DFSC1316: Digital Forensic and Information Assurance I

Lab 1 (Due 9/29/2017 23:59:99)

Rules:

1. All you answers will be <u>typed</u> unless otherwise being advised.
2. Submit you assignment in PDF version (Office word can be directly saved as PDF, or you can use virtual PDF printer to 'print' it as pdf).

This lab is to prepare you for monitoring and analyzing of network traffic that happened on your computer.

Getting Wireshark[1]

In order to run Wireshark, you will need to have access to a computer that supports both Wireshark and the *libpcap* or *WinPCap* packet capture library. The *libpcap* software will be installed for you, if it is not installed within your operating system, when you install Wireshark. See http://www.wireshark.org/download.html for a list of supported operating systems and download sites

Download and install the Wireshark software:

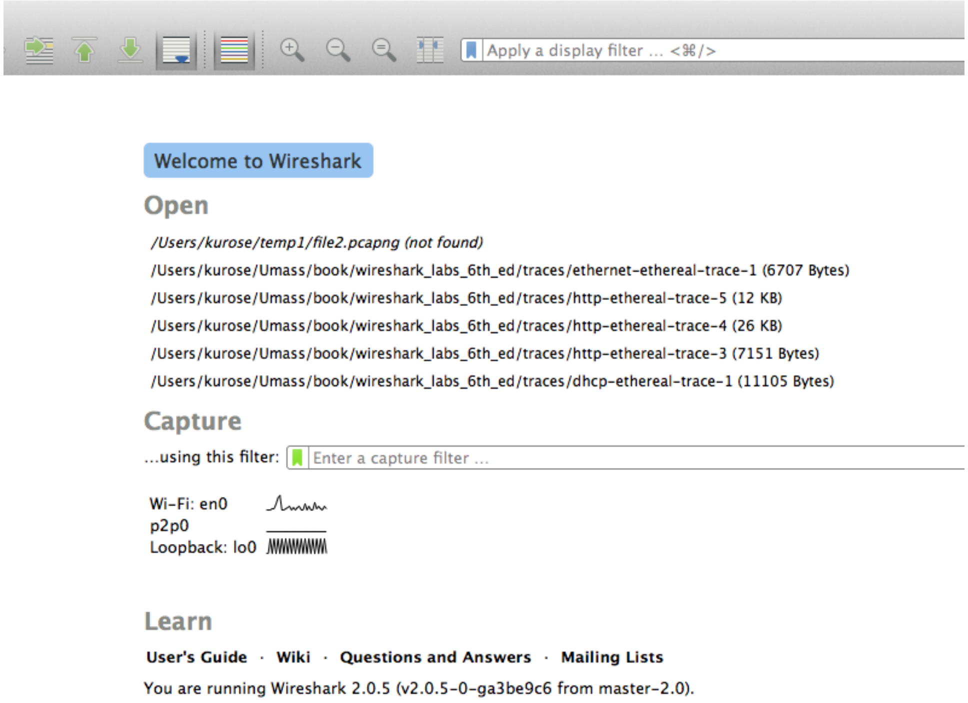
- Go to http://www.wireshark.org/download.html and download and install the Wireshark binary for your computer.

The Wireshark FAQ has a number of helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Wireshark.

Running Wireshark

When you run the Wireshark program, you'll get a startup screen that looks something like the screen below. Different versions of Wireshark will have different startup screens – so don't panic if yours doesn't look exactly like the screen below!

[1] This lab is created based on materials available at http://www-net.cs.umass.edu/wireshark-labs/



Apply a display filter … <⌘/>

Welcome to Wireshark

Open

/Users/kurose/temp1/file2.pcapng (not found)
/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/ethernet-ethereal-trace-1 (6707 Bytes)
/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/http-ethereal-trace-5 (12 KB)
/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/http-ethereal-trace-4 (26 KB)
/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/http-ethereal-trace-3 (7151 Bytes)
/Users/kurose/Umass/book/wireshark_labs_6th_ed/traces/dhcp-ethereal-trace-1 (11105 Bytes)

