5.2.1

Network Sniffing - HTTP Sessions

(Wireshark)

June 2008

Laboratory Overview

Objective

At the end of this lab students will have the ability to grab a web page off the network and capture it to a file for latter viewing.

Information for Laboratory

Students will require a platform with Wireshark functionality and another with a browser client on a non-switched or wireless network.

Student Preparation

The student will have reviewed:

http://www.wireshark.org web site
http://www.wireshark.org/faq.html
http://www.wireshark.org/docs/

The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Instructor Preparation

Before class, the instructor or a lab assistant will set up a Linux or Windows platform with Wireshark. Binaries are available from http://www.wireshark.org/download.html.

Estimated Completion Time

60 - 90 Minutes

HTTP Sniffing

Having the ability to look at and analyze packets on a network can be very informative. There are many reasons an administrator may want to see what is traversing the network. On a wireless or non-switched network, packets can be seen by both those that have legitimate needs and those that are up to nefarious activities.

Capturing web pages requires an understanding of how they are processed by the server and rendered by the browser. We will follow a http stream and see what can be displayed easily and that which requires more effort. The more highly formatted the page the harder it will be to reproduce. Products like wget (http://www.gnu.org/software/wget/) can grab web sites for off-line viewing. Wireshark will grab the stream and leave it up to the user to assemble.

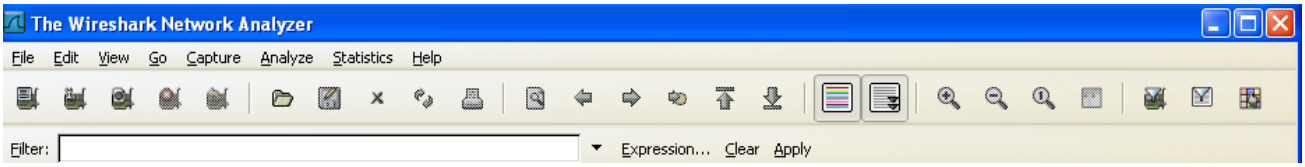
Network Analysis Software

There are several different programs, both commercial and shareware/freeware that incorporate the many different Packet Sniffing techniques on the market today (some are).

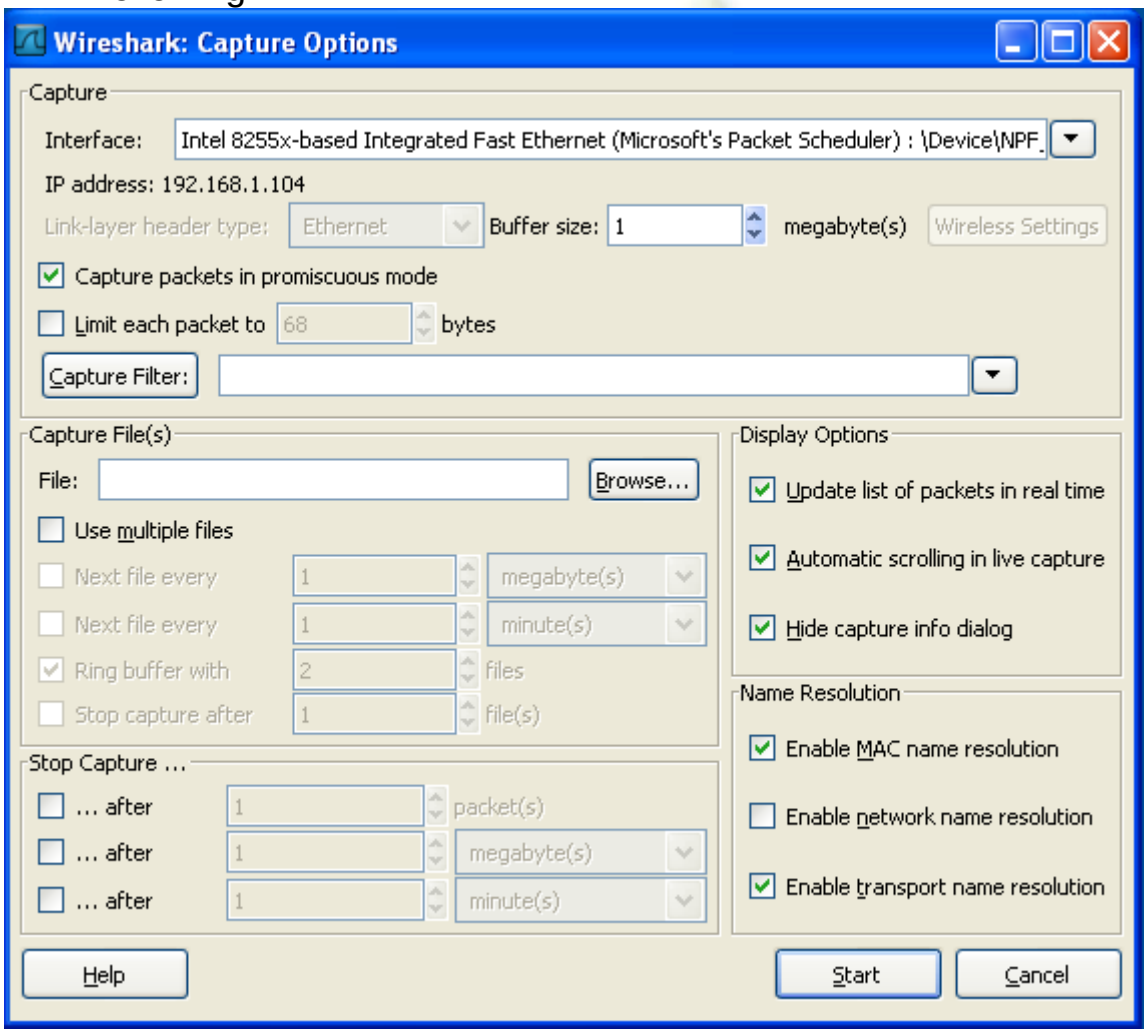
Wireshark
dsniff
Windump
Analyzer
more http://www.mirrors.wiretapped.net/security/packet-capture/

