Wireshark Tutorial

Getting Wireshark

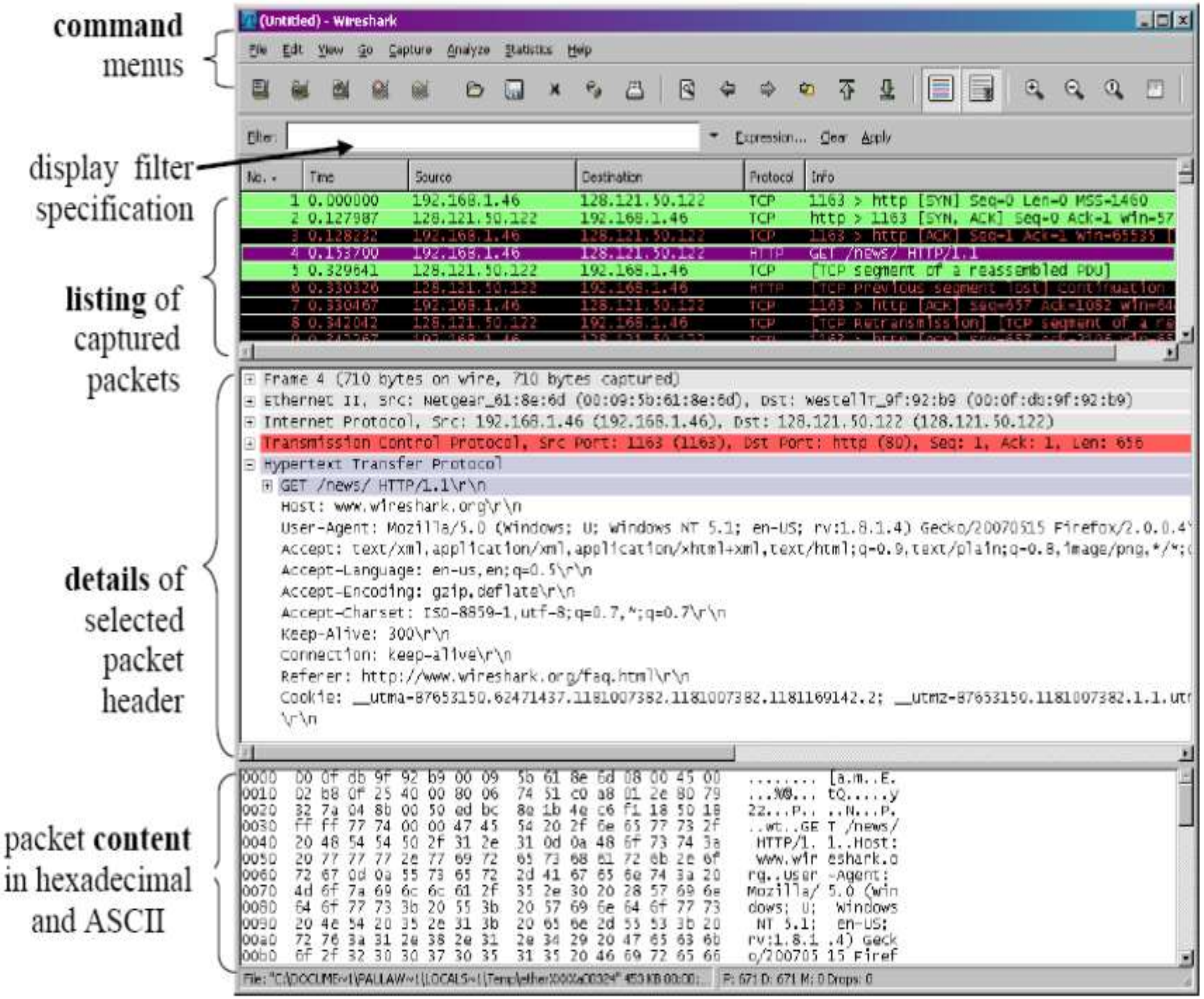
Wireshark for Windows and Mac OS X can be easily downloaded from its official website. If you are Linux users, you'll probably find Wireshark in its package repositories.