Capture

…using this filter: Enter a capture filter …

Wi-Fi: en0
p2p0
Loopback: lo0

Learn

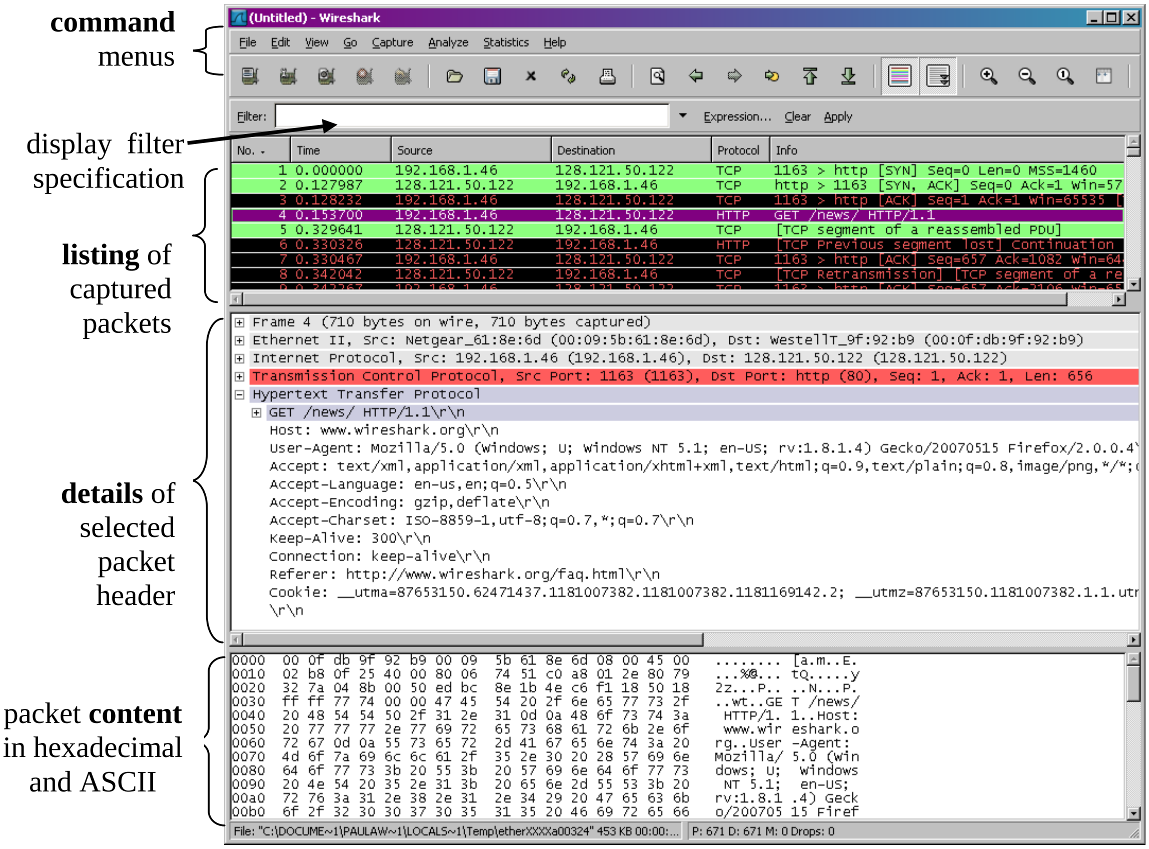
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.0.5 (v2.0.5-0-ga3be9c6 from master-2.0).

Figure 2: Initial Wireshark Screen

There’s not much interesting on this screen. But note that under the Capture section, there is a list of so-called interfaces. The computer we’re taking these screenshots from has just one real interface – “Wi-Fi en0,” which is the interface for Wi-Fi access. All packets to/from this computer will pass through the Wi-Fi interface, so it’s here where we want to capture packets. On a Mac/Windows, double click on this interface.

If you click on one of these interfaces to start packet capture (i.e., for Wireshark to begin capturing all packets being sent to/from that interface), a screen like the one below will be displayed, showing information about the packets being captured. Once you start packet capture, you can stop it by using the *Capture* pull down menu and selecting *Stop*.


