...	5/8/2007 2:09:33 ...	Web	[10.0.0.138]	1618	[70.86.31.45]	995	SSL session with https://70.86.31.45:995
		5/8/2007 2:09:...	5/8/2007 2:09:43 ...	VOIP	[10.0.0.138]	41656	[10.0.0.17]	17064	????: A call from ??? 10.0.0.138 to ??? 10.0.0.17
		5/8/2007 2:09:...	5/8/2007 2:09:44 ...	Web	[10.0.0.138]	1623	[64.236.91.24]	80	www.cnn.com:GET /element/sslj/autol/...
		5/8/2007 2:10:...	5/8/2007 2:10:22 ...	Web	[10.0.0.145]	3140	[70.86.31.45]	993	SSL session with https://70.86.31.45:993

Step 12. Scroll through the various conversations, some are HTTP, some VoIP, others IM. Whatever you were doing (as well as your other classmates at the same time on the same channel)

Step 13. Select a **VoIP stream**.

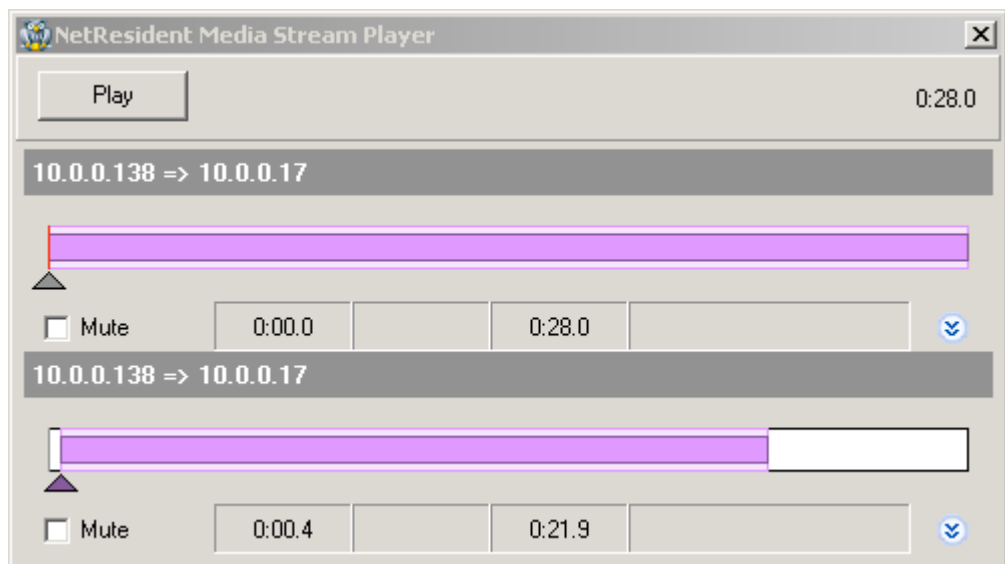
5/8/2007 2:09:...	5/8/2007 2:09:14 ...	Web	[10.0.0.138]	1576	[72.14.253.103]	443	SSL session with https://72.14.253.103
5/8/2007 2:09:...	5/8/2007 2:09:15 ...	Web	[10.0.0.138]	1578	[209.85.139.18]	443	SSL session with https://209.85.139.18
5/8/2007 2:09:...	5/8/2007 2:09:15 ...	Web	[10.0.0.138]	1582	[72.14.253.103]	443	SSL session with https://72.14.253.103
5/8/2007 2:09:...	5/8/2007 2:09:18 ...	Web	[10.0.0.138]	1580	[209.85.139.18]	443	SSL session with https://209.85.139.18
5/8/2007 2:09:...	5/8/2007 2:09:25 ...	Web	[10.0.0.138]	1603	[209.85.139.18]	80	mail.google.com:GET /mail/?auth=DQA...
5/8/2007 2:09:...	5/8/2007 2:09:33 ...	Web	[10.0.0.138]	1618	[70.86.31.45]	995	SSL session with https://70.86.31.45:995
5/8/2007 2:09:...	5/8/2007 2:09:43 ...	VOIP	[10.0.0.138]	41656	[10.0.0.17]	17064	????: A call from ??? 10.0.0.138 to ??? 10.0.0.17
5/8/2007 2:09:...	5/8/2007 2:09:44 ...	Web	[10.0.0.138]	1623	[64.236.91.24]	80	www.cnn.com:GET /element/sslj/autol/...
5/8/2007 2:10:...	5/8/2007 2:10:22 ...	Web	[10.0.0.145]	3140	[70.86.31.45]	993	SSL session with https://70.86.31.45:993

Step 14. Note the Detail and Media stream details available for this IP conversation.