Detailed installing steps can be found on the Internet, so this tutorial won't cover this part.

Running Wireshark

When you run the Wireshark program, the Wireshark graphical user interface shown in Figure 2 will de displayed. Initially, no data will be displayed in the various windows.

The Wireshark interface has five major components:


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
```

```
⊞ 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\PALLAW~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:...   P: 671 D: 671 M: 0 Drops: 0
```

Figure 2

Running Wireshark(cont’d)

- 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.

Running Wireshark(cont’d)

- 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 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 right-pointing or down-pointing arrowhead 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.

Running Wireshark(cont’d)

- 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.

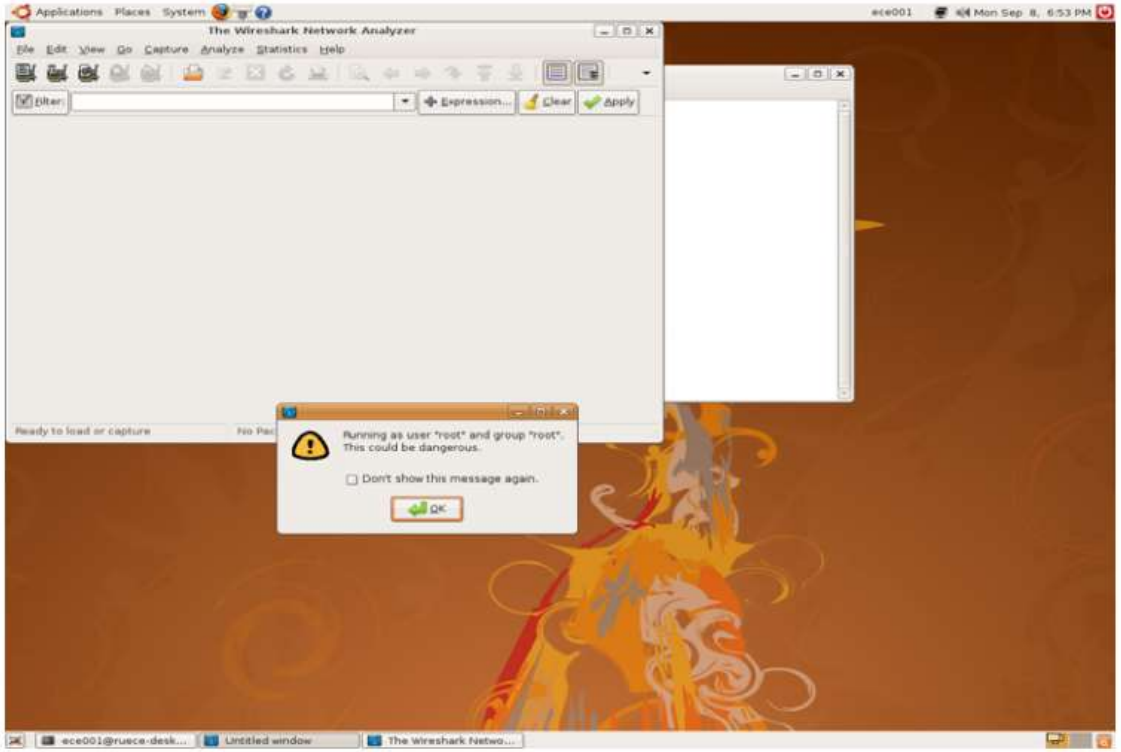
Test Run

The best way to learn about any new piece of software is to try it out! First, you need to know the network interconnections in the lab. The IP addresses are shown in Table 1 The 11 PCs are connected in the following fashion. (1 ↔ 2),(3 ↔ 4),(5 ↔ 6),(7 ↔ 8),(9 ↔2),(9 ↔ 1),(10 ↔ 3),(10 ↔ 4),(11 ↔ 5),and (11 ↔ 6). For ex (1 ↔ 2) means Pc1 and Pc2 are connected to the same switch. So PC1 and PC2 can communicate with each other. To perform the following steps, identify the two PCs for your test run.

Test Run(cont’d)

Do the following：

1. Start up your favorite web browser.
