Session 6 Workshop

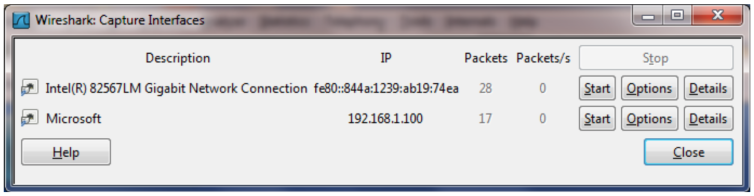
Universidad Icesi

2024-1

1 Taking Wireshark for a Test Run

Do the following:

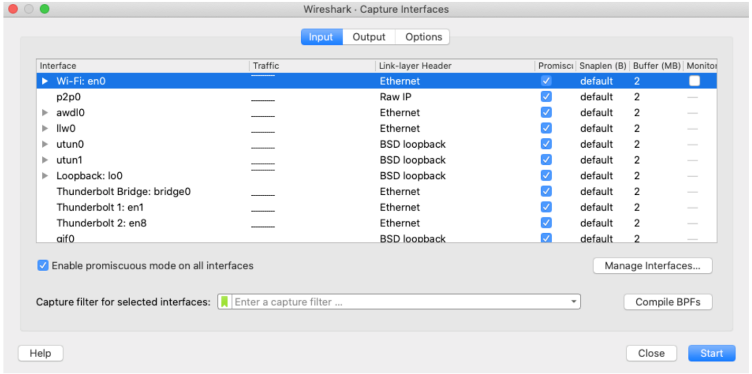
1. Start up your favorite web browser, which will display your selected homepage.
2. Start up the Wireshark software. Wireshark has not yet begun capturing packets.
3. To begin packet capture, select the Capture pull down menu and select Interfaces. This will cause the "Wireshark: Capture Interfaces" window to be displayed (on a PC) or you can choose Options on a Mac. You should see a list of interfaces, as shown in figure 1 (Windows) and 2 (Mac).



Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s	Stop		
Intel(R) 82567LM Gigabit Network Connection	fe80::844a:1239:ab19:74ea	28	0	Start	Options	Details
Microsoft	192.168.1.100	17	0	Start	Options	Details

Figure 1: Windows



Wireshark · Capture Interfaces

Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor
▶ Wi-Fi: en0		Ethernet	☑	default	2	□
p2p0		Raw IP	☑	default	2	—
▶ awdl0		Ethernet	☑	default	2	—
▶ llw0		Ethernet	☑	default	2	—
▶ utun0		BSD loopback	☑	default	2	—
▶ utun1		BSD loopback	☑	default	2	—
▶ Loopback: lo0		BSD loopback	☑	default	2	—
Thunderbolt Bridge: bridge0		Ethernet	☑	default	2	—
Thunderbolt 1: en1		Ethernet	☑	default	2	—
Thunderbolt 2: en8		Ethernet	☑	default	2	—
gif0		BSD loopback	☑	default	2	—

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Figure 2: Mac

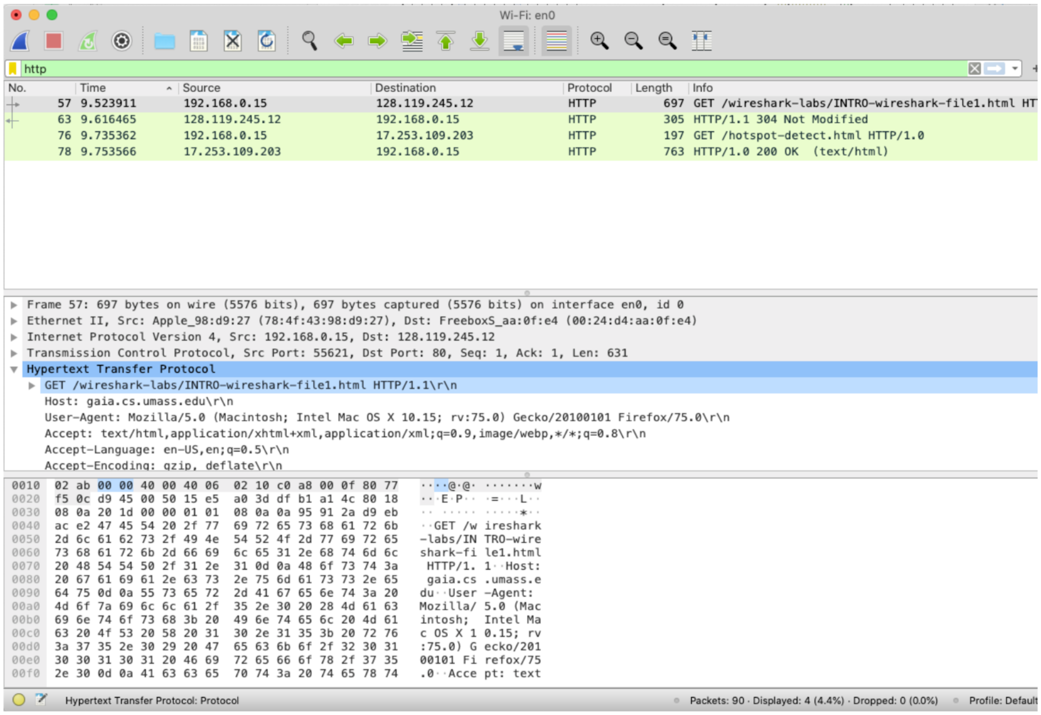
4. You'll see a list of the interfaces on your computer as well as a count of the packets that have been observed on that interface so far. On a Windows machine, click on Start for the interface on which you want to begin packet capture. On a Windows machine, select the interface and click Start on the bottom of the window). Packet capture will now begin - Wireshark is now capturing all packets being sent/received from/by your computer!
5. Once you begin packet capture, a window will appear. This window shows the packets being captured. By selecting Capture pulldown menu and selecting Stop, or by click on the red Stop square, you can stop packet capture. But don't stop packet capture yet. Let's capture some interesting packets first.