Calling Party	??? 10.0.0.138
Called Party	??? 10.0.0.17
VOIP Protocol	????
Media state	Can be decoded as an audio file

Media Streams				
??? 10.0.0.138				
	10.0.0.138 => 10.0.0.17			
	???? [0]	0:00:00.0	0:00:27.5	Can be decoded as an audio file
??? 10.0.0.17				
	10.0.0.138 => 10.0.0.17			
	???? [0]	0:00:00.4	0:00:21.5	Can be decoded as an audio file

Step 15. Since this audio file can be decoded... lets give it a try by clicking on the Play Button.



- Step 16. You can now listen back to your VoIP conversation.
- Step 17. Look at some of the other types of IP data streams Net Resident can decode.

MSN: Chat with (own passport ryan@inpnet.org)

- Ryan -(ryan@inpnet.org) 5/4/2007 12:35:27 PM	Entered chat
- Ryan -(ryan@inpnet.org) 5/4/2007 12:35:30 PM	well...it is kind of true...

Event Detail

More... ▾

dealmein.pgpartner.com

Check Prices

Kingston 1GB PC4200
DDR2
Price: **\$57.25**

Event Detail

Untitled

```

36031 [15[1*0.0.0.0]0.7948924@skytel.com"11a";Ed Schlichtenmyer"0.0.0.0;"0.0.0.0;"Ed Schlichtenmyer"Ed"0.0.0.0;"7948924@skytel.com"0.0.0.0]
0.0.0.0;"ashland@novell.com";42;"Amy Ahlander"0.0.0.0;"0.0.0.0;"Amy Ahlander"Amy"0.0.0.0;"ashland@novell.com"0.0.0.0]0.0.0.0;"Alicia
Boey"0.0.0.0;"0.0.0.0;"Alicia Boey";"Alicia"0.0.0.0;"aboey@novell.com"0.0.0.0]0.0.0.0;"accounts@stamps.com";4y;"Stamps.com Account Support"0.0.0.0;"0.0.0.0;"
Account Support""com"0.0.0.0;"accounts@stamps.com"0.0.0.0]0.0.0.0;"Adrian Spiga"0.0.0.0;"0.0.0.0;"Adrian
Spiga";"Adrian"0.0.0.0;"adrian@aimagnet.com"0.0.0.0]0.0.0.0;"Adrian Spiga"0.0.0.0;"0.0.0.0;"Adrian Spiga"Adrian"0.0.0.0;"adrian@aimagnet.com"0.0.0.0]0.0.0.0;"Alan Hall"0.0.0.0;"0.0.0.0;"Alan Hall";"Alan"0.0.0.0;"alhall@novell.com"0.0.0.0]
0.0.0.0;"alin@neobytesolutions.com";3q;"0.0.0.0;"0.0.0.0;"alin";"alin"0.0.0.0;"alin@neobytesolutions.com"0.0.0.0]0.0.0.0;"amarquez@novell.com";2a;"Andy Marquez"0.0.0.0;"0.0.0.0;"Andy
Marquez";"Andy"0.0.0.0;"amarquez@novell.com"0.0.0.0]0.0.0.0;"anna@vsa-bility.com";3u;"Anna Martin"0.0.0.0;"0.0.0.0;"Anna Martin";"Anna"0.0.0.0;"anna@vsa-bility.com"0.0.0.0]
0.0.0.0;"art@allencorpus.com";4b;"Art Allen"0.0.0.0;"0.0.0.0;"Art Allen";"Art"0.0.0.0;"art@allencorpus.com"0.0.0.0]0.0.0.0;"art@inpnet.org";4t;"Art Allen"0.0.0.0;"0.0.0.0;"Art
Allen";"Art"0.0.0.0;"art@inpnet.org"0.0.0.0]0.0.0.0;"sachae@novell.com";1;"Alan SCHAEFS"0.0.0.0;"0.0.0.0;"Alan SCHAEFS";"Alan"0.0.0.0;"sachae@novell.com"0.0.0.0]
0.0.0.0;"awierzbicka@novell.com";1a;"Agnieszka Wierzbicka"0.0.0.0;"0.0.0.0;"Agnieszka Wierzbicka";"Agnieszka"0.0.0.0;"awierzbicka@novell.com"0.0.0.0]

```

Here is a list of all the Protocols NetResident can decode.