2. Start up the Wireshark software. You will initially see a window like shown in Figure 3，except that no packet data will be displayed in the packet listing, packet-header, or packet-contents window, since Wireshark has not yet begun capturing packets. Make sure you check “Don't show this message again” and press “ok” on the small dialog box that pops up.
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, as in Fingure 4.
4. The network interfaces (i.e., the physical connections) that your computer has to the network are shown. The attached snapshot was taken from my computer. You may not see the exact same entries when you perform a capture in the lab. You will notice that eth0 and eth1 will be displayed. Click “Start” for interface eth0. Packet capture will now begin - all packets being sent / received from/by your computer are now being captured by Wireshark!

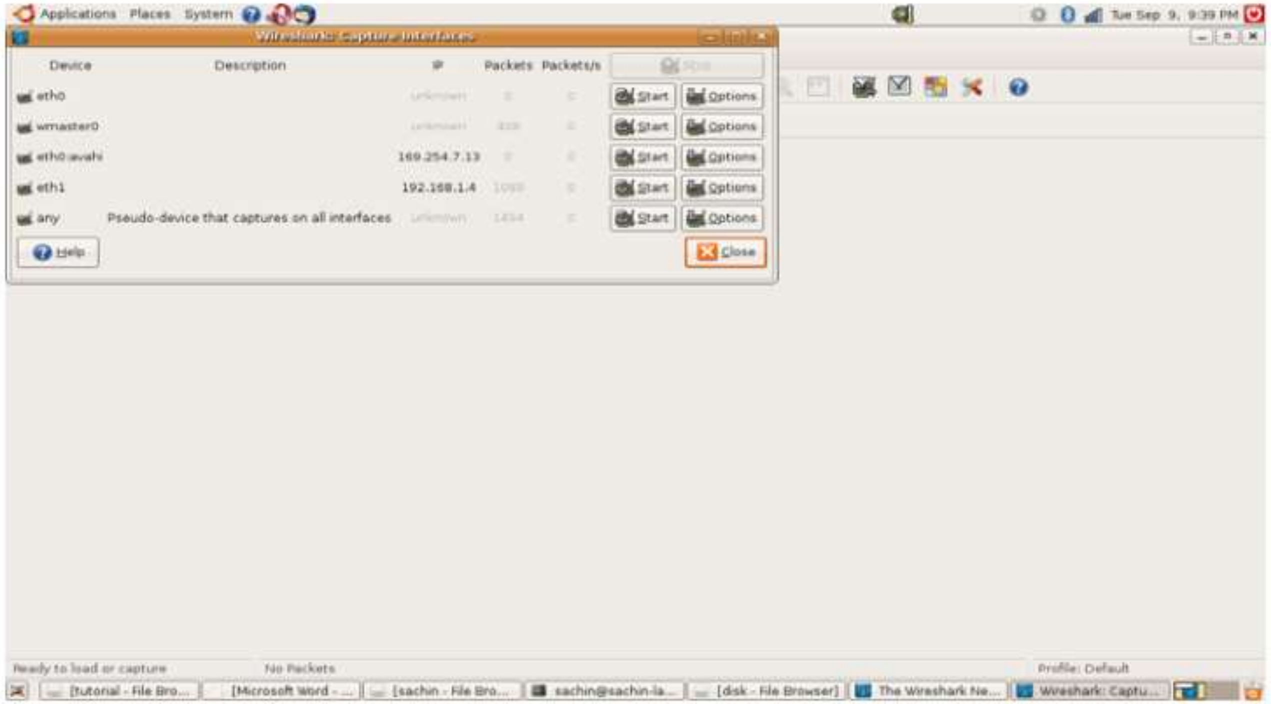


Applications Places System
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Ready to load or capture
OK

Running as user "root" and group "root". This could be dangerous.

□ Don't show this message again.

Fig. 3 Wireshark GUI



Device	Description	IP	Packets	Packets/s		
eth0		Unknown	0	0	Start	Options
wmaster0		Unknown	839	0	Start	Options
eth0:avahi		169.254.7.13	0	0	Start	Options
eth1		192.168.1.4	1099	0	Start	Options
any	Pseudo-device that captures on all interfaces	Unknown	1434	0	Start	Options

Ready to load or capture   No Packets   Profile: Default

Figure 4: Wireshark Capture Interfaces Window

Test Run(cont’d)

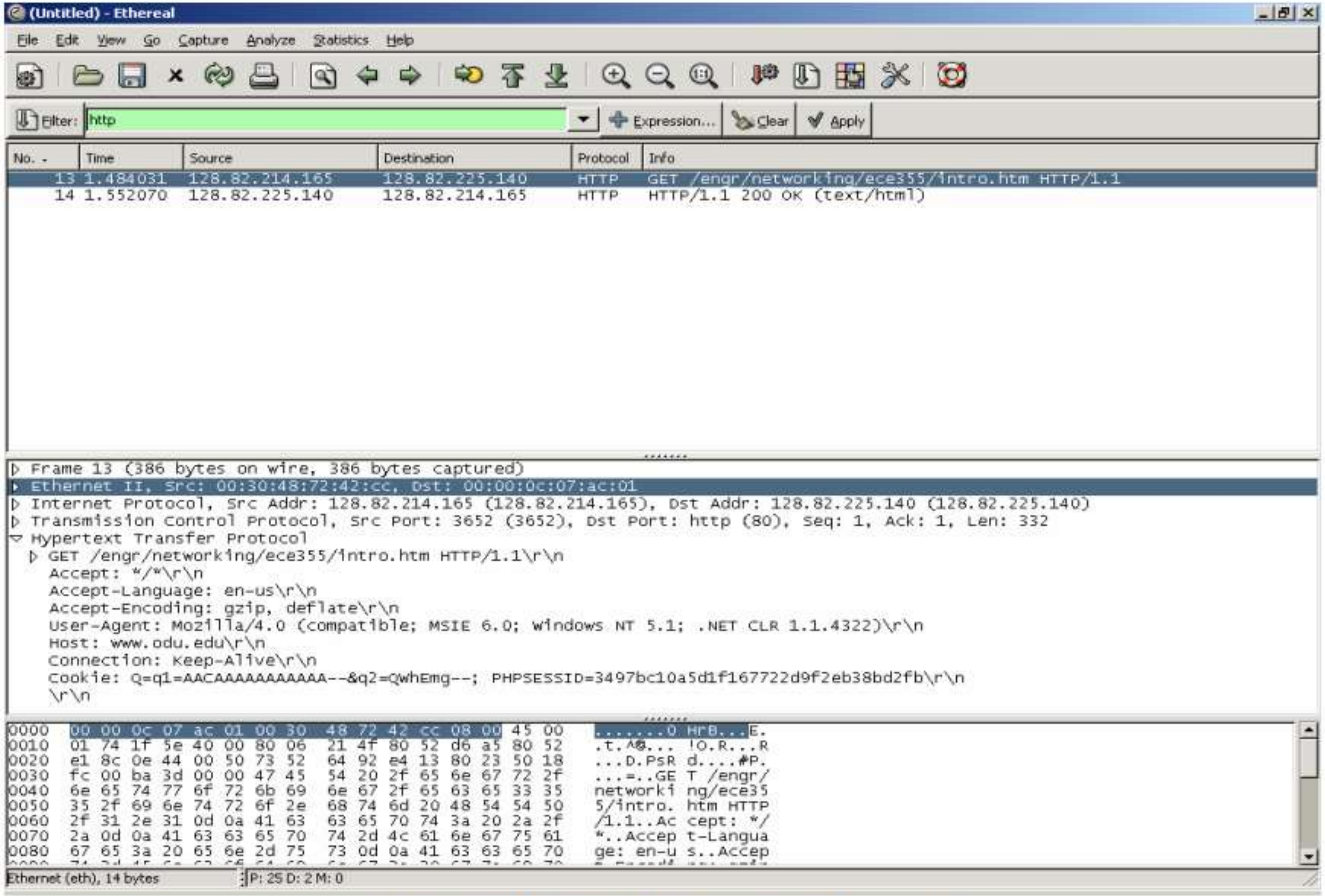
5. If you started your Web browser on PC1, you can only connect to PC2 and PC9 (refer to the interconnections listed at the start of this section). If you want to connect to PC2, refer to Table 1, and identify the IP address of eth0. The IP address is 10.0.1.3. If you wanted to connect to PC9, the IP address would be 10.0.1.17. While Wireshark is running, enter the URL: http://10.0.1.3/INTRO.htm to connect to the web server in PC2 and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at 10.0.1.3(PC2) and exchange HTTP messages with the server in order to download this page. The Ethernet frames containing these HTTP messages will be captured by Wireshark.

Test Run(cont’d)

6. After your browser has displayed the intro.htm page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture. The main Wireshark window should now look similar to Figure 2. 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 PC2 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 2). 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.
7. 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”). This will cause only HTTP message to be displayed in the packet-listing window.

Test Run(cont’d)

8. Select the first http message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer(ex. PC1) to the PC2 HTTP server. 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 window2. By clicking on right pointing and down-pointing arrows heads 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 5 (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).
9. Exit Wireshark



Filter: http