Step I: Open the Wireshark client.

Begin capturing packets by clicking on **Capture** on the menu bar, then clicking on Start. Note the keyboard shortcut CTRL-K will also start capturing packets.



You should see the capture options dialog box similar to the following:

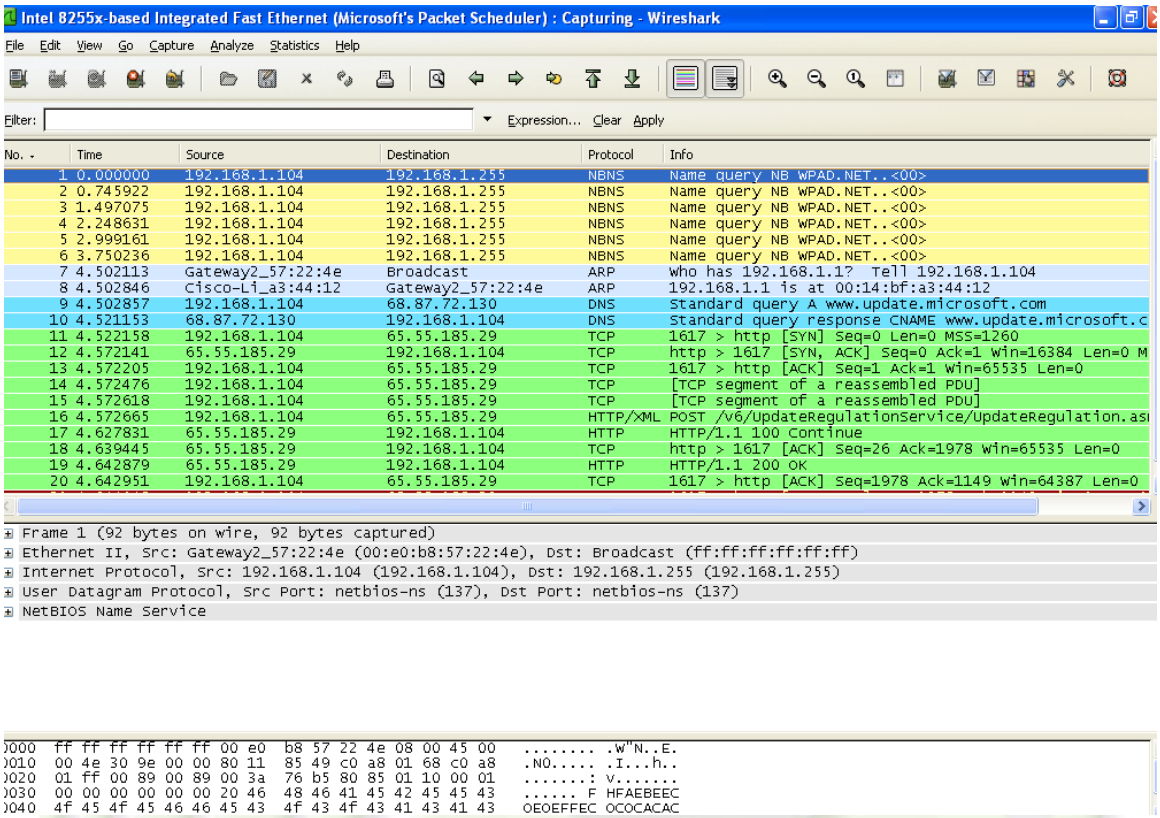


You may specify the name of a capture file for retention and later viewing. Be sure the interface is selected properly, but otherwise accept the defaults.

Step 2:

Click on the Start button.

You should now see something similar to the the following:
Please Note: Output may vary greatly due to lab environment!



Step 3: Initiate HTTP session

On your machine establish a http session. You may want to click on the Refresh button once you've established a connection with a web site.

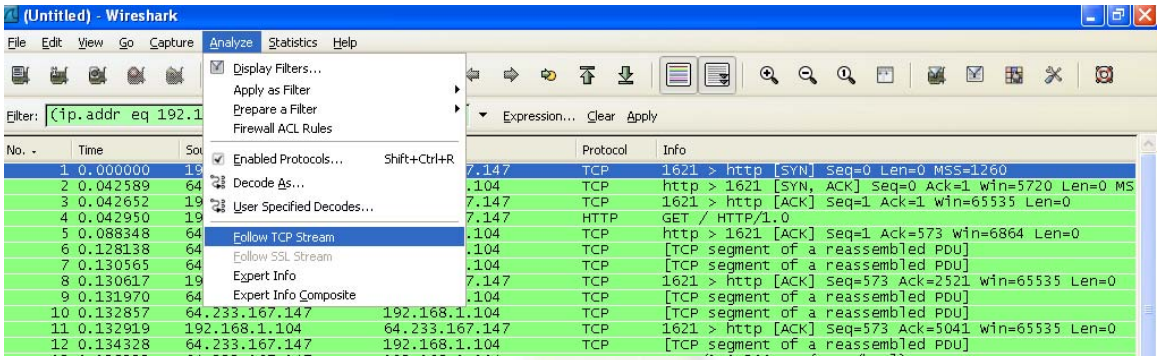
Step 4: Stop Capture

Stop the Wireshark capture either by pressing Ctrl-E or clicking on the Capture menu item and clicking on the Stop option. After the capture has been stopped, Wireshark should be populated with your web site browsing as well as any broadcast network activity within your lab.