Protocol	Description
<input checked="" type="checkbox"/> FTP	FTP Protocol
<input checked="" type="checkbox"/> Web	World Wide Web Protocol
<input checked="" type="checkbox"/> ICQ/AIM	ICQ and AIM messaging
<input checked="" type="checkbox"/> Irc	Internet relay chat protocol
<input checked="" type="checkbox"/> Mail	Mail protocols (POP3, SMTP, IMAP)
<input checked="" type="checkbox"/> MSN	MSN protocol
<input checked="" type="checkbox"/> News	News protocol (NNTP)
<input checked="" type="checkbox"/> Telnet	Telnet Protocol

Lab 3.2: Capture and Analyze POP3 Email Traffic

What you will do in this lab:

- Connect to a POP3 server to check incoming email
- Capture passwords using Winsniffer

Lab Part 1 - Capturing POP3 passwords using Winsniffer

- Step 1. Connect Ubiquiti card to classroom AP.



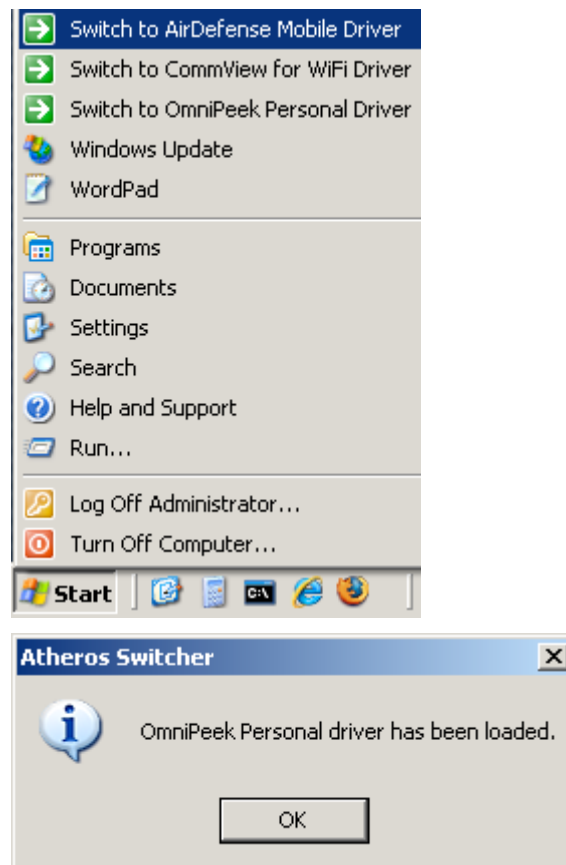
- Step 2. Launch *winsniffer*. Start → Network Analysis → *winsniffer*
- Step 3. Let instructor know that you are ready to capture passwords.
- Step 4. Instructor will now access a variety of sites that need passwords; FTP, IM, e-Mail, network shares, etc.
- Step 5. Verify passwords were captured in Winsniffer.

Lab Part 2 - View pop3 email content with Omnipeek

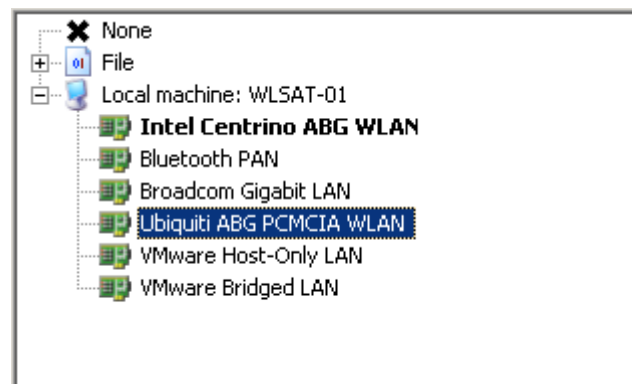
- Step 1. Insert the Ubiquiti Card in the PCMCIA Slot on the side of your WLSAT Laptop. (you can use either the small 2.2dBi or the 5dBi antennas - note the arrow on the bottom pointing to the antenna jack to use)



- Step 2. Go to **start** → 'Switch to OmniPeek Personal Driver'.



