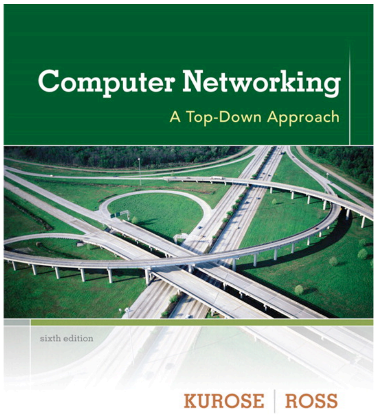
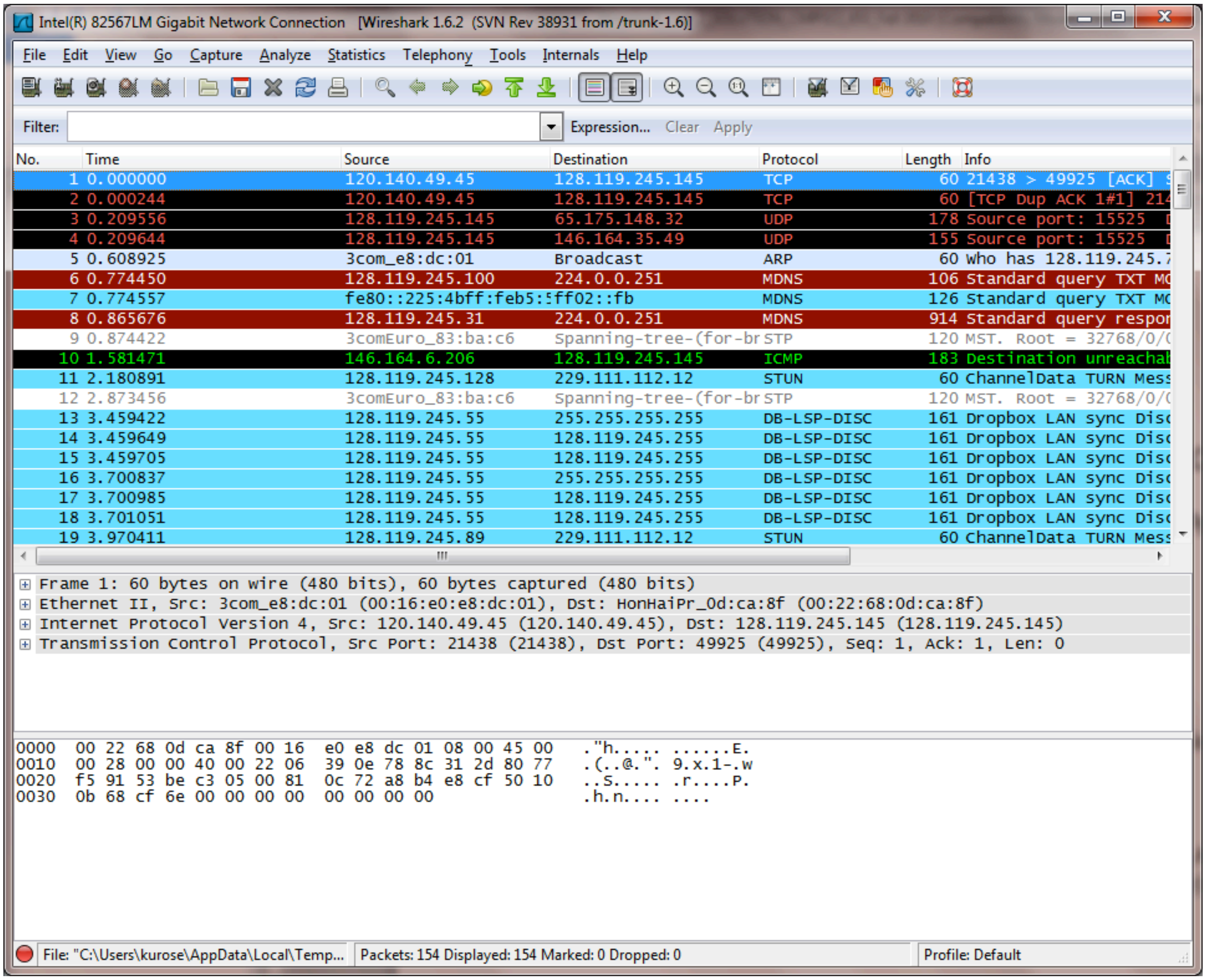
Wireshark Lab: Getting Started SOLUTION



