

Group Number:

Name/Surname of Members: Yiğit Emir Işıkcı / Ahmet Eren Akbaş

Student Number of Members: 2200356028 / 21945757

HTTP

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

Both of the browser and the server running in HTTP version 1.1 .

http						
No.	Time	Source	Destination	Protocol	Length	Info
56	2.434783	10.225.141.248	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
58	2.577722	128.119.245.12	10.225.141.248	HTTP	540	HTTP/1.1 200 OK (text/html)

> Frame 56: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \	0000	02 e0 52 0a 97 e1 90 e8	68 2c 61 c7 08 00
> Ethernet II, Src: AzureWav_2c:61:c7 (90:e8:68:2c:61:c7), Dst: 02:e0:52:0a:97:e1 (02:e0:52:0a:97:e1)	0010	02 15 46 08 40 00 80 06	a4 7d 0a e1 8d f8
> Internet Protocol Version 4, Src: 10.225.141.248, Dst: 128.119.245.12	0020	f5 0c cf 25 00 50 cf 16	39 00 0f 8b 9c 34
> Transmission Control Protocol, Src Port: 53029, Dst Port: 80, Seq: 1, Ack: 1, Len: 493	0030	02 02 61 e8 00 00 47 45	54 20 2f 77 69 72
> Hypertext Transfer Protocol	0040	68 61 72 6b 2d 6c 61 62	73 2f 48 54 54 50
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n	0050	69 72 65 73 68 61 72 6b	2d 66 69 6c 65 31
Host: gaia.cs.umass.edu\r\n	0060	74 6d 6c 20 48 54 54 50	2f 31 2e 31 0d 0a
	0070	73 74 3a 20 67 61 69 61	2e 63 73 2e 75 6d

Figure 1

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

Our browser accepts Turkish and English.

http						
No.	Time	Source	Destination	Protocol	Length	Info
56	2.434783	10.225.141.248	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
58	2.577722	128.119.245.12	10.225.141.248	HTTP	540	HTTP/1.1 200 OK (text/html)

> Frame 56: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{780BFAF8-E96E-413A-BEDB-C81933D21BCE}, id 0	
> Ethernet II, Src: AzureWav_2c:61:c7 (90:e8:68:2c:61:c7), Dst: 02:e0:52:0a:97:e1 (02:e0:52:0a:97:e1)	
> Internet Protocol Version 4, Src: 10.225.141.248, Dst: 128.119.245.12	
> Transmission Control Protocol, Src Port: 53029, Dst Port: 80, Seq: 1, Ack: 1, Len: 493	
> 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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n	
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n	
Accept-Encoding: gzip, deflate\r\n	
Accept-Language: tr-TR;q=0.9,en-US;q=0.8,en;q=0.7\r\n	
\r\n	
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]	
[HTTP request 1/1]	
[Response in frame: 58]	

Figure 2

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

Our IP address is 10.225.141.248 and servers ip address is 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
56	2.434783	10.225.141.248	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
58	2.577722	128.119.245.12	10.225.141.248	HTTP	540	HTTP/1.1 200 OK (text/html)

Figure 3

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

The status code is 200 OK.

No.	Time	Source	Destination	Protocol	Length	Info
56	2.434783	10.225.141.248	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
58	2.577722	128.119.245.12	10.225.141.248	HTTP	540	HTTP/1.1 200 OK (text/html)

Figure 4

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

The HTML file lastly modified at Friday, 20 October 2023

No.	Time	Source	Destination	Protocol	Length	Info
56	2.434783	10.225.141.248	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
58	2.577722	128.119.245.12	10.225.141.248	HTTP	540	HTTP/1.1 200 OK (text/html)

> Frame 58: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{780BFAF8-E96E-413A-BEDB-C81933D21BCE}, id 0
> Ethernet II, Src: BrocadeC_43:0d:00 (cc:4e:24:43:0d:00), Dst: AzureWav_2c:61:c7 (90:e8:68:2c:61:c7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.225.141.248
> Transmission Control Protocol, Src Port: 80, Dst Port: 53029, Seq: 1, Ack: 494, Len: 486
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
> Date: Fri, 20 Oct 2023 13:20:00 GMT\r\n
> Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
> Last-Modified: Fri, 20 Oct 2023 05:59:02 GMT\r\n
> ETag: "80-6081f91bbe297"\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 1/1]
> [Time since request: 0.142939000 seconds]
> [Request in frame: 56]
> Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
> File Data: 128 bytes
> Line-based text data: text/html (4 lines)

Figure 5

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

128 bytes of content being returned.

http						
No.	Time	Source	Destination	Protocol	Length	Info
56	2.434783	10.225.141.248	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
58	2.577722	128.119.245.12	10.225.141.248	HTTP	540	HTTP/1.1 200 OK (text/html)

> Frame 58: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{780BFAF8-E96E-413A-8EDB-C81933D21BCE}, id 0

> Ethernet II, Src: BrocadeC_43:0d:00 (cc:4e:24:43:0d:00), Dst: AzureWav_2c:61:c7 (90:e8:68:2c:61:c7)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.225.141.248

> Transmission Control Protocol, Src Port: 80, Dst Port: 53029, Seq: 1, Ack: 494, Len: 486

> **Hypertext Transfer Protocol**

> HTTP/1.1 200 OK\r\n

Date: Fri, 20 Oct 2023 13:20:00 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Fri, 20 Oct 2023 05:59:02 GMT\r\n

ETag: "80-6081f91bbe297"\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 1/1]

[Time since request: 0.142939000 seconds]

[Request in frame: 56]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

File Data: 128 bytes

> Line-based text data: text/html (4 lines)

Figure 6

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.

