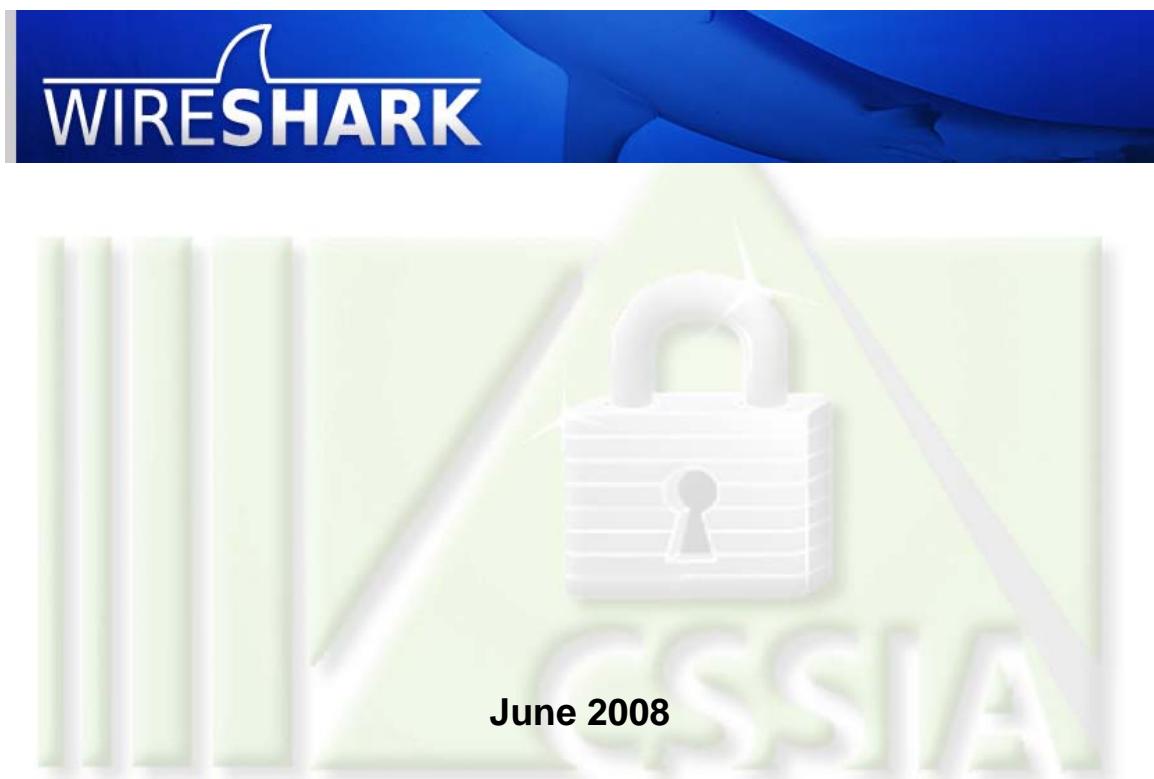


**5.2.1**

## **Network Sniffing - HTTP Sessions**

**(Wireshark)**



## 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**

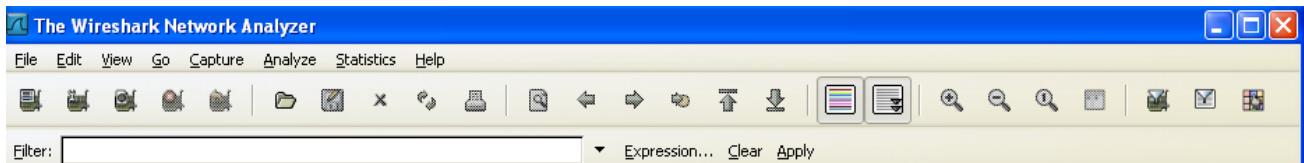
There are several different programs, both commercial and shareware/freeware that incorporate the many different Packet Sniffing techniques on the market today (some are).

