

## **Computer Network**

### **WireShark Lab 2**

**By:**

**Monil Shah**

**mds747**

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Ans. My Browser: HTTP version 1.1

Server: HTTP Version 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?

Ans. en-US

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Ans. My Computer: 192.168.1.161

Server: 128.119.245.12

4. What is the status code returned from the server to your browser?

Ans. Status Code : 200 OK

5. When was the HTML file that you are retrieving last modified at the server?

Ans. Wed Feb 15,2017 06:59:01 GMT

6. How many bytes of content are being returned to your browser?

Ans. 128 bytes

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Ans. No. File Data and Content-Length is same.

```
/var/folders/9w/3sz6p5916gd99qw1yxj6__zw0000gn/T//wireshark_en0_20170215220912_4kZCuI.pcapng 235 total packets, 4 shown
56 22:09:32.160549 192.168.1.161 128.119.245.12 HTTP 492 GET /
wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 56: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49344, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/56.0.2924.87 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 58]
[Next request in frame: 60]
```

```

58 22:09:32.176489 128.119.245.12 192.168.1.161 HTTP 552 HTTP/1.1
200 OK (text/html)
Frame 58: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Ethernet II, Src: Verizon_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.161
Transmission Control Protocol, Src Port: 80, Dst Port: 49344, Seq: 1, Ack: 427, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 16 Feb 2017 03:09:32 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Wed, 15 Feb 2017 06:59:01 GMT\r\n
ETag: "80-5488c5724d16b"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\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 1/2]
[Time since request: 0.015940000 seconds]
[Request in frame: 56]
[Next request in frame: 60]
[Next response in frame: 61]
File Data: 128 bytes
Line-based text data: text/html

```

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Ans. No

```

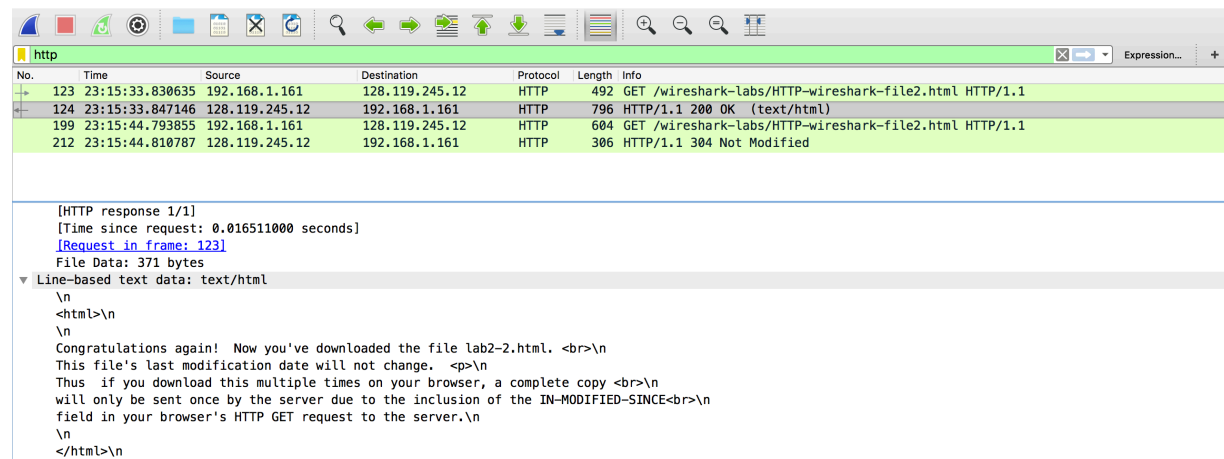
/var/folders/9w/3sz6p5916gd99qw1yxj6__zw0000gn/T/wireshark_en0_20170215231526_rD4cyx.pcapng 250 total packets, 4 shown

123 23:15:33.830635 192.168.1.161 128.119.245.12 HTTP 492 GET /
wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 123: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49971, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/56.0.2924.87 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 124]

```

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Ans. Yes it returns. See screenshot below



