

## LAB 2 PART ONE

Screenshots:

GET request:

MY IP

// gaia IP

HTTP Version

No.	Time	Source	Destination	Protocol	Leng	Info
7	0.074793	69.91.217.229	128.119.245.12	HTTP	470	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
15	0.150959	128.119.245.12	69.91.217.229	HTTP	542	HTTP/1.1 200 OK (text/html)
17	1.176774	69.91.217.229	128.119.245.12	HTTP	416	GET /favicon.ico HTTP/1.1
18	1.255035	128.119.245.12	69.91.217.229	HTTP	540	HTTP/1.1 404 Not Found (text/html)

> Frame 7: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface 0

> Ethernet II, Src: IntelCor\_84:1b:2e (60:57:18:84:1b:2e), Dst: IETF-VRRP-VRID\_27 (00:00:5e:00:01:27)

> Internet Protocol Version 4, Src: 69.91.217.229, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 55561, Dst Port: 80, Seq: 1, Ack: 1, Len: 416

> Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file1.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 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: 15]

[Next request in frame: 17]

Response:

HTTP Version

1st Status Code

2nd Status Code

No.	Time	Source	Destination	Protocol	Leng	Info
7	0.074793	69.91.217.229	128.119.245.12	HTTP	470	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
15	0.150959	128.119.245.12	69.91.217.229	HTTP	542	HTTP/1.1 200 OK (text/html)
17	1.176774	69.91.217.229	128.119.245.12	HTTP	416	GET /favicon.ico HTTP/1.1
18	1.255035	128.119.245.12	69.91.217.229	HTTP	540	HTTP/1.1 404 Not Found (text/html)

> Frame 15: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0

> Ethernet II, Src: JuniperN\_ef:ef:f0 (88:e0:f3:ef:ef:f0), Dst: IntelCor\_84:1b:2e (60:57:18:84:1b:2e)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 69.91.217.229

> Transmission Control Protocol, Src Port: 80, Dst Port: 55561, Seq: 1, Ack: 417, Len: 488

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK

Date: Wed, 12 Oct 2016 20:15:20 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

Last-Modified: Wed, 12 Oct 2016 05:59:01 GMT\r\n

Etag: "80-53ea4b0944bd7"\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: 0.07616000 seconds]

[Request in frame: 7]

[Next request in frame: 17]

[Next response in frame: 18]

File Data: 128 bytes

> Line-based text data: text/html

Questions:

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

My browser is running HTTP version 1.1. The server is also running HTTP version 1.1

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

The Accept-Language part of the header indicates that it will accept en-US or US English at a quality value of 1.0 then English at a quality value of .8

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

My computer is at: 69.91.217.229

The gaia.cs.umass.edu is located at: 128.119.245.12

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

The returned status code for the first request was 200 or OK

A second request was made and the server returned a status code of 404 or Not Found

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

The date and time indicated by the last-modified field is Wed, 12 Oct 2016 and 5:59:01 GMT

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

128 Bytes are being returned to the browser

**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.**

Some of the data included in the other layers of the protocol are in the header including the acknowledgement number for the TCP and an Urgent Pointer which is also included in the TCP information.

**PART 2**

## GET Request #1

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane at the top shows several packets, with packet 48 selected. The packet details pane below shows the structure of the selected packet:

- Frame 37: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface 0
- Ethernet II, Src: IntelCor\_84:1b:2e (60:57:18:84:1b:2e), Dst: Cisco-Li\_94:a4:05 (48:f8:b3:94:a4:05)
- Internet Protocol Version 4, Src: 192.168.1.125, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 56636, Dst Port: 80, Seq: 1, Ack: 1, Len: 416
- 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 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 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 1/2]
  - [Response in frame: 48]
  - [Next request in frame: 91]

