

Wireshark Lab: Getting Started v6.0

LAB SOLUTION #1

90009559

MANASI SHARMA

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

ANSWER:

The protocols that appeared in the protocol column in the unfiltered packet-listing window in step above: TCP, ARP, HTTP.

No.	Time	Source	Destination	Protocol	Length	Info
31	22:05:38.635872000	Netgear_e1:c8:28	Apple_0f:31:e8	ARP	42	192.168.2.1 j
32	22:05:38.779786000	127.0.0.1	127.0.0.1	TCP	56	57537→8585 [f
33	22:05:38.635920000	192.168.2.25	128.119.245.12	TCP	78	57538→80 [SYN
34	22:05:38.779822000	127.0.0.1	127.0.0.1	TCP	56	8585→57537 [A
35	22:05:38.701299000	128.119.245.12	192.168.2.25	TCP	74	80→57538 [SYN
36	22:05:38.701508000	192.168.2.25	128.119.245.12	TCP	66	57538→80 [ACK
37	22:05:38.702831000	192.168.2.25	128.119.245.12	HTTP	695	GET /wireshar
38	22:05:38.770768000	128.119.245.12	192.168.2.25	TCP	66	80→57538 [ACK
39	22:05:38.771912000	128.119.245.12	192.168.2.25	HTTP	446	HTTP/1.1 200
40	22:05:38.771999000	192.168.2.25	128.119.245.12	TCP	66	57538→80 [ACK
41	22:05:39.058385000	192.168.2.12	255.255.255.255	DB-LSP-DI	145	Dropbox LAN s
42	22:05:39.060102000	192.168.2.12	255.255.255.255	DB-LSP-DI	145	Dropbox LAN s
43	22:05:39.061818000	192.168.2.12	255.255.255.255	DB-LSP-DI	145	Dropbox LAN s

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:

```
▼ Frame 37: 695 bytes on wire (5560 bits), 695 bytes captured (5560 bits) on interface 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 20, 2014 22:05:38.702831000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1413857138.702831000 seconds
[Time delta from previous captured frame: 0.001323000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 3.004268000 seconds]
Frame Number: 37
Frame Length: 695 bytes (5560 bits)
Capture Length: 695 bytes (5560 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Number of per-protocol-data: 1]
[Hypertext Transfer Protocol, key 0]
```

The frame section of the GET request : the time the packet arrived is 22:05:38.702831000

```
▼ Frame 39: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 20, 2014 22:05:38.771912000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1413857138.771912000 seconds
[Time delta from previous captured frame: 0.001144000 seconds]
[Time delta from previous displayed frame: 0.069081000 seconds]
[Time since reference or first frame: 3.073349000 seconds]
Frame Number: 39
Frame Length: 446 bytes (3568 bits)
Capture Length: 446 bytes (3568 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Number of per-protocol-data: 1]
[Hypertext Transfer Protocol, key 0]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
▶ Ethernet II, Src: Netgear_el:c8:28 (84:1b:5e:e1:c8:28), Dst: Apple_0f:31:e8 (2c:f0:ee:0f:31:e8)
```

The frame section of the GET request : the time the packet arrived is 22:05:38.771912000

Therefore, the time took from HTTP GET to HTTP OK is

$$.771912000 - .702831000 = 0.069081000 \text{ second}$$

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

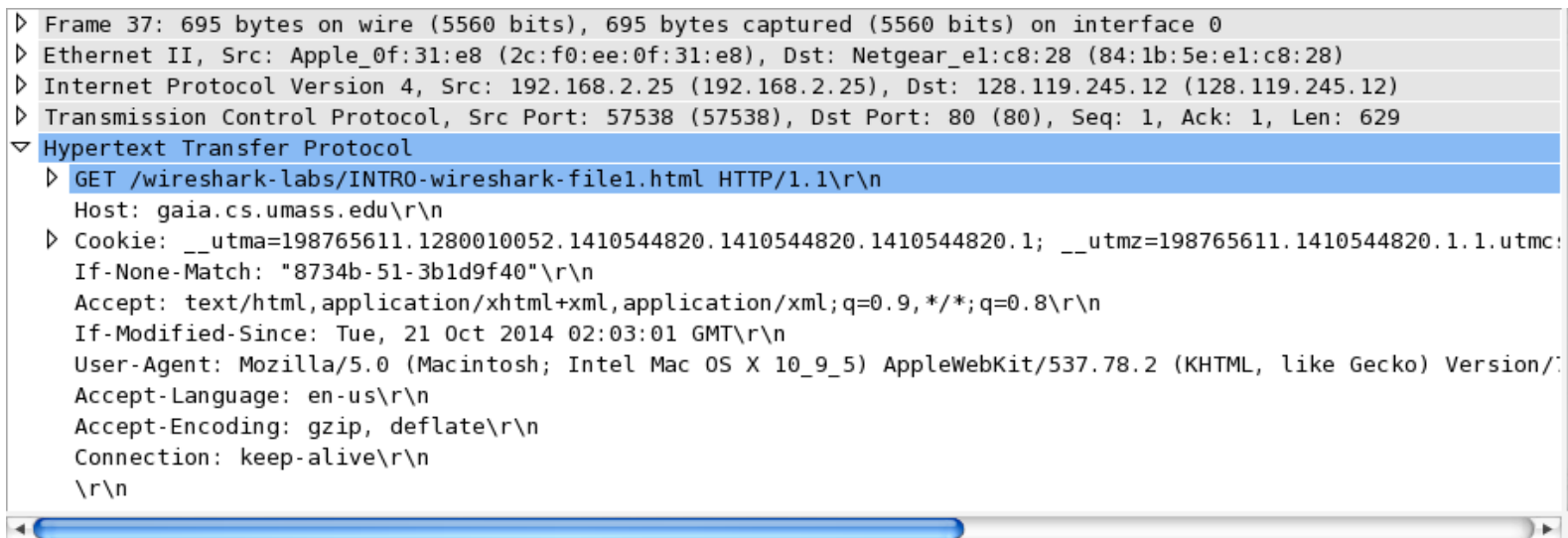
```
Protocol: TCP (6)
  Header checksum: 0x0147 [validation disabled]
  Source: 128.119.245.12 (128.119.245.12)
  Destination: 192.168.2.25 (192.168.2.25)
```

This datagram is HTTP GET. It is sent from my computer to the web server.

My computer's IP address is 128.119.245.12 (source)

The web server's IP address is 192.168.2.25(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.



.....

- ▷ Frame 39: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0
- ▷ Ethernet II, Src: Netgear_e1:c8:28 (84:1b:5e:e1:c8:28), Dst: Apple_0f:31:e8 (2c:f0:ee:0f:31:e8)
- ▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.25 (192.168.2.25)
- ▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 57538 (57538), Seq: 1, Ack: 630, Len: 380

▼ Hypertext Transfer Protocol

- ▷ HTTP/1.1 200 OK\r\n
 - Date: Tue, 21 Oct 2014 02:05:38 GMT\r\n
 - Server: Apache/2.2.3 (CentOS)\r\n
 - Last-Modified: Tue, 21 Oct 2014 02:05:01 GMT\r\n
 - ETag: "8734b-51-4244ad40"\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