Supplement to *Computer Networking: A Top-Down Approach, 6th ed.,* J.F. Kurose and K.W. Ross

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):


Intel(R) 82567LM Gigabit Network Connection [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	120.140.49.45	128.119.245.145	TCP	60	21438 > 49925 [ACK] S
2	0.000244	120.140.49.45	128.119.245.145	TCP	60	[TCP Dup ACK 1#1] 214
3	0.209556	128.119.245.145	65.175.148.32	UDP	178	Source port: 15525 D
4	0.209644	128.119.245.145	146.164.35.49	UDP	155	Source port: 15525 D
5	0.608925	3com_e8:dc:01	Broadcast	ARP	60	Who has 128.119.245.7
6	0.774450	128.119.245.100	224.0.0.251	MDNS	106	Standard query TXT MC
7	0.774557	fe80::225:4bff:feb5:5	ff02::fb	MDNS	126	Standard query TXT MC
8	0.865676	128.119.245.31	224.0.0.251	MDNS	914	Standard query respon
9	0.874422	3comEuro_83:ba:c6	Spanning-tree-(for-br	STP	120	MST. Root = 32768/0/0
10	1.581471	146.164.6.206	128.119.245.145	ICMP	183	Destination unreachab
11	2.180891	128.119.245.128	229.111.112.12	STUN	60	ChannelData TURN Mess
12	2.873456	3comEuro_83:ba:c6	Spanning-tree-(for-br	STP	120	MST. Root = 32768/0/0
13	3.459422	128.119.245.55	255.255.255.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
14	3.459649	128.119.245.55	128.119.245.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
15	3.459705	128.119.245.55	128.119.245.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
16	3.700837	128.119.245.55	255.255.255.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
17	3.700985	128.119.245.55	128.119.245.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
18	3.701051	128.119.245.55	128.119.245.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
19	3.970411	128.119.245.89	229.111.112.12	STUN	60	ChannelData TURN Mess

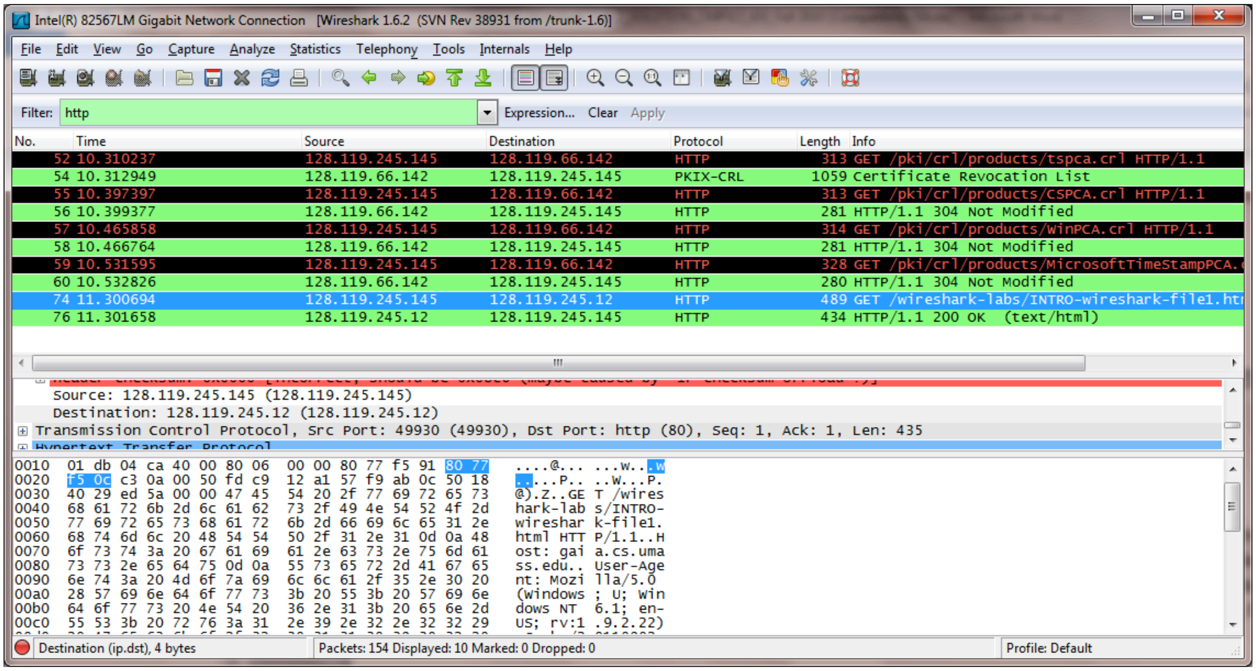
```
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: 3com_e8:dc:01 (00:16:e0:e8:dc:01), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
⊞ Internet Protocol Version 4, Src: 120.140.49.45 (120.140.49.45), Dst: 128.119.245.145 (128.119.245.145)
⊞ Transmission Control Protocol, Src Port: 21438 (21438), Dst Port: 49925 (49925), Seq: 1, Ack: 1, Len: 0
```

```
0000  00 22 68 0d ca 8f 00 16  e0 e8 dc 01 08 00 45 00   ."h..... ......E.
0010  00 28 00 00 40 00 22 06  39 0e 78 8c 31 2d 80 77   .(..@.". 9.x.1-.w
0020  f5 91 53 be c3 05 00 81  0c 72 a8 b4 e8 cf 50 10   ..S..... .r....P.
0030  0b 68 cf 6e 00 00 00 00  00 00 00 00              .h.n.... ....
```