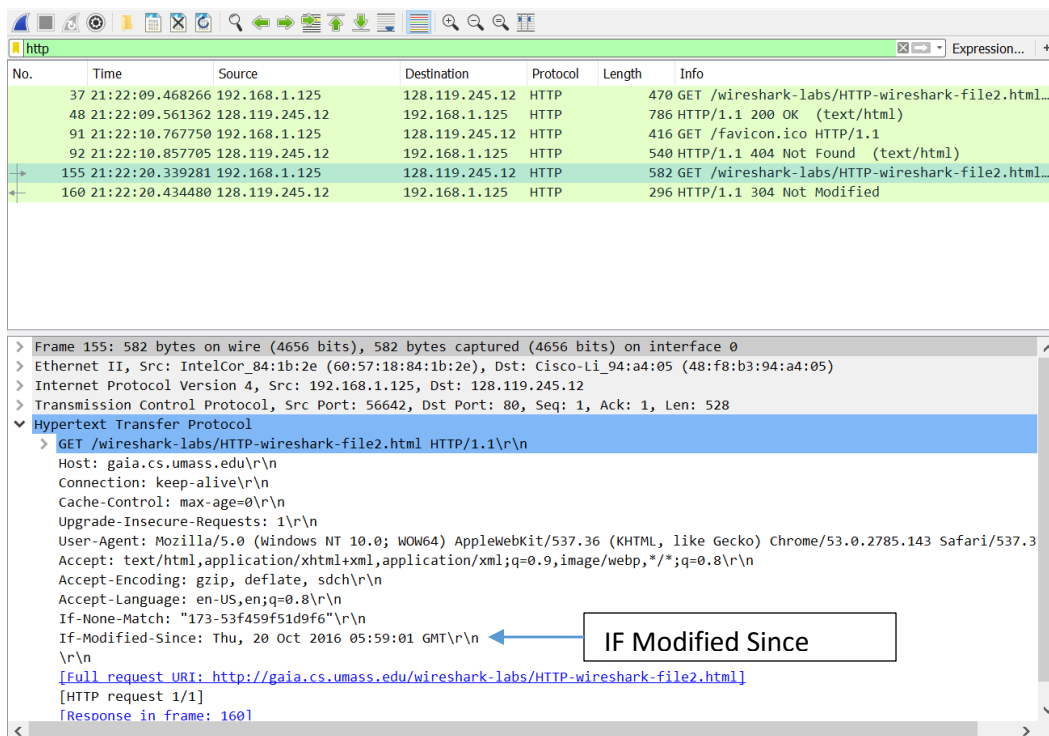
## GET Response #1

The screenshot shows a Wireshark capture of an HTTP GET response. The packet list pane at the top shows several packets, with packet 48 selected. The packet details pane below shows the structure of the selected packet:

- Frame 48: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface 0
- Ethernet II, Src: Cisco-Li\_94:a4:05 (48:f8:b3:94:a4:05), Dst: IntelCor\_84:1b:2e (60:57:18:84:1b:2e)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.125
- Transmission Control Protocol, Src Port: 80, Dst Port: 56636, Seq: 1, Ack: 417, Len: 732
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
  - Date: Fri, 21 Oct 2016 04:22:03 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
  - Last-Modified: Thu, 20 Oct 2016 05:59:01 GMT\r\n
  - ETag: "173-53f459f51d9f6"\r\n
  - Accept-Ranges: bytes\r\n
  - Content-Length: 371\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: 0.093096000 seconds]
  - [Request in frame: 37]
  - [Next request in frame: 91]
  - [Next response in frame: 92]

A blue arrow points from the text box "Content Length 371 = size of html doc" to the "Content-Length: 371\r\n" line in the packet details pane.

