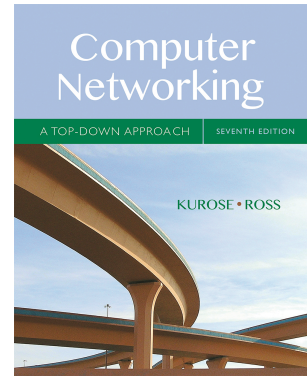


Wireshark Lab: Getting Started **SOLUTION**

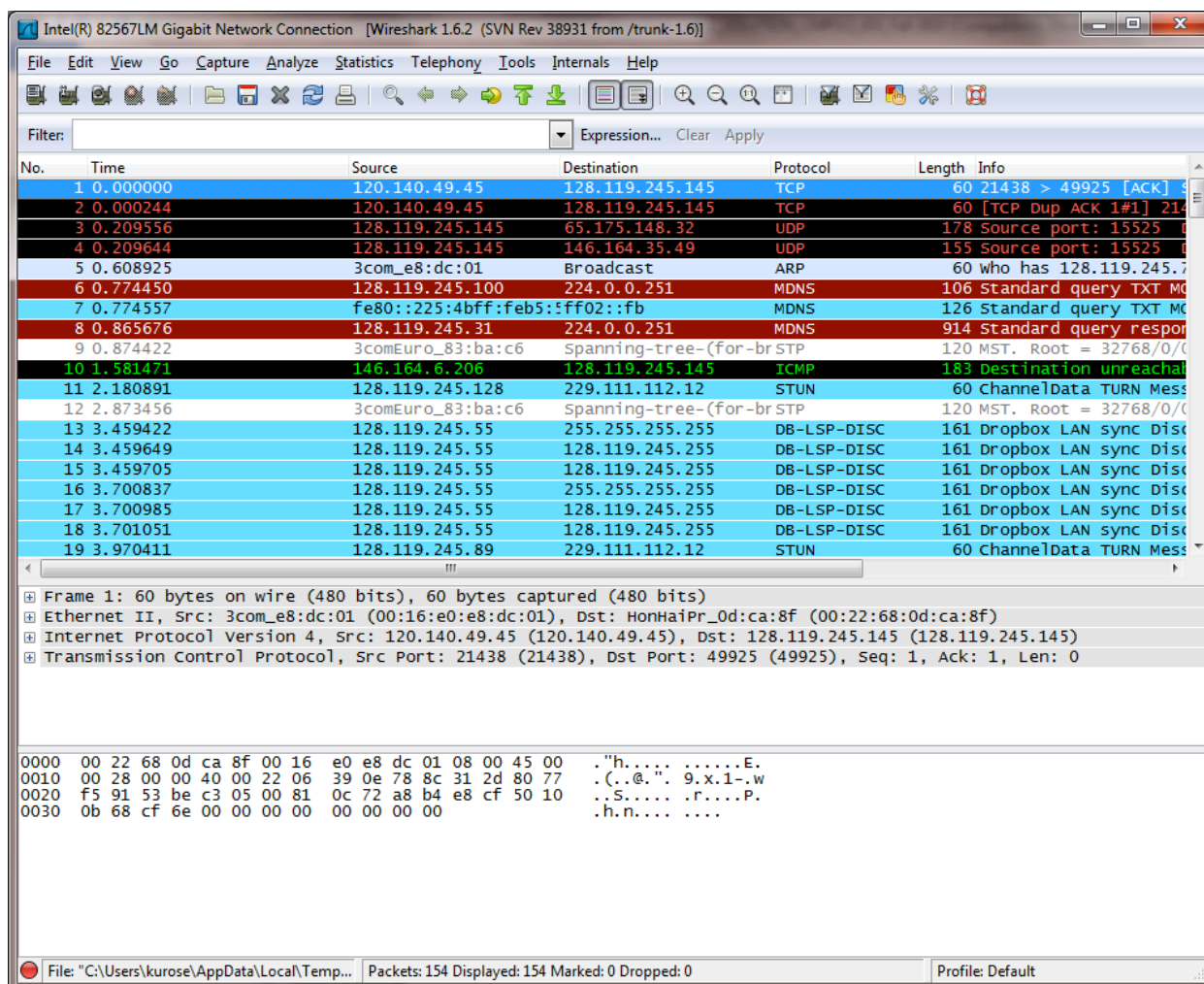
Supplement to *Computer Networking: A Top-Down Approach*, 7th ed., J.F. Kurose and K.W. Ross