To do so, we'll need to generate some network traffic. Let's do so using a web browser, which will use the HTTP protocol to download content from a website.

6. While Wireshark is running, enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at gaia.cs.umass.edu and exchange HTTP messages with the server in order to download this page. The Ethernet or WiFi frames containing these HTTP messages (as well as all other frames passing through your Ethernet or WiFi adapter) will be captured by Wireshark.

7. After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture by selecting stop in the Wireshark capture window. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well. Even though the only action you took was to download a web page, there were evidently many other protocols running on your computer that are unseen by the user.

8. Type in "http" (without the quotes, and in lower case - all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered "http") or just hit return. This will cause only HTTP message to be displayed in the packet-listing window. The figure 3 below shows a screenshot after the http filter has been applied to the packet capture window. Note also that in the Selected packet details window, we've chosen to show detailed content for the Hypertext Transfer Protocol application message that was found within the TCP segment, that was inside the IPv4 datagram that was inside the Ethernet II (WiFi) frame. Focusing on content at a specific message, segment, datagram and frame level lets us focus on just what we want to look at (in this case HTTP messages).



```
http
```

```
No.      Time        Source            Destination       Protocol  Length  Info
     57  9.523911    192.168.0.15      128.119.245.12    HTTP         697  GET /wireshark-labs/INTRO-wireshark-file1.html HT
     63  9.616465    128.119.245.12    192.168.0.15      HTTP         305  HTTP/1.1 304 Not Modified
     76  9.735362    192.168.0.15      17.253.109.203    HTTP         197  GET /hotspot-detect.html HTTP/1.0
     78  9.753566    17.253.109.203    192.168.0.15      HTTP         763  HTTP/1.0 200 OK  (text/html)
```

```
▶ Frame 57: 697 bytes on wire (5576 bits), 697 bytes captured (5576 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: FreeboxS_aa:0f:e4 (00:24:d4:aa:0f:e4)
▶ Internet Protocol Version 4, Src: 192.168.0.15, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 55621, Dst Port: 80, Seq: 1, Ack: 1, Len: 631
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
```

```
0010  02 ab 00 00 40 00 40 06  02 10 c0 a8 00 0f 80 77   ····@·@· ·······w
0020  f5 0c d9 45 00 50 15 e5  a0 3d df b1 a1 4c 80 18   ···E·P·· ·=···L··
0030  08 0a 20 1d 00 00 01 01  08 0a 0a 95 91 2a d9 eb   ·· ····· ·····*··
0040  ac e2 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-wire
0060  73 68 61 72 6b 2d 66 69  6c 65 31 2e 68 74 6d 6c   shark-fi le1.html
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0080  20 67 61 69 61 2e 63 73  2e 75 6d 61 73 73 2e 65    gaia.cs .umass.e
0090  64 75 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   du··User -Agent: 
00a0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 4d 61 63   Mozilla/ 5.0 (Mac
00b0  69 6e 74 6f 73 68 3b 20  49 6e 74 65 6c 20 4d 61   intosh;  Intel Ma
00c0  63 20 4f 53 20 58 20 31  30 2e 31 35 3b 20 72 76   c OS X 1 0.15; rv
00d0  3a 37 35 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   :75.0) G ecko/201
00e0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 37 35   00101 Fi refox/75
00f0  2e 30 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   .0··Acce pt: text
```

Hypertext Transfer Protocol: Protocol
Packets: 90 · Displayed: 4 (4.4%) · Dropped: 0 (0.0%)
Profile: Default

FIGURE 3: Details

9. Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server. (Look for an HTTP GET message in the "listing of captured packets" portion of the Wireshark window that shows "GET" followed by the gaia.cs.umass.edu URL that you entered. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message

header information will be displayed in the packet-header window . By clicking on '+' and '-' and right-pointing and down-pointing arrowheads to the left side of the packet details window, minimize the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. Maximize the amount information displayed about the HTTP protocol. Your Wireshark display should now look roughly as shown in figure 3. (Note, in particular, the minimized amount of protocol information for all protocols except HTTP, and the maximized amount of protocol information for HTTP in the packet-header window).

10. Exit Wireshark.

2 Questions

The goal of this workshop was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet- listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)
3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?
4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.