## GET Request #2



Wireshark packet capture showing GET Request #2. The packet list table is as follows:

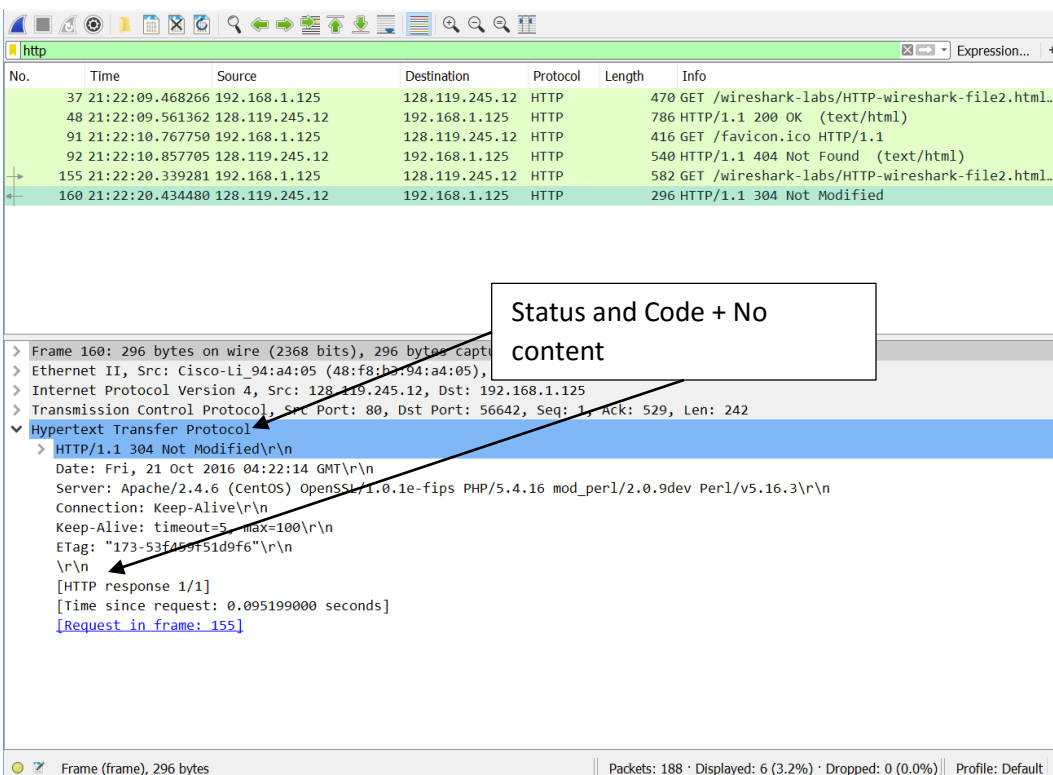
No.	Time	Source	Destination	Protocol	Length	Info
37	21:22:09.468266	192.168.1.125	128.119.245.12	HTTP	470	GET /wireshark-labs/HTTP-wireshark-file2.html...
48	21:22:09.561362	128.119.245.12	192.168.1.125	HTTP	786	HTTP/1.1 200 OK (text/html)
91	21:22:10.767750	192.168.1.125	128.119.245.12	HTTP	416	GET /favicon.ico HTTP/1.1
92	21:22:10.857705	128.119.245.12	192.168.1.125	HTTP	540	HTTP/1.1 404 Not Found (text/html)
155	21:22:20.339281	192.168.1.125	128.119.245.12	HTTP	582	GET /wireshark-labs/HTTP-wireshark-file2.html...
160	21:22:20.434480	128.119.245.12	192.168.1.125	HTTP	296	HTTP/1.1 304 Not Modified

The packet details pane for frame 155 shows the Hypertext Transfer Protocol section:

```
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.3\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate, sdch\r\nAccept-Language: en-US,en;q=0.8\r\nIf-None-Match: "173-53f459f51d9f6"\r\nIf-Modified-Since: Thu, 20 Oct 2016 05:59:01 GMT\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]\r\n[HTTP request 1/1]\r\n[Response in frame: 160]
```

A callout box labeled "IF Modified Since" points to the "If-Modified-Since" header field.