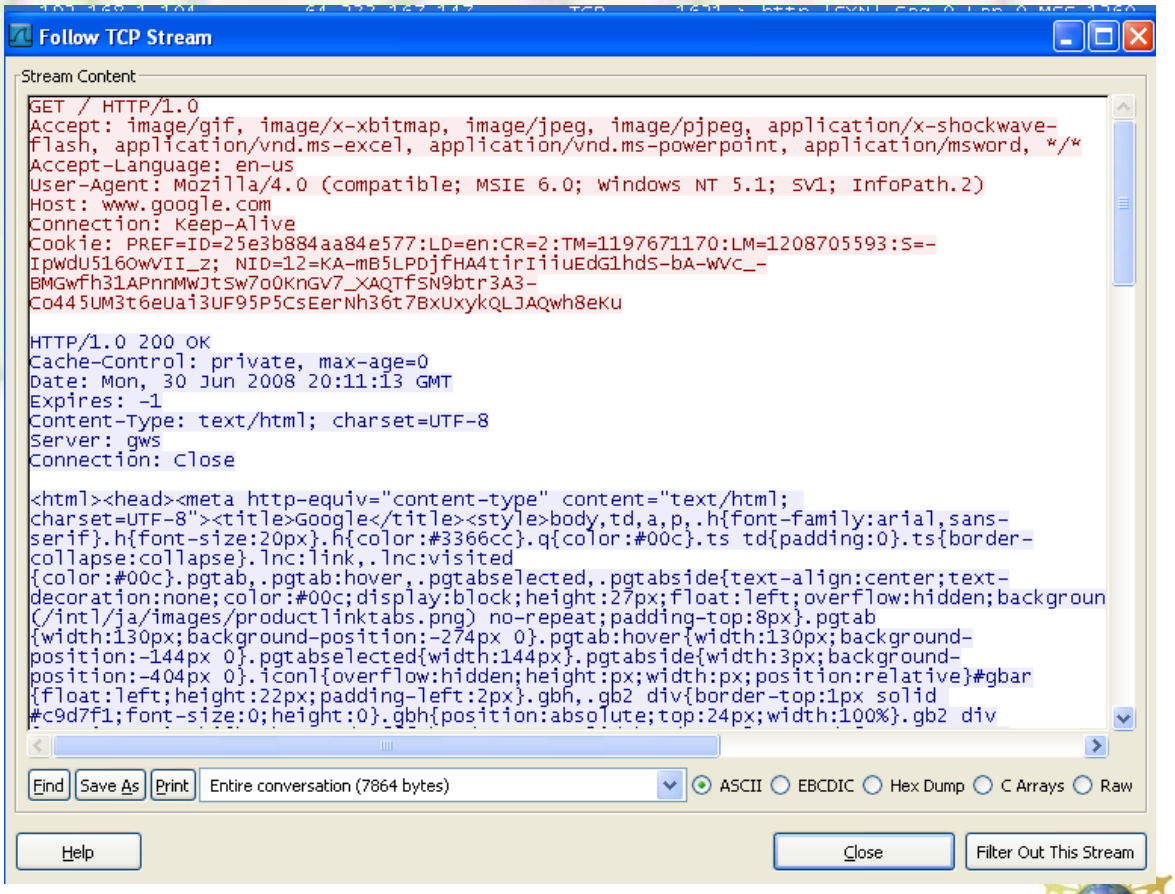
Step 5: Analyze Stream

1) Select Analyze
2) Select Follow TCP Steam

See a screen shot below for an example