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

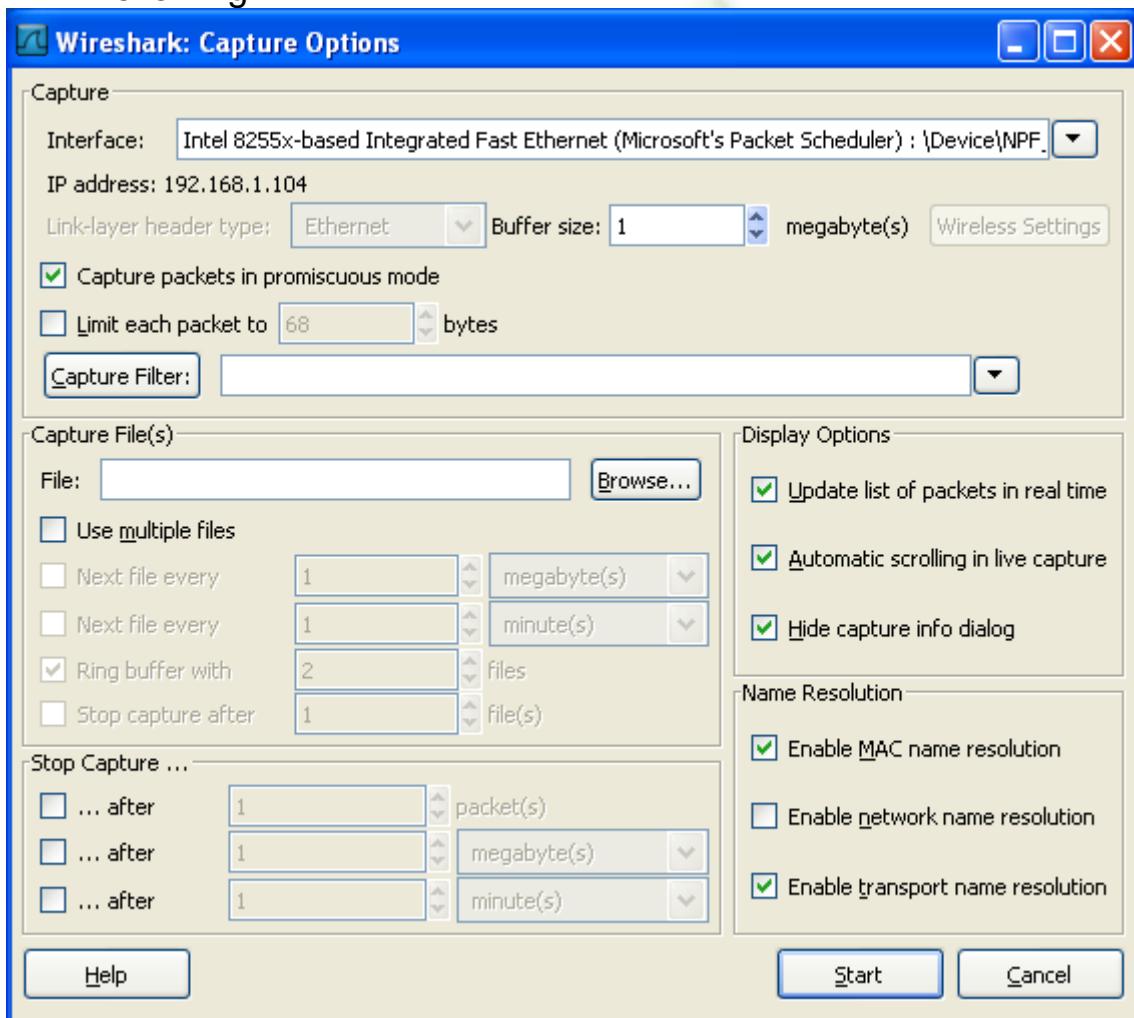


## Step I: Open the Wireshark client.

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!