- Step 3. Launch *OmniPeek Personal.start* → *Wireless Tools* → *wildPackets OmniPeek Personal*.
- Step 4. Choose the *Ubiquiti ABG PCMCIA WLAN* as the adapter to use. Then click *OK* to continue.



- Step 5. Start a capture on channel *6*.
- Step 6. View capture in *OmniPeek* and verify email content was able to be viewed.

Lab 3.4: Using three AirPcap's to capture ALL the packets as a device roams across channels DEMO

Instructor will Demo Airpcap Trio

This lab shows a USB hub, with three AirPcap devices all connected at the same time. Using a 'Virtual' NIC interface, all three can be combined into a single packet stream. Thus showing all packets from channels 1, 6 and 11 simultaneously in a single packet trace. What a great way to 'see' a STA (Client) roaming from one AP to the next.

When monitoring on a single channel is not enough, multiple AirPcap adapters can be plugged into a hub or your laptop and used to capture traffic simultaneously on different channels. The AirPcap driver provides support for this operation through our **Multichannel Aggregator (MCA)** technology, that exports multiple AirPcap adapters as a single capture stream. Other solutions implement multi-channel monitoring using a single radio and channel-hopping. This means that you are monitoring each channel only part of the time, missing important packets.

Lab 3.5: Capture and analyze web traffic using Driftnet and Etherape



Etherape allows you to see, in real-time, the following: bandwidth consumption, established communications, threats of an attack, etc.

Driftnet is a tool designed to capture and display images found in network traffic. It is designed to pick up all images it can see in real-time and either shows them on screen using webcollage or saves them to folder.

Product Information

Source

Open Source GPL

<http://www.ex-parrot.com/~chris/driftnet/>

<http://etherape.sourceforge.net/>

Where, When, Why

As an analyst, it is important to know the tools that are available to view open network traffic. Information gathered by using tools such as these can aid an attacker in further exploiting the network. If the traffic is unencrypted, anyone with the right tools can see this traffic without being authenticated.

Driftnet's uses may be considered controversial. It can be used to spy on others browsing habits, help determine the cause for major bandwidth consumption, or serve as an alternative to searching through log files to validate those in violation of corporate security policy.

Usage and Features

- Monitor network usage
- Determine how much time is wasted on unproductive habits on network
- Spy on a user

Requirements / Dependencies

- Linux with Libpcap, Libjpeg, Libungif, and GTK installed

Where to Go for More Information

<http://www.ex-parrot.com/~chris/driftnet/>

<http://etherape.sourceforge.net/>

What you will do in this lab:

- View and save images found in wireless traffic

Lab Part 1 - Using Driftnet

Step 1. Reboot into *Backtrack Linux* on your WLSAT Laptop.



Step 2. To open a command prompt **click** on the **terminal icon** in the lower left-hand corner.



Step 3. To view all the available options and parameters of *Driftnet* type **driftnet -help**.

```
bt ~ # driftnet --help
driftnet: unrecognised option --
driftnet, version 0.1.6
Capture images from network traffic and display them in an X window.

Synopsis: driftnet [options] [filter code]

Options:

-h          Display this help message.
-v          Verbose operation.
-i interface Select the interface on which to listen (default: all
            interfaces).
-p          Do not put the listening interface into promiscuous mode.
-a          Adjunct mode; do not display images on screen, but save
            them to a temporary directory and announce their names on
            standard output.
-m number  Maximum number of images to keep in temporary directory
            in adjunct mode.
-d directory Use the named temporary directory.
-x prefix  Prefix to use when saving images.
-s          Attempt to extract streamed audio data from the network,
            in addition to images. At present this supports MPEG data
            only.
-S         Extract streamed audio but not images.
-M command Use the given command to play MPEG audio data extracted
            with the -s option; this should process MPEG frames
            supplied on standard input. Default: `mpg123 -'.
```

Filter code can be specified after any options in the manner of tcpdump(8).
The filter code will be evaluated as `tcp and (user filter code)'

You can save images to the current directory by clicking on them.