## Response #2



Wireshark packet capture showing Response #2. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
37	21:22:09.468266	192.168.1.125	128.119.245.12	HTTP	470	GET /wireshark-labs/HTTP-wireshark-file2.html...
48	21:22:09.561362	128.119.245.12	192.168.1.125	HTTP	786	HTTP/1.1 200 OK (text/html)
91	21:22:10.767750	192.168.1.125	128.119.245.12	HTTP	416	GET /favicon.ico HTTP/1.1
92	21:22:10.857705	128.119.245.12	192.168.1.125	HTTP	540	HTTP/1.1 404 Not Found (text/html)
155	21:22:20.339281	192.168.1.125	128.119.245.12	HTTP	582	GET /wireshark-labs/HTTP-wireshark-file2.html...
160	21:22:20.434480	128.119.245.12	192.168.1.125	HTTP	296	HTTP/1.1 304 Not Modified

The packet details pane for frame 160 shows the Hypertext Transfer Protocol section:

```
> HTTP/1.1 304 Not Modified\r\nDate: Fri, 21 Oct 2016 04:22:14 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\nConnection: Keep-Alive\r\nKeep-Alive: timeout=5,max=100\r\nETag: "173-53f459f51d9f6"\r\n\r\n[HTTP response 1/1]\r\n[Time since request: 0.095199000 seconds]\r\n[Request in frame: 155]
```

Two callout boxes are present: "Status and Code + No content" points to the "304 Not Modified" status line, and "IF Modified Since" points to the "If-None-Match" header field in the previous frame's details.

- 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?**

No, it is not there.

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

In the header it declares the content length being 371, which is the exact length of the text/html file. Meaning the server did not send anything extra beyond the file and the information in the response header.

In the response header however there's an extra field called Etag which is sent back to the server in the second HTTP GET response, meaning it was likely sent by the server and saved by the client.

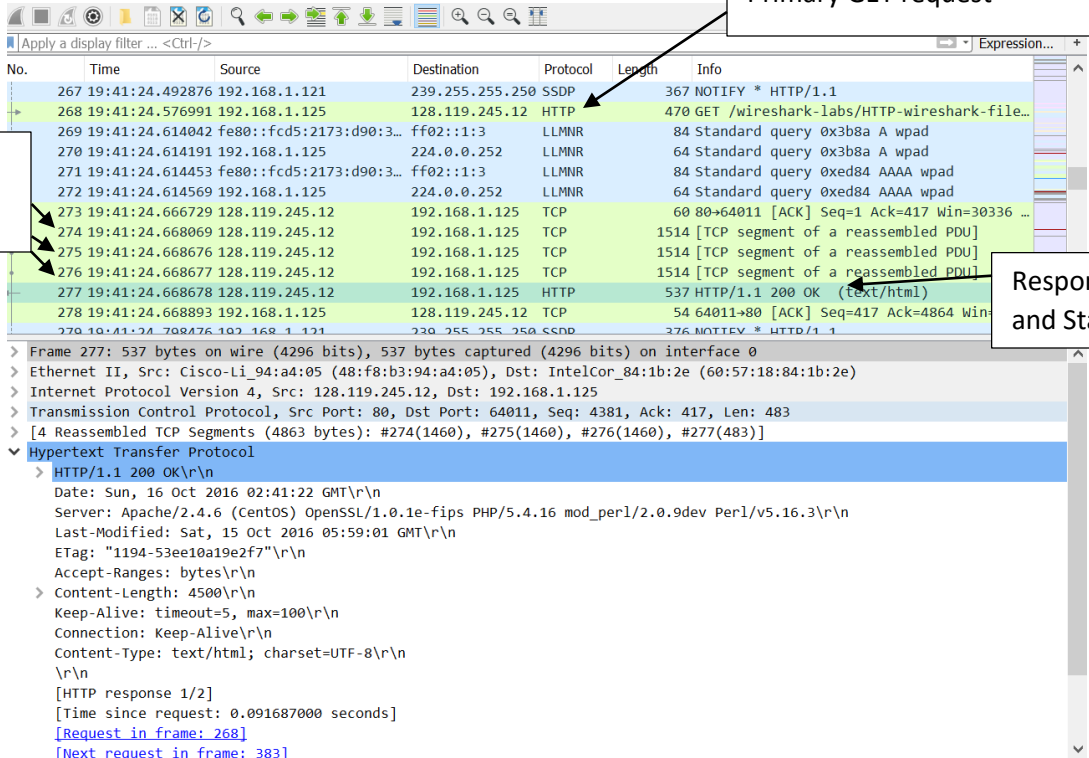
- 10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?**