The screenshot shows the Wireshark interface with a list of captured network frames. The columns include No., Time, Source, Destination, Protocol, and Info. Key entries include a Name query for 'WPAD' and a DNS request for 'www.update.microsoft.com'. Below the list is a detailed hex dump of frame 1.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.104	192.168.1.255	NBNS	Name query NB WPAD.NET..<00>
2	0.745922	192.168.1.104	192.168.1.255	NBNS	Name query NB WPAD.NET..<00>
3	1.497075	192.168.1.104	192.168.1.255	NBNS	Name query NB WPAD.NET..<00>
4	2.248631	192.168.1.104	192.168.1.255	NBNS	Name query NB WPAD.NET..<00>
5	2.999163	192.168.1.104	192.168.1.255	NBNS	Name query NB WPAD.NET..<00>
6	3.750236	192.168.1.104	192.168.1.255	NBNS	Name query NB WPAD.NET..<00>
7	4.502113	Gateway2_57:22:4e	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.104
8	4.502846	Cisco-L1_a3:44:12	Gateway2_57:22:4e	ARP	192.168.1.1 is at 00:14:b1:a3:44:12
9	4.502857	192.168.1.104	68.87.72.130	DNS	Standard query A www.update.microsoft.com
10	4.521153	68.87.72.130	192.168.1.104	DNS	Standard query response CNAME www.update.microsoft.c
11	4.522158	192.168.1.104	65.55.185.29	TCP	1617 > http [SYN] Seq=0 Len=0 MSS=1260
12	4.572141	65.55.185.29	192.168.1.104	TCP	http > 1617 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 M
13	4.572205	192.168.1.104	65.55.185.29	TCP	1617 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
14	4.572476	192.168.1.104	65.55.185.29	TCP	[TCP segment of a reassembled PDU]
15	4.572618	192.168.1.104	65.55.185.29	TCP	[TCP segment of a reassembled PDU]
16	4.572665	192.168.1.104	65.55.185.29	HTTP/XML POST	/v6/UpdateRegulationservice/UpdateRegulation.asi
17	4.627831	65.55.185.29	192.168.1.104	HTTP	HTTP/1.1 100 Continue
18	4.639445	65.55.185.29	192.168.1.104	TCP	http > 1617 [ACK] Seq=26 Ack=1978 win=65535 Len=0
19	4.642879	65.55.185.29	192.168.1.104	HTTP	HTTP/1.1 200 OK
20	4.642951	192.168.1.104	65.55.185.29	TCP	1617 > http [ACK] Seq=1978 Ack=1149 win=64387 Len=0

Frame 1 (92 bytes on wire, 92 bytes captured)  
Ethernet II, Src: Gateway2\_57:22:4e (00:0:b8:57:22:4e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.255 (192.168.1.255)  
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)  
NetBIOS Name Service

Hex	Dec	Text
0000	ff ff ff ff ff ff 00 e0 b8 57 22 4e 08 00 45 00	..... .w"n..E.
0010	00 4e 30 9e 00 00 80 11 85 49 c0 a8 01 68 c0 a8	.N0.....I...h..
0020	01 ff 00 89 00 89 00 3a 76 b5 80 85 01 10 00 01	.....: v.....
0030	00 00 00 00 00 00 20 46 48 46 41 45 42 45 45 43	..... F HFAEBEEC
0040	4f 45 4f 45 46 46 45 43 4f 43 4f 43 41 43 41 43	OEOEFFEC OCOCACAC