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time       Source           Destination      Protocol  Info
   1 0.000000   192.168.1.46     128.121.50.122   TCP       1163 > http [SYN] Seq=0 Len=0 MSS=1460
   2 0.127987   128.121.50.122   192.168.1.46     TCP       http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
   3 0.128232   192.168.1.46     128.121.50.122   TCP       1163 > http [ACK] Seq=1 Ack=1 Win=65535 [
   4 0.153700   192.168.1.46     128.121.50.122   HTTP      GET /news/ HTTP/1.1
   5 0.329641   128.121.50.122   192.168.1.46     TCP       [TCP segment of a reassembled PDU]
   6 0.330326   128.121.50.122   192.168.1.46     HTTP      [TCP Previous segment lost] Continuation
   7 0.330467   192.168.1.46     128.121.50.122   TCP       1163 > http [ACK] Seq=657 Ack=1082 Win=64
   8 0.342042   128.121.50.122   192.168.1.46     TCP       [TCP Retransmission] [TCP segment of a re
   9 0.342267   192.168.1.46     128.121.50.122   TCP       1163 > http [ACK] Seq=657 Ack=2106 Win=65
```

```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
⊟ Hypertext Transfer Protocol
  ⊞ GET /news/ HTTP/1.1\r\n
    Host: www.wireshark.org\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.wireshark.org/faq.html\r\n
    Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
    \r\n
```