No.	Time	Source	Destination	Protocol	Length	Info
123	23:15:33.830635	192.168.1.161	128.119.245.12	HTTP	492	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
124	23:15:33.847146	128.119.245.12	192.168.1.161	HTTP	796	HTTP/1.1 200 OK (text/html)
199	23:15:44.793855	192.168.1.161	128.119.245.12	HTTP	604	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
212	23:15:44.810787	128.119.245.12	192.168.1.161	HTTP	306	HTTP/1.1 304 Not Modified

[HTTP response 1/1]  
[Time since request: 0.016511000 seconds]  
[Request in frame: 123]  
File Data: 371 bytes

Line-based text data: text/html

```
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans. Yes. Wed, Feb 15 2017 06:59:01 GMT

```
/var/folders/9w/3sz6p5916gd99qw1yxj6__zw0000gn/T//wireshark_en0_20170215231526_rD4cyx.pcapng 250 total packets, 4 shown

199 23:15:44.793855 192.168.1.161 128.119.245.12 HTTP 604 GET /
wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 199: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits) on interface 0
Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49975, Dst Port: 80, Seq: 1, Ack: 1, Len: 538
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/56.0.2924.87 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
If-None-Match: "173-5488c3724c5b3"\r\n
If-Modified-Since: Wed, 15 Feb 2017 06:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 212]
```

11. What is the HTTP status code and phrase returned from the

server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Ans. 304 Not Modified. This is much shorter than the full response packet seen previously. The file is already in cache memory.

```
/var/folders/9w/3sz6p5916gd99qwlyxj6__zw0000gn/T//wireshark_en0_20170215231526_rD4cyx.pcapng 250 total packets, 4 shown