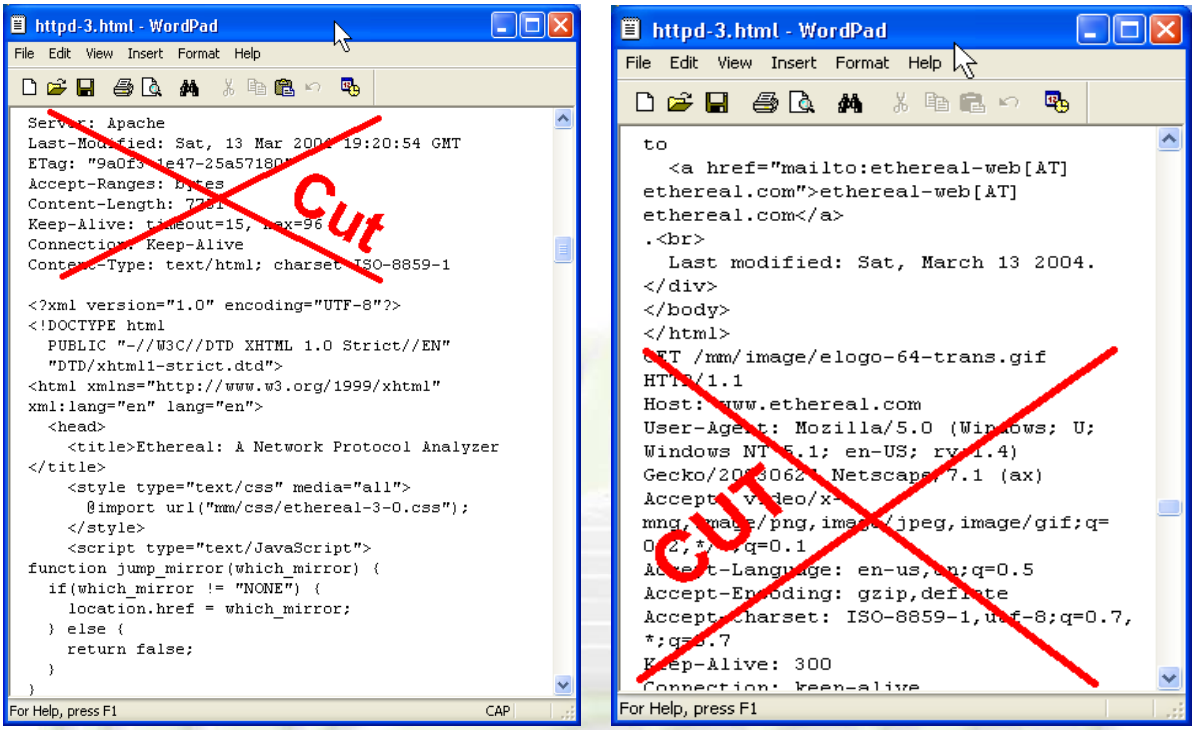
The program will process the stream and display the contents: Your screen will look similar to the one shown below:



1) Click “Save As” to save the file
2) Why is some of the file in red and some in blue?

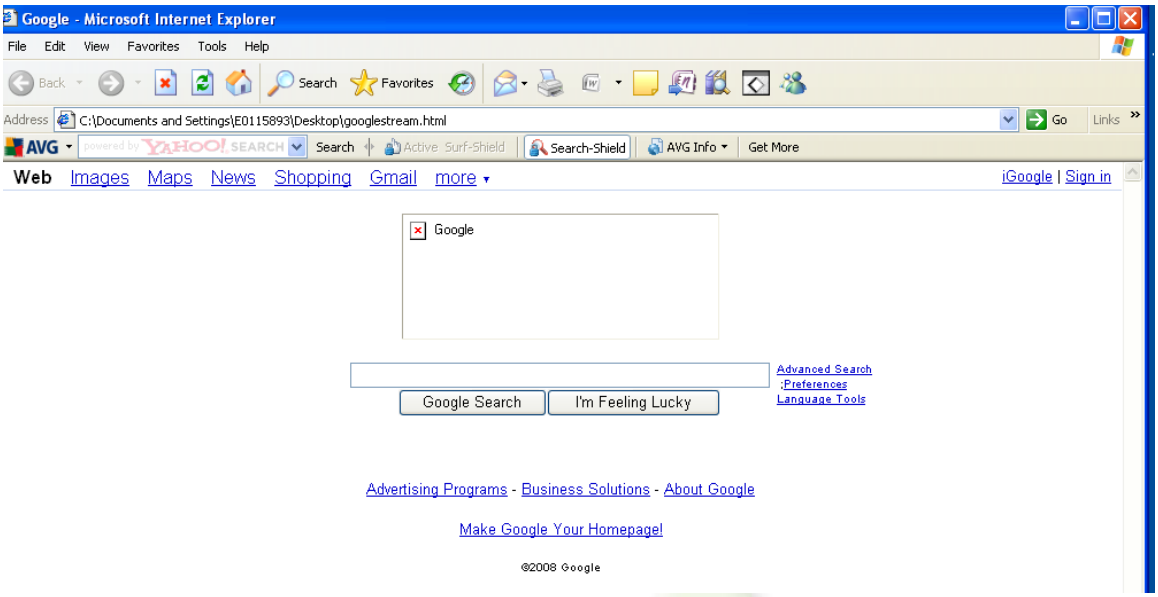
Step 6: Open the html file in a text editor (such as WordPad)

Cut out everything that is not part of the html page. Pages can start with <html> or <?xml> and end with </html>.



Save the edited file as testfile.html.
The saved file should look like a html file.

Step 7: Open the html file in a text Browser.
In this example, the main page from Google.com was captured, edited and saved. Here is sample screen shot below:



Step 8:

Get a screen shot of your edited html page as it is displayed by a browser. Save to a Word document, put your name in the document and print off for your instructor.

1) What happened to the formatting and images?
2) Can you capture the images and have the page display correctly?
3) What can be gleaned by capturing http traffic?

Summary Discussion

Analyzing traffic on a network can provide a clearer picture of what is happening. It can be used to follow break-in attempts as well as spying on users. If you are running the packet sniffer on against your machine you can see what the applications are doing. Who does your machine talk to when it boots? Does it call home? This has been a quick look at one of the many features of network analyzers.

Appendix:

This lab was developed using Wireshark Version 0.99.6a (SVN

Rev 22276), which can be obtained from:

www.wireshark.org

-or-

http://www.download.com

Note that Ethereal, in particular WinPcap, may have difficulty starting a capture from a wireless network adaptor. Click off the promiscuous mode on the capture dialog page for your wireless adapter and it should work.

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).