The IF-MODIFIED-SINCE header is followed by the date Sat, 15 Oct 2016 05:59:01 GMT\r\n

- 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.**

The HTTP Status code and phrase returned by the response to the second GET request is Status code: 304 with Response Phrase: Not Modified. The server does not return the contents of the file because it determined sending the contents of the file is unnecessary as the file had not been modified since it was previously sent. The ETag is sent again though.

### PART 3



The image shows a Wireshark packet capture of an HTTP transaction. The packet list pane displays the following key packets:

No.	Time	Source	Destination	Protocol	Length	Info
267	19:41:24.492876	192.168.1.121	239.255.255.250	SSDP	367	NOTIFY * HTTP/1.1
268	19:41:24.576991	192.168.1.125	128.119.245.12	HTTP	470	GET /wireshark-labs/HTTP-wireshark-file...
269	19:41:24.614042	fe80::fcd5:2173:d90:3...	ff02::1:3	LLMNR	84	Standard query 0x3b8a A wpa
270	19:41:24.614191	192.168.1.125	224.0.0.252	LLMNR	64	Standard query 0x3b8a A wpa
271	19:41:24.614453	fe80::fcd5:2173:d90:3...	ff02::1:3	LLMNR	84	Standard query 0xed84 AAAA wpa
272	19:41:24.614569	192.168.1.125	224.0.0.252	LLMNR	64	Standard query 0xed84 AAAA wpa
273	19:41:24.666729	128.119.245.12	192.168.1.125	TCP	60	80->64011 [ACK] Seq=1 Ack=417 Win=30336 ...
274	19:41:24.668069	128.119.245.12	192.168.1.125	TCP	1514	[TCP segment of a reassembled PDU]
275	19:41:24.668676	128.119.245.12	192.168.1.125	TCP	1514	[TCP segment of a reassembled PDU]
276	19:41:24.668677	128.119.245.12	192.168.1.125	TCP	1514	[TCP segment of a reassembled PDU]
277	19:41:24.668678	128.119.245.12	192.168.1.125	HTTP	537	HTTP/1.1 200 OK (text/html)
278	19:41:24.668893	192.168.1.125	128.119.245.12	TCP	54	64011->80 [ACK] Seq=417 Ack=4864 Win...

The packet details pane for packet 277 shows the following HTTP response structure:

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Sun, 16 Oct 2016 02:41:22 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
    Last-Modified: Sat, 15 Oct 2016 05:59:01 GMT\r\n
    ETag: "1194-53ee10a19e2f7"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\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: 0.091687000 seconds]
    [Request in frame: 268]
    [Next request in frame: 383]
  
```

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?

My browser sent two GET requests, packet numbers 268 and 383. Packet number 268, the first one, contains the GET message for the bill of rights. The second request is requesting the /favicon.ico, which gets a 404 Not found response.

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

Packet Number 277 has the code and phrase associated with the response.

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

The status is 200 and the phrase is OK.

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

There were three TCP responses sent of length 1514 each.

## PART 4

Wireshark packet capture showing HTTP traffic. The packet list displays several GET requests. A callout box highlights 5 GET requests based on times, indicating they are sent before kurose starts.

No.	Time	Source	Destination	Protocol	Length	Info
118	21:08:56.896092	192.168.1.125	128.119.245.12	HTTP	470	GET /Wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
126	21:08:56.991758	128.119.245.12	192.168.1.125	HTTP	1129	HTTP/1.1 200 OK (text/html)
132	21:08:57.001590	192.168.1.125	128.119.245.12	HTTP	441	GET /pearson.png HTTP/1.1
136	21:08:57.095010	128.119.245.12	192.168.1.125	HTTP	747	HTTP/1.1 200 OK (PNG)
163	21:08:57.442072	192.168.1.125	128.119.240.90	HTTP	455	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
167	21:08:57.531710	128.119.240.90	192.168.1.125	HTTP	510	HTTP/1.1 302 Found (text/html)
179	21:08:57.791856	192.168.1.125	128.119.240.90	HTTP	455	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
274	21:08:58.296373	128.119.240.90	192.168.1.125	HTTP	526	HTTP/1.1 200 OK (JPEG JFIF image)
277	21:08:58.310737	192.168.1.125	128.119.245.12	HTTP	416	GET /favicon.ico HTTP/1.1
279	21:08:58.397557	128.119.245.12	192.168.1.125	HTTP	540	HTTP/1.1 404 Not Found (text/html)

Frame 118: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface 0  
> Ethernet II, Src: IntelCor\_84:1b:2e (60:57:18:84:1b:2e), Dst: Cisco-Li\_94:a4:05 (48:f8:b3:94:a4:05)  
> Internet Protocol Version 4, Src: 192.168.1.125, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 64508, Dst Port: 80, Seq: 1, Ack: 1, Len: 416  
> Hypertext Transfer Protocol

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

There were a total of 5 GET requests sent from my browser.

No. 118 gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

No. 132 gaia.cs.umass.edu/pearson.png

No. 163 manic.cs.umass.edu/~kurose/cover\_5<sup>th</sup>\_ed.jpg

No. 179 caite.cs.umass.edu/~kurose/cover\_5<sup>th</sup>\_ed.jpg

No. 279 gaia.cs.umass.edu/favicon.ico

### 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.

The two images were downloaded serially. You can tell it's done serially by the sequence of events. The second GET request is not made until the first response is received and the image is sent, meaning they are not happening at the same time as they would if the images were downloaded in parallel.

## PART 5

http

Response 1 Status and Code

No.	Time	Source	Destination	Protocol	Length	Info
1626	20:57:00.843731	192.168.1.125	128.119.245.12	HTTP	485	GET /wireshark-labs/protected_pages/HTTP-wireshar...
1631	20:57:00.938657	128.119.245.12	192.168.1.125	HTTP	773	HTTP/1.1 401 Unauthorized (text/html)
1696	20:57:21.753363	192.168.1.125	128.119.245.12	HTTP	544	GET /wireshark-labs/protected_pages/HTTP-wireshar...
1700	20:57:21.847670	128.119.245.12	192.168.1.125	HTTP	585	HTTP/1.1 404 Not Found (text/html)
1703	20:57:22.838646	192.168.1.125	128.119.245.12	HTTP	431	GET /favicon.ico HTTP/1.1
1704	20:57:22.929574	128.119.245.12	192.168.1.125	HTTP	540	HTTP/1.1 404 Not Found (text/html)

> Frame 1696: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface 0

> Ethernet II, Src: IntelCor\_84:1b:2e (60:57:18:84:1b:2e), Dst: Cisco-Li\_94:a4:05 (48:f8:b3:94:a4:05)

> Internet Protocol Version 4, Src: 192.168.1.125, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 64434, Dst Port: 80, Seq: 1, Ack: 1, Len: 490

▼ 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 d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 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

[\[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wiresharkfile5.html\]](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html)

[HTTP request 1/2]

[\[Response in frame: 1700\]](#)

[\[Next request in frame: 1703\]](#)

New Authorization Field

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

The initial response in packet 1631 is a 401 status code with the phrase: Unauthorized.

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

There is a new field labeled Authorization in the second request followed by an alphanumeric phrase in Base64 format.