```
0000  00 0f db 9f 92 b9 00 09  5b 61 8e 6d 08 00 45 00   ........ [a.m..E.
0010  02 b8 0f 25 40 00 80 06  74 51 c0 a8 01 2e 80 79   ...%@... tQ.....y
0020  32 7a 04 8b 00 50 ed bc  8e 1b 4e c6 f1 18 50 18   2z...P.. ..N...P.
0030  ff ff 77 74 00 00 47 45  54 20 2f 6e 65 77 73 2f   ..wt..GE T /news/
0040  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0050  20 77 77 77 2e 77 69 72  65 73 68 61 72 6b 2e 6f    www.wir eshark.o
0060  72 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   rg..User -Agent: 
0070  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080  64 6f 77 73 3b 20 55 3b  20 57 69 6e 64 6f 77 73   dows; U;  Windows
0090  20 4e 54 20 35 2e 31 3b  20 65 6e 2d 55 53 3b 20    NT 5.1;  en-US; 
00a0  72 76 3a 31 2e 38 2e 31  2e 34 29 20 47 65 63 6b   rv:1.8.1 .4) Geck
00b0  6f 2f 32 30 30 37 30 35  31 35 20 46 69 72 65 66   o/200705 15 Firef
```

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:... | P: 671 D: 671 M: 0 Drops: 0

Figure 3: Wireshark Graphical User Interface, during packet capture and analysis

The Wireshark interface has five major components:

- The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now are the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application. The Capture menu allows you to begin packet capture.

- The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is *not* a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest-level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.
- The **packet-header details window** provides details about the packet selected (highlighted) in the packet-listing window. (To select a packet in the packet-listing window, place the cursor over the packet's one-line summary in the packet-listing window and click with the left mouse button.). These details include information about the Ethernet frame (assuming the packet was sent/received over an Ethernet interface) and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the plus minus boxes to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.
- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.
- Towards the top of the Wireshark graphical user interface, is the **packet display filter field,** into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

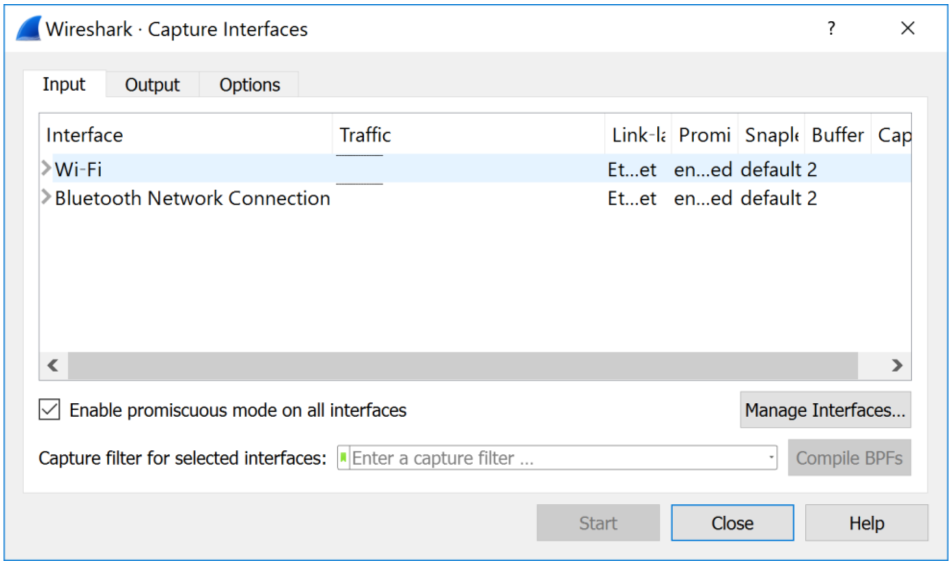
Taking Wireshark for a Test Run

The best way to learn about any new piece of software is to try it out! We'll assume that your computer is connected to the Internet via a wireless connection. Do the following

1. Start up your favorite web browser, which will display your selected homepage.

2. Start up the Wireshark software. You will initially see a window similar to that shown in Figure 2. Wireshark has not yet begun capturing packets.

3. To begin packet capture, select the *Capture* pull down menu and select *Options.* This will cause the "Wireshark: Capture Interfaces" window to be displayed, as shown in Figure 4.



Interface	Traffic	Link-la	Promi	Snapl	Buffer	Cap
Wi-Fi		Et...et	en...ed	default	2	
Bluetooth Network Connection		Et...et	en...ed	default	2	

☑ Enable promiscuous mode on all interfaces

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

Figure 4: Wireshark Capture Interface Window

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. Click on one interface, and then click on *Start* for the interface on which you want to begin packet capture (in the case, the Wi-Fi Connection). 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 similar to that shown in Figure 3 will appear. This window shows the packets being captured. By selecting *Capture* pulldown menu and selecting *Stop*, 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, such as using the web browser to browse some webpages.

6. While Wireshark is running, enter the URL:
   www.shsu.edu
   and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at www.shsu.edu and exchange HTTP messages with the server in order to download this page. The Internet frames containing these HTTP messages (as well as all other frames passing through your Wi-Fi adapter) will be captured by Wireshark.

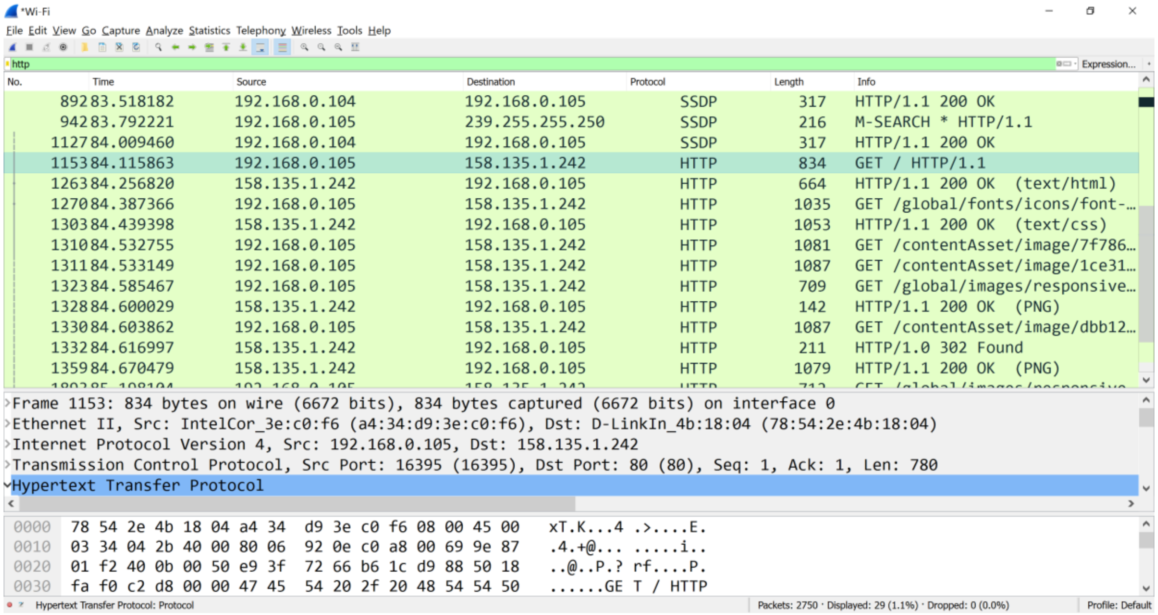
7. Stop Wireshark packet capture by selecting stop in the Wireshark capture window. The main Wireshark window should now look similar to Figure 3. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the www.shsu.edu web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (see, e.g., the many different protocol types shown in the *Protocol* column in Figure 3). 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 simply press Enter. This will cause only HTTP message to be displayed in the packet-listing window.

