



Lab 1

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

Answer

32	4.43524600	192.168.1.11	8.8.8.8	DNS	77 Standard query 0xc2c1 A gaia.cs.umass.edu
33	4.43551700	192.168.1.11	8.8.8.8	DNS	77 Standard query 0xc2c1 A gaia.cs.umass.edu
34	4.48738800	8.8.8.8	192.168.1.11	DNS	93 Standard query response 0xc2c1 A 128.119.245.12
35	4.48820500	192.168.1.11	128.119.245.12	TCP	66 49215 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 wS=4 SA
36	4.48837400	192.168.1.11	128.119.245.12	TCP	66 [TCP out-of-order] 49215 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 wS=4 SA
37	4.58342400	128.119.245.12	192.168.1.11	TCP	66 http > 49215 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 wS=4 SA
38	4.58349200	192.168.1.11	128.119.245.12	TCP	54 49215 > http [ACK] Seq=1 Ack=1 win=65700 Len=0
39	4.58391700	192.168.1.11	128.119.245.12	HTTP	506 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
40	4.58444600	192.168.1.11	128.119.245.12	TCP	60 49215 > http [ACK] Seq=1 Ack=1 win=65700 Len=0
41	4.58444700	192.168.1.11	128.119.245.12	HTTP	506 [TCP Retransmission] GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
42	4.67761000	128.119.245.12	192.168.1.11	TCP	60 http > 49215 [ACK] Seq=1 Ack=453 win=6912 Len=0
43	4.67819600	128.119.245.12	192.168.1.11	HTTP	434 HTTP/1.1 200 OK (text/html)

According to above screenshot, for this webpage downloading process, at first, the DNS protocol was used to translate the URL to IP address, and then the TCP (transport layer) connection was established between the client and the server. Finally, the HTTP (application layer) connection was established based on the TCP connection which established in step 2.

Thus, the 3 different protocols could be DNS, TCP and HTTP.

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.)

Answer

39	4.58391700	192.168.1.11	128.119.245.12	HTTP	506 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
41	4.58444700	192.168.1.11	128.119.245.12	HTTP	506 [TCP Retransmission] GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
43	4.67819600	128.119.245.12	192.168.1.11	HTTP	434 HTTP/1.1 200 OK (text/html)
49	4.84627400	192.168.1.11	128.119.245.12	HTTP	341 GET /favicon.ico HTTP/1.1
50	4.84638000	192.168.1.11	128.119.245.12	HTTP	341 [TCP Retransmission] GET /favicon.ico HTTP/1.1

Frame 39: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
 Interface id: 0
 Encapsulation type: Ethernet (1)
 Arrival Time: Jan 26, 2014 17:43:14.752657000 Mountain Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1390783394.752657000 seconds

According to above screenshot, the GET request was arrived at Jan 26, 2014 17:43:14.752657000.

43	4.67819600	128.119.245.12	192.168.1.11	HTTP	434 HTTP/1.1 200 OK (text/html)
----	------------	----------------	--------------	------	---------------------------------

Frame 43: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface 0
 Interface id: 0
 Encapsulation type: Ethernet (1)
 Arrival Time: Jan 26, 2014 17:43:14.846936000 Mountain Standard Time
 [Time shift for this packet: 0.000000000 seconds]

According to above screenshot, the HTTP OK is arrived at Jan 26, 2014 17:43:14.846936000

Therefore, the time took from HTTP GET to HTTP OK is .846936000 - .752657000 = 0.094279 seconds

Home Page: <http://www.public.asu.edu/~bhao2>

3. **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

```

39 4.58391700 192.168.1.11 128.119.245.12 HTTP 506 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
41 4.58444700 192.168.1.11 128.119.245.12 HTTP 506 [TCP Retransmission] GET /wireshark-labs/INTRO-wireshark
43 4.67819600 128.119.245.12 192.168.1.11 HTTP 434 HTTP/1.1 200 OK (text/html)

```

[Frame 39: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
 [Ethernet II, Src: Vmware_b4:cb:20 (00:0c:29:b4:cb:20), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
 [Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 128.119.245.12 (128.119.245.12)
 Version: 4
 Header Length: 20 bytes
 [Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 492
 Identification: 0x2102 (8450)
 [Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 [Header checksum: 0x0000 [incorrect, should be 0xa0d2 (may be caused by "IP checksum offload"?)]
 Source: 192.168.1.11 (192.168.1.11)
 Destination: 128.119.245.12 (128.119.245.12)

Above screenshot is the HTTP GET. This datagram is supposed to be sent from my computer to the web server. Thus, my computer's IP address is 192.168.1.11, the web server's IP address is 128.119.245.12 (gaia.cs.umass.edu).

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.**

Answer

The answer could be found in following pages.

No.	Time	Source	Destination	Protocol	Length	Info
39	4.583917000	192.168.1.11	128.119.245.12	HTTP	506	GET /wireshark-1

Frame 39: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
Ethernet II, Src: Vmware_b4:cb:20 (00:0c:29:b4:cb:20), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 128.119.245.12 (128.119.245.12)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 492
Identification: 0x2102 (8450)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [incorrect, should be 0xa0d2 (may be caused by "IP checksum offload"?)]
Source: 192.168.1.11 (192.168.1.11)
Destination: 128.119.245.12 (128.119.245.12)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 49215 (49215), Dst Port: http (80), Seq: 1, Ack: 1, Len: 492
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/vnd.ms-word, application/javascript\r\n
Accept-Language: en-US\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2)\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Next request in frame: 41]

No.	Time	Source	Destination	Protocol	Length	Info
43	4.678196000	128.119.245.12	192.168.1.11	HTTP	434	HTTP/1.1 200 OK

Frame 43: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface 0
Ethernet II, Src: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9), Dst: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.11 (192.168.1.11)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 420
Identification: 0xe0ab (57515)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 50
Protocol: TCP (6)
Header checksum: 0x2f71 [correct]
Source: 128.119.245.12 (128.119.245.12)
Destination: 192.168.1.11 (192.168.1.11)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: http (80), Dst Port: 49215 (49215), Seq: 1, Ack: 453, Len: 434
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 27 Jan 2014 00:43:20 GMT\r\n
Server: Apache/2.2.3 (CentOS)\r\n
Last-Modified: Mon, 27 Jan 2014 00:43:01 GMT\r\n
ETag: "8734b-51-fd624f40"\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
[HTTP response 2/2]
[Time since request: 0.093749000 seconds]
[Prev request in frame: 39]
[Request in frame: 41]
Line-based text data: text/html
<html>\r\n
Congratulations! You've downloaded the first Wireshark lab file!\r\n
</html>\r\n