File: "C:\Users\kurose\AppData\Local\Temp... Packets: 154 Displayed: 154 Marked: 0 Dropped: 0 Profile: Default

Q2. How long did it take from when the HTTP GET message was sent until the HTT 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


Intel(R) 82567LM Gigabit Network Connection [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: http

```
No.  Time       Source           Destination      Protocol  Length Info
  52 10.310237  128.119.245.145  128.119.66.142   HTTP         313 GET /pki/crl/products/tspca.crl HTTP/1.1
  54 10.312949  128.119.66.142   128.119.245.145  PKIX-CRL    1059 Certificate Revocation List
  55 10.397397  128.119.245.145  128.119.66.142   HTTP         313 GET /pki/crl/products/CSPCA.crl HTTP/1.1
  56 10.399377  128.119.66.142   128.119.245.145  HTTP         281 HTTP/1.1 304 Not Modified
  57 10.465858  128.119.245.145  128.119.66.142   HTTP         314 GET /pki/crl/products/WinPCA.crl HTTP/1.1
  58 10.466764  128.119.66.142   128.119.245.145  HTTP         281 HTTP/1.1 304 Not Modified
  59 10.531595  128.119.245.145  128.119.66.142   HTTP         328 GET /pki/crl/products/MicrosoftTimeStampPCA.
  60 10.532826  128.119.66.142   128.119.245.145  HTTP         280 HTTP/1.1 304 Not Modified
  74 11.300694  128.119.245.145  128.119.245.12   HTTP         489 GET /wireshark-labs/INTRO-wireshark-file1.htr
  76 11.301658  128.119.245.12   128.119.245.145  HTTP         434 HTTP/1.1 200 OK  (text/html)
```

```
    Source: 128.119.245.145 (128.119.245.145)
    Destination: 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
```

```
0010  01 db 04 ca 40 00 80 06  00 00 80 77 f5 91 80 77   ....@... ...w...w
0020  f5 0c c3 0a 00 50 fd c9  12 a1 57 f9 ab 0c 50 18   .....P.. ..W...P.
0030  40 29 ed 5a 00 00 47 45  54 20 2f 77 69 72 65 73   @).Z..GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1..H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  55 73 65 72 2d 41 67 65   ss.edu.. User-Age
0090  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0
00a0  28 57 69 6e 64 6f 77 73  3b 20 55 3b 20 57 69 6e   (Windows ; U; Win
00b0  64 6f 77 73 20 4e 54 20  36 2e 31 3b 20 65 6e 2d   dows NT  6.1; en-
00c0  55 53 3b 20 72 76 3a 31  2e 39 2e 32 2e 32 32 29   US; rv:1 .9.2.22)
```

Destination (ip.dst), 4 bytes | Packets: 154 Displayed: 10 Marked: 0 Dropped: 0 | Profile: Default

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/IN
Frame 74: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
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.
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.
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
```