Step 4. Create a directory for *Driftnet* to dump into:

```
mkdir /tmp/driftnet_images
```

- Step 5. Now *Driftnet* will capture all images it sees that are destined to a common access point. We need to make sure that we associated with the access point first but WE DON'T WANT AN IP ADDRESS! You can do so by using your discovery tool of choice (airodump-ng, kismet, network stumbler, etc.) For example, if I want to see all images on the HOTlabs network I would type the following:

```
./ath_normal1 ← just in case your card is in monitor mode
```

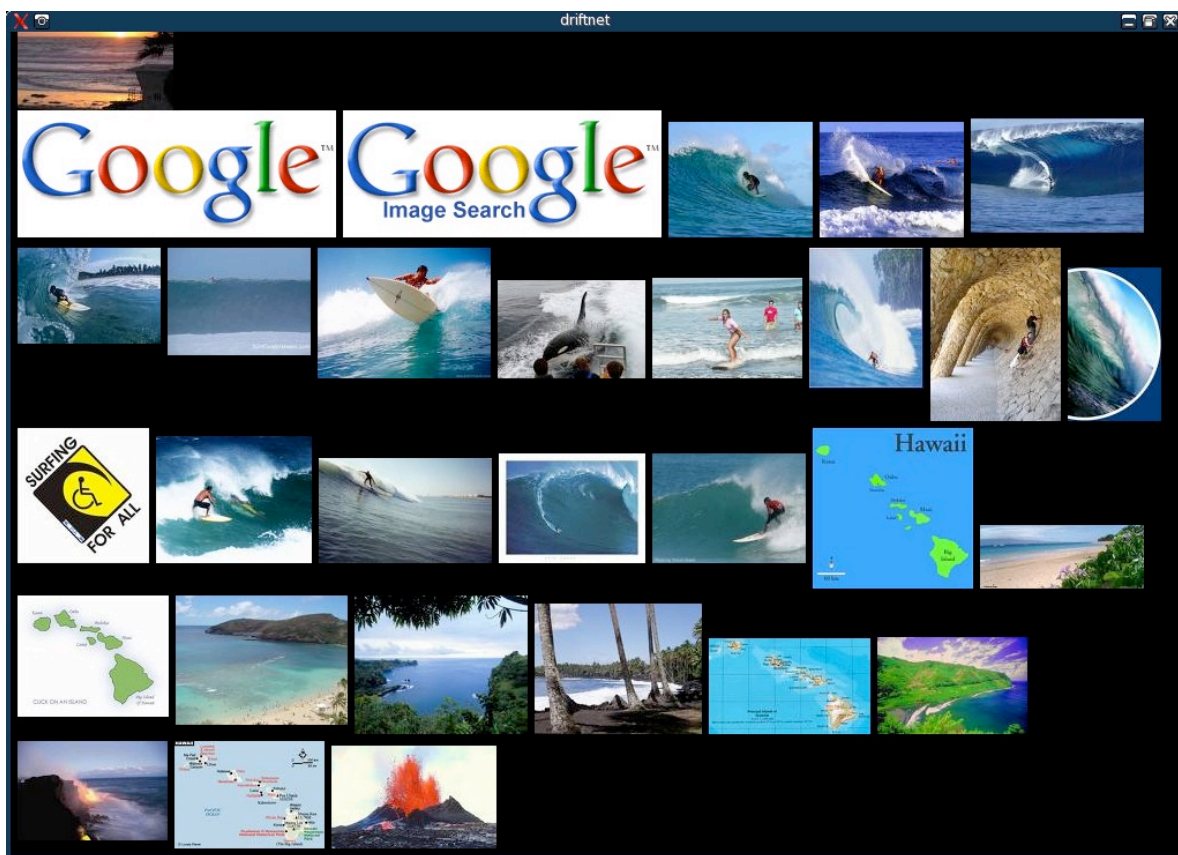
```
ifconfig ath0 down
iwconfig ath0 essid "HOTlabs"
ifconfig ath0 up
```

NOTE: Your ath0 interface should *NOT* be in monitor mode for this tool to work properly. If it is in monitor mode you will get a link type error. If you get that error, simply type `./ath_normal1` and that script will put your card into the default managed mode.