### 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.

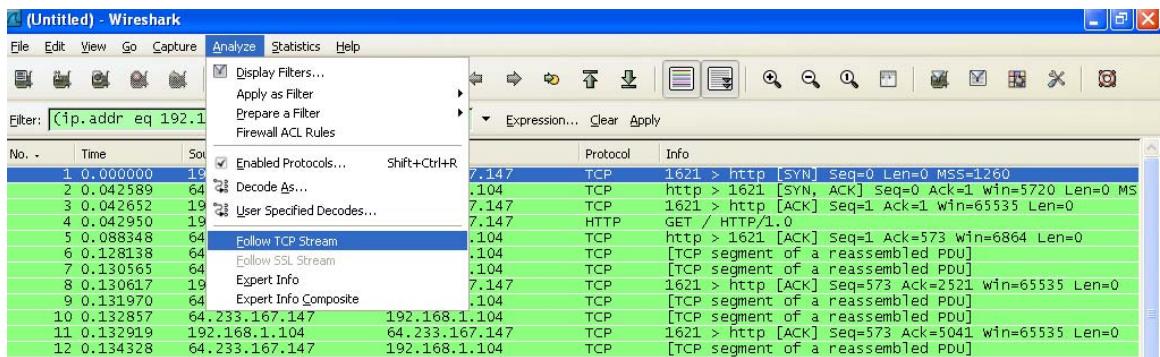
### Step 4: Stop Capture

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.