212 23:15:44.810787 128.119.245.12 192.168.1.161 HTTP 306 HTTP/1.1
304 Not Modified
Frame 212: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface 0
Ethernet II, Src: Verizon_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.161
Transmission Control Protocol, Src Port: 80, Dst Port: 49975, Seq: 1, Ack: 539, Len: 240
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Date: Thu, 16 Feb 2017 04:15:44 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-5488c3724c5b3"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.016932000 seconds]
[Request in frame: 199]
```

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Ans. One HTTP GET Request. Packet Number: 11

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Ans. Packet Number: 16

14. What is the status code and phrase in the response?

Ans. HTTP/1.1 200 OK

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of

Rights?

Ans. Four TCP Segments

The image shows a Wireshark packet capture of an HTTP GET request. The packet list shows two packets: packet 11 (HTTP GET) and packet 16 (HTTP GET). Packet 16 is selected, and the packet details pane shows the reassembled TCP segments. The segments are: [Frame: 13, payload: 0-1447 (1448 bytes)], [Frame: 14, payload: 1448-2895 (1448 bytes)], [Frame: 15, payload: 2896-4343 (1448 bytes)], and [Frame: 16, payload: 4344-4860 (517 bytes)]. The total reassembled TCP length is 4861 bytes. The packet details pane also shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol headers.

No.	Time	Source	Destination	Protocol	Length	Info
11	23:43:50.139680	192.168.1.161	128.119.245.12	HTTP	492	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
16	23:43:50.159124	128.119.245.12	192.168.1.161	HTTP	583	HTTP/1.1 200 OK (text/html)

Frame 16: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0  
Ethernet II, Src: Verizon\_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple\_9c:a6:65 (4c:32:75:9c:a6:65)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.161  
Transmission Control Protocol, Src Port: 80, Dst Port: 50010, Seq: 4345, Ack: 427, Len: 517  
[4 Reassembled TCP Segments (4861 bytes): #13(1448), #14(1448), #15(1448), #16(517)]  
[Frame: 13, payload: 0-1447 (1448 bytes)]  
[Frame: 14, payload: 1448-2895 (1448 bytes)]  
[Frame: 15, payload: 2896-4343 (1448 bytes)]  
[Frame: 16, payload: 4344-4860 (517 bytes)]  
[Segment count: 4]  
[Reassembled TCP length: 4861]  
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a2054...]

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Ans. Four GET request message browser send.

Internet Addresses: 128.119.245.12

128.119.240.90

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain

Ans. Images were downloaded serially. The source ports are incrementing every time using separate TCP connections.

Source Ports: 50047,50048,50049

The image displays two screenshots of the Wireshark network traffic analysis tool. The top screenshot shows a list of captured packets, with packet 22 selected. The bottom screenshot shows the details of packet 45, which is an HTTP GET request for a file named 'cover\_5th\_ed.jpg'.

No.	Time	Source	Destination	Protocol	Length	Info
16	00:02:20.214971	192.168.1.161	128.119.245.12	HTTP	492	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
17	00:02:20.242570	128.119.245.12	192.168.1.161	HTTP	1139	HTTP/1.1 200 OK (text/html)
22	00:02:20.250260	192.168.1.161	128.119.245.12	HTTP	463	GET /pearson.png HTTP/1.1
27	00:02:20.276581	128.119.245.12	192.168.1.161	HTTP	781	HTTP/1.1 200 OK (PNG)
32	00:02:20.277972	192.168.1.161	128.119.240.90	HTTP	477	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
34	00:02:20.297069	128.119.240.90	192.168.1.161	HTTP	522	HTTP/1.1 302 Found (text/html)
45	00:02:20.317593	192.168.1.161	128.119.240.90	HTTP	477	GET /~kurose/cover_5th_ed.jpg HTTP/1.1

Frame 22: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface 0

- Ethernet II, Src: Apple\_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon\_f1:47:66 (48:5d:36:f1:47:66)
- Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 50047, Dst Port: 80, Seq: 427, Ack: 1074, Len: 397
  - Source Port: 50047
  - Destination Port: 80
  - [Stream index: 1]
  - [TCP Segment Len: 397]
  - Sequence number: 427 (relative sequence number)
  - [Next sequence number: 824 (relative sequence number)]
  - Acknowledgment number: 1074 (relative ack number)
  - Header Length: 32 bytes
  - Flags: 0x018 (PSH, ACK)
  - Window size value: 4096
  - [Calculated window size: 131072]

Frame 45: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface 0

- Ethernet II, Src: Apple\_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon\_f1:47:66 (48:5d:36:f1:47:66)
- Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.240.90
- Transmission Control Protocol, Src Port: 50049, Dst Port: 80, Seq: 1, Ack: 1, Len: 411
  - Source Port: 50049
  - Destination Port: 80
  - [Stream index: 3]
  - [TCP Segment Len: 411]
  - Sequence number: 1 (relative sequence number)
  - [Next sequence number: 412 (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]

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?  
 Ans. HTTP/1.1 401 Unauthorized

/var/folders/9w/3sz6p5916gd99qw1yxj6\_\_zw0000gn/T//wireshark\_en0\_20170216002730\_LFe5te.pcapng 1119 total packets, 4 shown

```
911 00:27:54.427255 128.119.245.12 192.168.1.161 HTTP 783 HTTP/1.1
401 Unauthorized (text/html)
Frame 911: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits) on interface 0
Ethernet II, Src: Verizon_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.161
Transmission Control Protocol, Src Port: 80, Dst Port: 50091, Seq: 1, Ack: 442, Len: 717
  Source Port: 80
  Destination Port: 50091
  [Stream index: 11]
  [TCP Segment Len: 717]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 718 (relative sequence number)]
  Acknowledgment number: 442 (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: 0x960f [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [SEQ/ACK analysis]
Hypertext Transfer Protocol
  HTTP/1.1 401 Unauthorized\r\n
```

ANS 18

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Ans. AUTHORIZATION is the new field included in the HTTP GET message as shown in screenshot below.



```
1056 00:28:27.759275 192.168.1.161 128.119.245.12 HTTP 566 GET /
wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
Frame 1056: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface 0
Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50094, Dst Port: 80, Seq: 1, Ack: 1, Len: 500
  Source Port: 50094
  Destination Port: 80
  [Stream index: 18]
  [TCP Segment Len: 500]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 501 (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: 0xbba1 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [SEQ/ACK analysis]
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm0=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like
```

ANS 19