- Step 6. Now we can simply pass that directory to driftnet and tell it what interface to listen on and the program will do the rest.

At the command prompt type:

```
driftnet -i ath0 -d /tmp/driftnet_images
```



It is obvious that someone is searching for surf related topics on Google!

NOTE: You will want to make the window as big as it can go to avoid truncation of any images. If you want to save any of the images, you can simply click on the image and it will save into the folder from which you ran driftnet. Driftnet will delete all images that are found in the folder when driftnet closes to save space. If you want to save any images then you need to move them to another folder before driftnet closes.

Lab Part 2 - Using Etherape

Step 1. To open a command prompt **click** on the **terminal icon** in the lower left-hand corner. 

Step 2. Type **etherape --help** to get a list of all options and parameters.

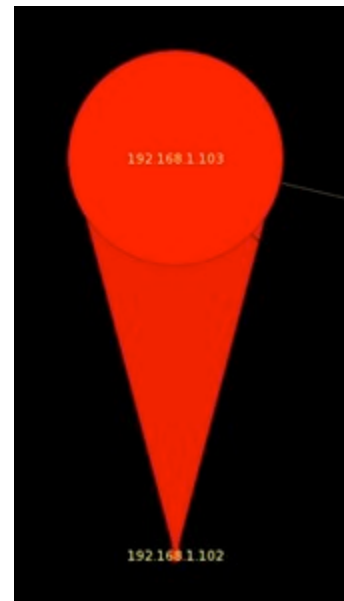
Step 3. To view traffic on either the channel your card is in or on the network that you are connected to simply type **etherape** at the command prompt.

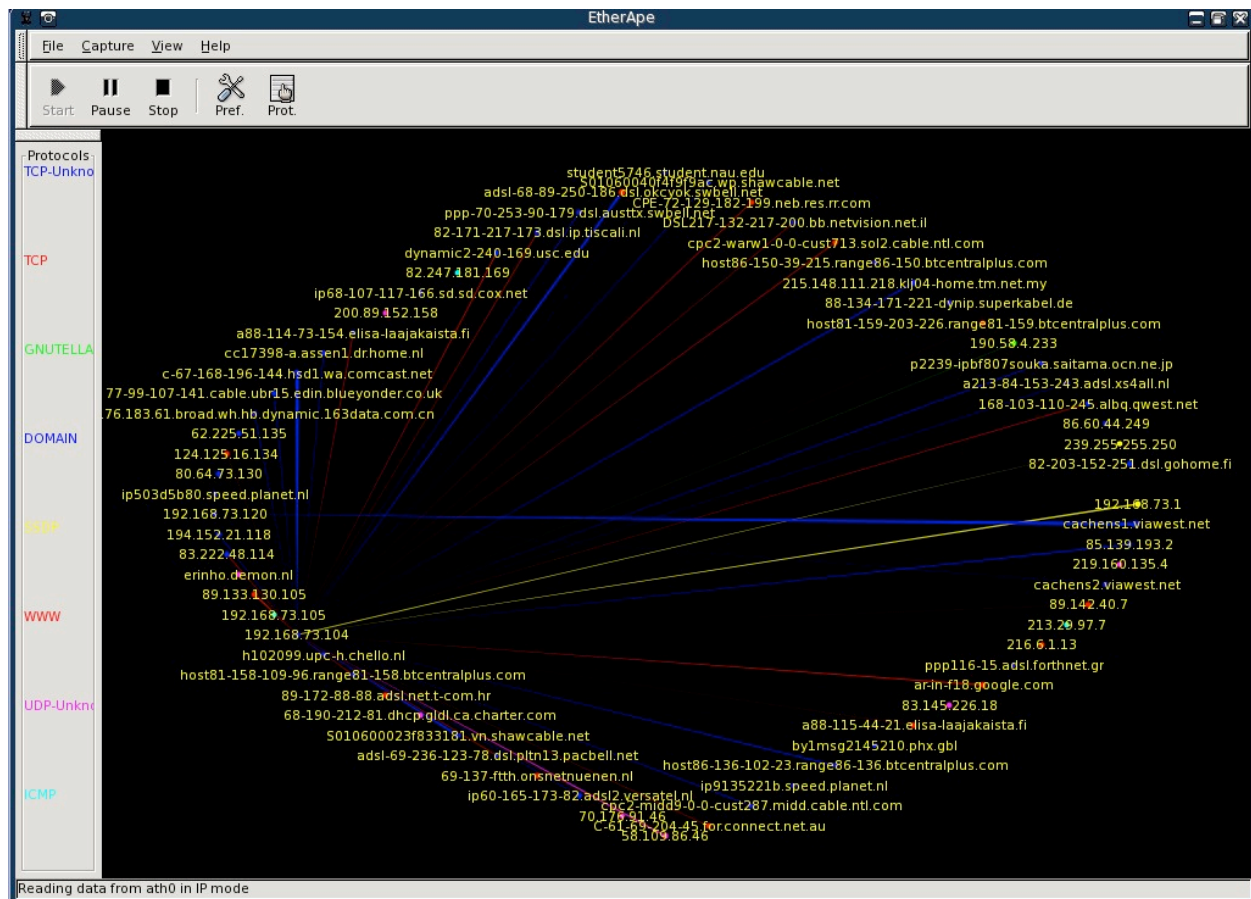
NOTE: If you are connected to a switched network then you will only be able to see broadcast traffic unless you are on a spanned port or are poisoning a host in order to route their traffic to your machine. This exercise is assuming that you are using a wireless card to view wireless traffic.