9. Find the HTTP GET message that was sent from your computer to the www.shsu.edu HTTP server. (Look for an HTTP GET message in the “listing of captured packets” portion of the Wireshark window (see Figure 3) that shows “GET” with the destination shows as some IP address. How to know what “GET” message is related to www.shsu.edu? Type the destination IP address into your web browser, if it is the correct IP, www.shsu.edu main page will be displayed. 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 the right-pointing and down-pointing arrowheads to the left side of the packet details window, Ethernet, Internet Protocol, and Transmission Control Protocol information will be displayed. Your Wireshark display should now look roughly as shown in Figure 5.

10. Exit Wireshark

Congratulations! You’ve now completed the lab.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
http
```

```
No.   Time        Source          Destination      Protocol  Length  Info
  892 83.518182   192.168.0.104   192.168.0.105    SSDP       317    HTTP/1.1 200 OK
  942 83.792221   192.168.0.105   239.255.255.250  SSDP       216    M-SEARCH * HTTP/1.1
 1127 84.009460   192.168.0.104   192.168.0.105    SSDP       317    HTTP/1.1 200 OK
 1153 84.115863   192.168.0.105   158.135.1.242    HTTP       834    GET / HTTP/1.1
 1263 84.256820   158.135.1.242   192.168.0.105    HTTP       664    HTTP/1.1 200 OK  (text/html)
 1270 84.387366   192.168.0.105   158.135.1.242    HTTP      1035    GET /global/fonts/icons/font-…
 1303 84.439398   158.135.1.242   192.168.0.105    HTTP      1053    HTTP/1.1 200 OK  (text/css)
 1310 84.532755   192.168.0.105   158.135.1.242    HTTP      1081    GET /contentAsset/image/7f786…
 1311 84.533149   192.168.0.105   158.135.1.242    HTTP      1087    GET /contentAsset/image/1ce31…
 1323 84.585467   192.168.0.105   158.135.1.242    HTTP       709    GET /global/images/responsive…
 1328 84.600029   158.135.1.242   192.168.0.105    HTTP       142    HTTP/1.1 200 OK  (PNG)
 1330 84.603862   192.168.0.105   158.135.1.242    HTTP      1087    GET /contentAsset/image/dbb12…
 1332 84.616997   158.135.1.242   192.168.0.105    HTTP       211    HTTP/1.0 302 Found
 1359 84.670479   158.135.1.242   192.168.0.105    HTTP      1079    HTTP/1.1 200 OK  (PNG)
```

```
>Frame 1153: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface 0
>Ethernet II, Src: IntelCor_3e:c0:f6 (a4:34:d9:3e:c0:f6), Dst: D-LinkIn_4b:18:04 (78:54:2e:4b:18:04)
>Internet Protocol Version 4, Src: 192.168.0.105, Dst: 158.135.1.242
>Transmission Control Protocol, Src Port: 16395 (16395), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 780
vHypertext Transfer Protocol
```

```
0000  78 54 2e 4b 18 04 a4 34  d9 3e c0 f6 08 00 45 00   xT.K...4 .>....E.
0010  03 34 04 2b 40 00 80 06  92 0e c0 a8 00 69 9e 87   .4.+@... .....i..
0020  01 f2 40 0b 00 50 e9 3f  72 66 b6 1c d9 88 50 18   ..@..P.? rf....P.
0030  fa f0 c2 d8 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
```

Hypertext Transfer Protocol: Protocol | Packets: 2750 · Displayed: 29 (1.1%) · Dropped: 0 (0.0%) | Profile: Default

Figure 5: Wireshark window after step 9

What to hand in

The goal of this lab 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 with attached screenshots, based on your Wireshark experimentation:

1. (25pts) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above. Mark them in the screenshot.

2. (25pts) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? Clearly mark the packets in the screenshot (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began.)

3. (25 pts) What is the Internet address of www.shsu.edu? What is the Internet address of your computer?

4. (25pts) 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 choose to print as a PDF file. If you do not have a PDF printer on your computer, you may need to install one, such as Foxit PDF reader/printer.

5. (Optional, no points) Find one message at your choice, other than a HTTP message, find out what is the source and/or destination, and try to explain why this message has been sent (e.g., what application may have sent it, where it was sent to, etc.)