```
No. -   Time       Source          Destination     Protocol  Info
   13 1.484031   128.82.214.165  128.82.225.140  HTTP      GET /engr/networking/ece355/intro.htm HTTP/1.1
   14 1.552070   128.82.225.140  128.82.214.165  HTTP      HTTP/1.1 200 OK (text/html)
```

```
▷ Frame 13 (386 bytes on wire, 386 bytes captured)
▷ Ethernet II, Src: 00:30:48:72:42:cc, Dst: 00:00:0c:07:ac:01
▷ Internet Protocol, Src Addr: 128.82.214.165 (128.82.214.165), Dst Addr: 128.82.225.140 (128.82.225.140)
▷ Transmission Control Protocol, Src Port: 3652 (3652), Dst Port: http (80), Seq: 1, Ack: 1, Len: 332
▽ Hypertext Transfer Protocol
  ▷ GET /engr/networking/ece355/intro.htm HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)\r\n
    Host: www.odu.edu\r\n
    Connection: Keep-Alive\r\n
    Cookie: Q=q1=AACAAAAAAAAAAA--&q2=QwhEmg--; PHPSESSID=3497bc10a5d1f167722d9f2eb38bd2fb\r\n
    \r\n
```

```
0000  00 00 0c 07 ac 01 00 30  48 72 42 cc 08 00 45 00   .......0 HrB...E.
0010  01 74 1f 5e 40 00 80 06  21 4f 80 52 d6 a5 80 52   .t.^@... !O.R...R
0020  e1 8c 0e 44 00 50 73 52  64 92 e4 13 80 23 50 18   ...D.PsR d....#P.
0030  fc 00 ba 3d 00 00 47 45  54 20 2f 65 6e 67 72 2f   ...=..GE T /engr/
0040  6e 65 74 77 6f 72 6b 69  6e 67 2f 65 63 65 33 35   networki ng/ece35
0050  35 2f 69 6e 74 72 6f 2e  68 74 6d 20 48 54 54 50   5/intro. htm HTTP
0060  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1..Ac cept: */
0070  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *..Accep t-Langua
0080  67 65 3a 20 65 6e 2d 75  73 0d 0a 41 63 63 65 70   ge: en-u s..Accep
```

Ethernet (eth), 14 bytes   P: 25 D: 2 M: 0

Figure 5: Wireshark display after step 9

More Tutorials

A detailed video tutorial could find in the following link:

https://www.youtube.com/watch?v=TkCSr30UojM

Official Tutorial Link:

https://www.wireshark.org/docs/