

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

No.	Time	Source	Destination	Protocol	Length	Info
20	12.620913	192.168.0.7	64.233.167.189	QUIC	80	Payload (Encrypted), CID: 168993240893453.
21	14.553237	192.168.0.7	192.168.0.1	DNS	77	Standard query 0x6add A gaia.cs.umass.edu
22	14.683127	192.168.0.1	192.168.0.7	DNS	93	Standard query response 0x6add A gaia.cs...
23	14.684664	192.168.0.7	128.119.245.12	TCP	78	51601 → 80 [SYN] Seq=0 Win=65535 Len=0 MS...
24	14.805720	128.119.245.12	192.168.0.7	TCP	74	80 → 51601 [SYN, ACK] Seq=0 Ack=1 Win=289...
25	14.805818	192.168.0.7	128.119.245.12	TCP	66	51601 → 80 [ACK] Seq=1 Ack=1 Win=131744 L...
26	14.830741	192.168.0.7	128.119.245.12	HTTP	312	GET /wireshark-labs/INTRO-wireshark-file1...
27	14.954625	128.119.245.12	192.168.0.7	TCP	66	80 → 51601 [ACK] Seq=1 Ack=247 Win=30080 ...
28	14.954630	128.119.245.12	192.168.0.7	HTTP	506	HTTP/1.1 200 OK (text/html)
29	14.954719	192.168.0.7	128.119.245.12	TCP	66	51601 → 80 [ACK] Seq=247 Ack=441 Win=1313...
30	16.252944	192.168.0.7	192.168.0.1	DNS	77	Standard query 0xd1fa A gaia.cs.umass.edu
31	16.255102	192.168.0.1	192.168.0.7	DNS	93	Standard query response 0xd1fa A gaia.cs...
32	16.256302	192.168.0.7	128.119.245.12	TCP	78	51627 → 80 [SYN] Seq=0 Win=65535 Len=0 MS...
33	16.257631	192.168.0.7	54.247.164.119	HTTP	196	GET /V3/01/12.245.119.128.ip/ HTTP/1.1
34	16.259609	192.168.0.7	54.247.164.119	HTTP	252	GET /V3/01/1.jverfunex-2qynof-2sVAGEB-2qj...

▶ Frame 26: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface 0

0000 5c d9 98 c2 4a af 3c 15 c2 bc f3 9e 08 00 45 00 \...J... .....

## 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.)*

**The HTTP GET message arrived at Jun 20, 2016 17:17:46.653080000 BST:**

26	14.830741	192.168.0.7	128.119.245.12	HTTP	312	GET /wireshark-labs/INTRO-wireshark-file1..
27	14.954625	128.119.245.12	192.168.0.7	TCP	66	80 → 51601 [ACK] Seq=1 Ack=247 Win=30080 ..

Frame 26: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface 0  
 Interface id: 0 (en0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Jun 20, 2016 17:17:46.653080000 BST

**The HTTP OK message arrived at Jun 20, 2016 17:17:46.776969000 BST:**

```

28 14.954630    128.119.245.12    192.168.0.7      HTTP      506 HTTP/1.1 200 OK (text/html)
ame 28: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Jun 20, 2016 17:17:46.776969000 BST

```

**So, it took about 124 ms for the OK message to be received.**

3. *What is the Internet address of the [gaia.cs.umass.edu](http://gaia.cs.umass.edu) (also known as [www.net.cs.umass.edu](http://www.net.cs.umass.edu))? What is the Internet address of your computer?*

**The IP address of [www.net.cs.umass.edu](http://www.net.cs.umass.edu) is 128.119.245.12 and the IP address of my computer is 192.168.0.7.**

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.*

**I printed them both as PDF's, which I have attached below (first the GET and then the OK message):**

```
26 14.830741      192.168.0.7      128.119.245.12      HTTP      312      GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 26: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Jun 20, 2016 17:17:46.653080000 BST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1466439466.653080000 seconds
[Time delta from previous captured frame: 0.024923000 seconds]
[Time delta from previous displayed frame: 0.024923000 seconds]
[Time since reference or first frame: 14.830741000 seconds]
Frame Number: 26
Frame Length: 312 bytes (2496 bits)
Capture Length: 312 bytes (2496 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: D-LinkCo_c2:4a:af (5c:d9:98:c2:4a:af)
Destination: D-LinkCo_c2:4a:af (5c:d9:98:c2:4a:af)
Source: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.7, Dst: 128.119.245.12
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 298
Identification: 0x7800 (30720)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x8b9a [validation disabled]
Source: 192.168.0.7
Destination: 128.119.245.12
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 51601 (51601), Dst Port: 80 (80), Seq: 1, Ack: 1, Len:
246
Source Port: 51601
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 246]
Sequence number: 1      (relative sequence number)
[Next sequence number: 247      (relative sequence number)]
Acknowledgment number: 1      (relative ack number)
Header Length: 32 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 4117
[Calculated window size: 131744]
[Window size scaling factor: 32]
Checksum: 0x076b [validation disabled]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
From: 192.168.0.7\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/14.64.0\r\n
Accept: */*\r\n
```

Accept-Language: en\r\n  
Content-Length: 0\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 1/1]  
[Response in frame: 28]

```
28 14.954630      128.119.245.12      192.168.0.7      HTTP      506      HTTP/1.1 200 OK
(text/html)
Frame 28: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Jun 20, 2016 17:17:46.776969000 BST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1466439466.776969000 seconds
[Time delta from previous captured frame: 0.000005000 seconds]
[Time delta from previous displayed frame: 0.000005000 seconds]
[Time since reference or first frame: 14.954630000 seconds]
Frame Number: 28
Frame Length: 506 bytes (4048 bits)
Capture Length: 506 bytes (4048 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: D-LinkCo_c2:4a:af (5c:d9:98:c2:4a:af), Dst: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e)
Destination: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e)
Source: D-LinkCo_c2:4a:af (5c:d9:98:c2:4a:af)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.7
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 492
Identification: 0x9b8a (39818)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 53
Protocol: TCP (6)
Header checksum: 0x724e [validation disabled]
Source: 128.119.245.12
Destination: 192.168.0.7
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 51601 (51601), Seq: 1, Ack: 247, Len:
440
Source Port: 80
Destination Port: 51601
[Stream index: 1]
[TCP Segment Len: 440]
Sequence number: 1      (relative sequence number)
[Next sequence number: 441      (relative sequence number)]
Acknowledgment number: 247      (relative ack number)
Header Length: 32 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 235
[Calculated window size: 30080]
[Window size scaling factor: 128]
Checksum: 0x6db2 [validation disabled]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 20 Jun 2016 16:17:46 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
\n
Last-Modified: Mon, 20 Jun 2016 05:59:01 GMT\r\n
```

```
ETag: "51-535af66ac2cd6"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
```

```
[HTTP response 1/1]
```

```
[Time since request: 0.123889000 seconds]
```

```
[Request in frame: 26]
```

```
Line-based text data: text/html
```

```
<html>\n
```

```
Congratulations! You've downloaded the first Wireshark lab file!\n
```

```
</html>\n
```