© 2005-2016, J.F. Kurose and K.W. Ross, All Rights Reserved



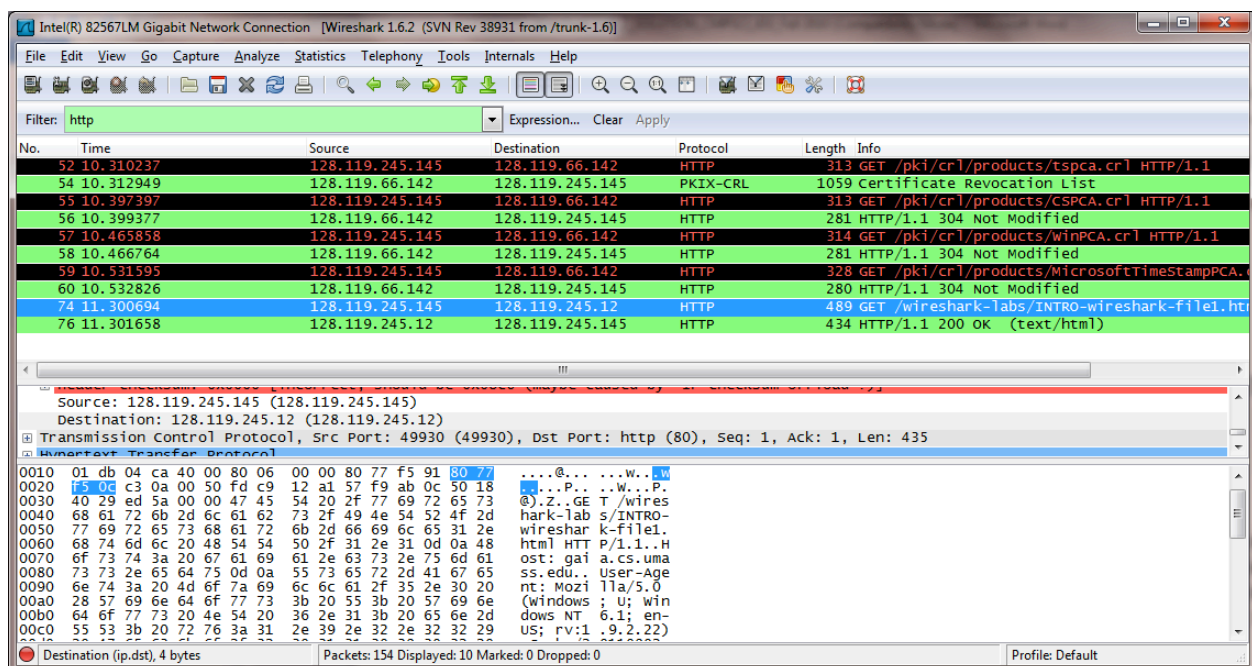
Q1. List the 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Answer: Some of the protocols listed in the screenshot below are UDP, TCP, ARP, ICMP, MDNS, and STUN. (Note you weren't asked to do a screenshot, but here is mine):



Q2. 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.)

Answer: As shown in the screen shot below (you didn't have to provide this), the GET was sent at 11.300694 and the reply was received at 11.301658. The delay was thus 0.000964 secs



Q3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

Answer: As shown in the screen shot below (you didn't have to provide this), the IP address of gaia.cs.umass.edu is 128.119.245.145; the IP address of my laptop is 128.119.66.142

Q4. Print the HTTP GET and REPLY messages displayed in step 9 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.

Answer: The print out of the two HTTP messages are below:

HTTP GET message:

```
No. Time Source Destination Protocol Length Info
74 11.300694 128.119.245.145 128.119.245.12 HTTP 489 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 74: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface eth0
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: DellComp_3b:8f:cd (00:06:5b:3b:8f:cd)
Internet Protocol Version 4, Src: 128.119.245.145 (128.119.245.145), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 49930 (49930), Dst Port: http (80), Seq: 1, Ack: 1, Len: 435
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 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.22) Gecko/20110902 Firefox/3.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
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: 115\r\n
```

Connection: keep-alive\r\n\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

HTTP REPLY message:

```
No. Time Source Destination Protocol Length Info
76 11.301658 128.119.245.12 128.119.245.145 HTTP 434 HTTP/1.1 200 OK (text
Frame 76: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits)
Ethernet II, Src: DellComp_3b:8f:cd (00:06:5b:3b:8f:cd), Dst: HonHaiPr_0d:ca:8f
(00:22:68:0d:ca:8f)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
128.119.245.145 (128.119.245.1)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49930 (49930),
Seq: 1, Ack: 436, Len: 38
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 26 Sep 2011 19:52:01 GMT\r\n
Server: Apache/2.2.3 (CentOS)\r\n
Last-Modified: Mon, 26 Sep 2011 19:51:01 GMT\r\n
ETag: "8734b-51-7a797340"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
Line-based text data: text/html
```