Step 4. From this point on you are seeing, in real-time, what is happening on the network or 'in the air'. The protocols are color coded off to the left and the bandwidth consumption is indicated by the increasing and decreasing shapes next to the ip addresses/hostnames/domain names.

This would indicate that 192.168.1.103 is receiving a lot of traffic from 192.168.1.102.

To see what a large download of a shockwave file looks like browse to www.2advanced.com and enter the site. At first you will notice a lot of traffic and bandwidth are used but when you visit the site a second time not that much are used. That is due to your browser caching the site locally on your own computer so that it doesn't have to reuse resources.





By using *Etherape* with a wireless card, you can see that it becomes very difficult to interpret everything but it offers a way to determine very quickly who the active hosts / potential targets are without being associated with any access point.

To further utilize *Etherape* you may **double click in the protocol color coding window** to the left in order to view what types of traffic are used the most.

The screenshot shows the 'EtherApe: Protocols' window with a table of traffic statistics. The table has five columns: Protocol, Inst Traffic, Accum Traffic, Last Heard, and Packets. The protocols listed are DOMAIN, GNUTELLA, ICMP, SSDP, TCP, TCP-Unknown, UDP-Unknown, and WWW.

Protocol	Inst Traffic	Accum Traffic	Last Heard	Packets
DOMAIN	0 bps	6.729 Kbytes	9" ago	43
GNUTELLA	0 bps	719 bytes	12" ago	12
ICMP	0 bps	546 bytes	1'58" ago	6
SSDP	0 bps	1.117 Kbytes	41" ago	4
TCP	1.113 Kbps	36.484 Kbytes	0" ago	562
TCP-Unknown	998 bps	623.229 Kbytes	0" ago	1110
UDP-Unknown	365 bps	8.818 Kbytes	1" ago	43
WWW	0 bps	516.951 Kbytes	17" ago	375

- Step 5. For a graphical view of network usage, ***Etherape*** is perfect. However, if you are looking to analyze the traffic in more detail you may use your favorite protocol analyzer.

NOTE: you may also import traffic gathered with a protocol analyzer into ***Etherape*** from the command line with the **-r** switch; ***Etherape*** will then proceed to incrementally display the traffic as if it's viewing the traffic in real-time as well.

What you learned in this Lab:

In this Lab you learned to use ***Etherape*** and ***Driftnet*** to:

- Graphically view network traffic in real-time
- View and save images that are in transit