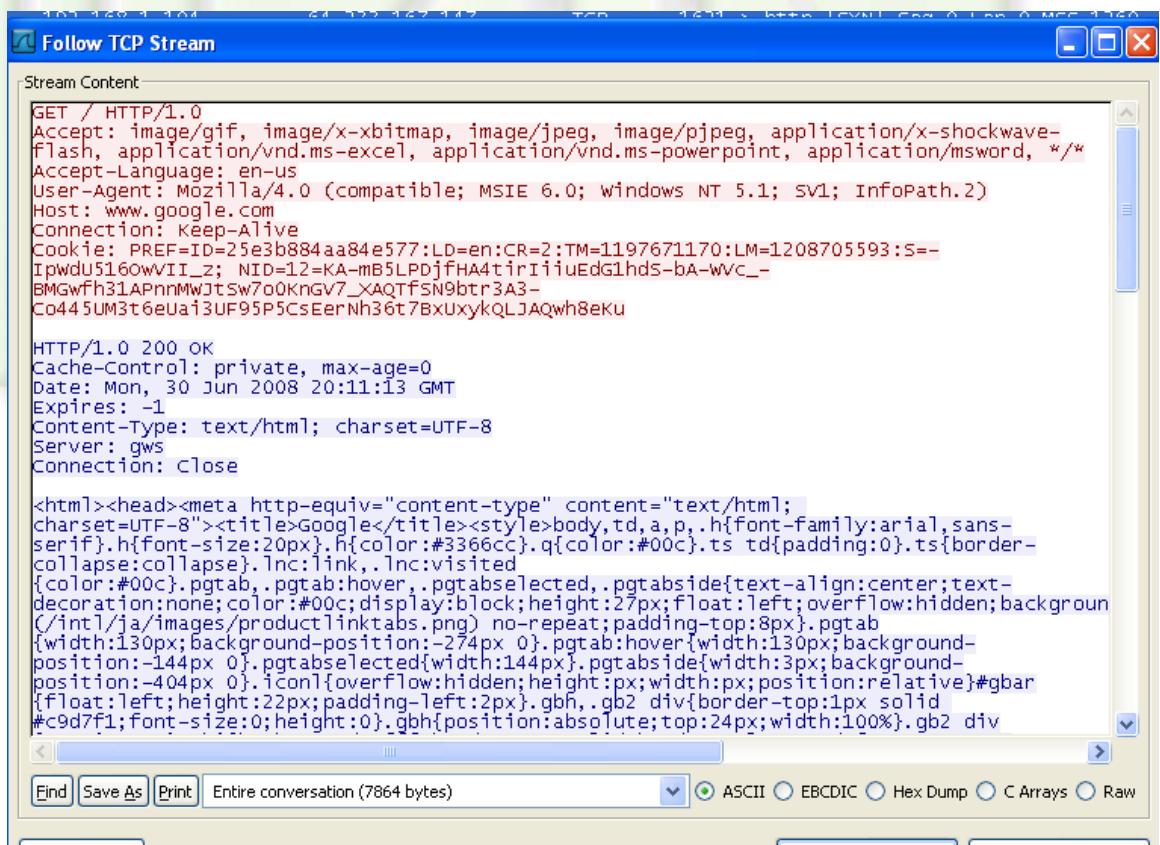


## Step 5: Analyze Stream

- 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>.

```
httpd-3.html - WordPad
File Edit View Insert Format Help
File Edit View Insert Format Help
Server: Apache
Last-Modified: Sat, 13 Mar 2004 19:20:54 GMT
ETag: "9a0f3e47-25a57180"
Accept-Ranges: bytes
Content-Length: 751
Keep-Alive: timeout=15, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html
PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"
xml:lang="en" lang="en">
<head>
<title>Ethereal: A Network Protocol Analyzer
</title>
<style type="text/css" media="all">
@import url("mm/css/ethereal-3-0.css");
</style>
<script type="text/JavaScript">
function jump_mirror(which_mirror) {
if(which_mirror != "NONE") {
location.href = which_mirror;
} else {
return false;
}
}
</script>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
<meta name="generator" content="Ethereal 1.0.0" />
<meta name="keywords" content="Protocol Analyzer, Network, Ethern&hellip;
```

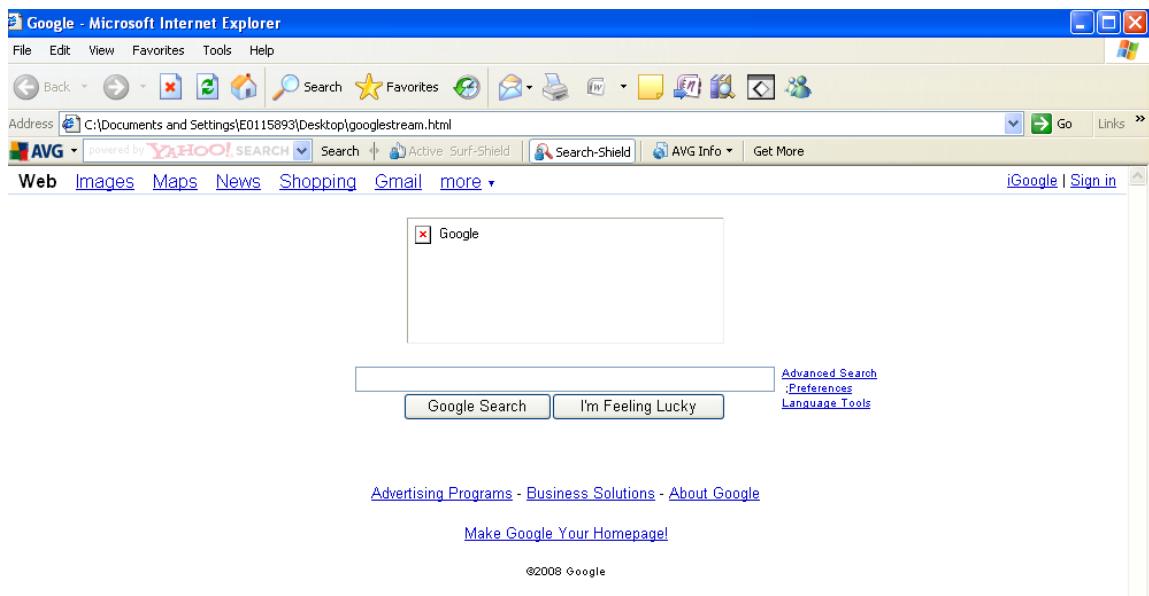
to  
<a href="mailto:ethereal-web[AT]ethereal.com">ethereal-web[AT]ethereal.com</a>  
.cbr  
Last modified: Sat, March 13 2004.  
</div>  
</body>  
</html>  
GET /mm/image/elogos-64-trans.gif  
HTTP/1.1  
Host: www.ethereal.com  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4)  
Gecko/20030624 Netscape/7.1 (ax)  
Accept: video/x-mng, image/png, image/jpeg, image/gif;q=0.2,\*/\*;q=0.1  
Accept-Language: en-us,en;q=0.5  
Accept-Encoding: gzip,deflate  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
Keep-Alive: 300  
Connection: keep-alive

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](http://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).