No, all headers in raw data listed in packet content window too.

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?

There is no an “IF-MODIFIED-SINCE” line in first GET request.

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

Yes, server returned the contents of the file at the first response.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows four packets: a GET request (No. 41), a 200 OK response (No. 43), and two subsequent GET requests (Nos. 95 and 98). The details pane for packet 43 is expanded, showing the HTTP response structure. The status line is '200 OK (text/html)'. The response headers include Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length (371), Keep-Alive, Connection, and Content-Type (text/html; charset=UTF-8). The response body is shown as 'Line-based text data: text/html (10 lines)' and contains HTML content with a congratulatory message and information about file modification dates.

No.	Time	Source	Destination	Protocol	Length	Info
41	3.458218	10.225.141.248	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	3.601324	128.119.245.12	10.225.141.248	HTTP	784	HTTP/1.1 200 OK (text/html)
95	10.575376	10.225.141.248	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
98	10.718682	128.119.245.12	10.225.141.248	HTTP	294	HTTP/1.1 304 Not Modified

```
Date: Fri, 20 Oct 2023 13:51:37 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 20 Oct 2023 05:59:02 GMT\r\n
ETag: "173-6081f91bbdac7"\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 1/1]
[Time since request: 0.143106000 seconds]
[Request in frame: 41]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\r\n
This file's last modification date will not change. <p>\r\n
Thus if you download this multiple times on your browser, a complete copy <br>\r\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
\r\n
</html>\r\n
```

Figure 7

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?

Yes, there is a line named “If-Modified-Since” at second GET request. The information after this line indicates our last accessed date to website.

http						
No.	Time	Source	Destination	Protocol	Length	Info
41	3.458218	10.225.141.248	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	3.601324	128.119.245.12	10.225.141.248	HTTP	784	HTTP/1.1 200 OK (text/html)
95	10.575376	10.225.141.248	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
98	10.718682	128.119.245.12	10.225.141.248	HTTP	294	HTTP/1.1 304 Not Modified


```

> Ethernet II, Src: AzureWav_2c:61:c7 (90:e8:68:2c:61:c7), Dst: 02:e0:52:0a:97:e1 (02:e0:52:0a:97:e1)
> Internet Protocol Version 4, Src: 10.225.141.248, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53269, Dst Port: 80, Seq: 1, Ack: 1, Len: 584
< Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    < [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
      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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: tr-TR,tr;q=0.9\r\n
      If-None-Match: "173-6081f91bbdac7"\r\n
      If-Modified-Since: Fri, 20 Oct 2023 05:59:02 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: 98]
  
```

Figure 8

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.

HTTP Status 304: Not Modified

The server didn't send new content because the browser used cached data. If the file changed, it would've served the new one, but it just said, "Get the old cached file"

http						
No.	Time	Source	Destination	Protocol	Length	Info
41	3.458218	10.225.141.248	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	3.601324	128.119.245.12	10.225.141.248	HTTP	784	HTTP/1.1 200 OK (text/html)
95	10.575376	10.225.141.248	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
98	10.718682	128.119.245.12	10.225.141.248	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 98: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{780BFAF8-E96E-413A-BED8-C81933D218CE}	
> Ethernet II, Src: BrocadeC_43:0d:00 (cc:4e:24:43:0d:00), Dst: AzureWav_2c:61:c7 (90:e8:68:2c:61:c7)	
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.225.141.248	
> Transmission Control Protocol, Src Port: 80, Dst Port: 53269, Seq: 1, Ack: 585, Len: 240	
~ Hypertext Transfer Protocol	
~ HTTP/1.1 304 Not Modified\r\n	
~ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]	
[HTTP/1.1 304 Not Modified\r\n]	
[Severity level: Chat]	
[Group: Sequence]	
Response Version: HTTP/1.1	
Status Code: 304	
[Status Code Description: Not Modified]	
Response Phrase: Not Modified	
Date: Fri, 20 Oct 2023 13:51:44 GMT\r\n	
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n	
Connection: Keep-Alive\r\n	
Keep-Alive: timeout=5, max=100\r\n	
ETag: "173-6081f91bbdac7"\r\n	
\r\n	
[HTTP response 1/1]	
[Time since request: 0.143306000 seconds]	
[Request in frame: 95]	
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]	

Figure 9

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?

HTTP GET request messages are sent 2 times. Packet number that contains GET message for the Bill or Rights is 8.

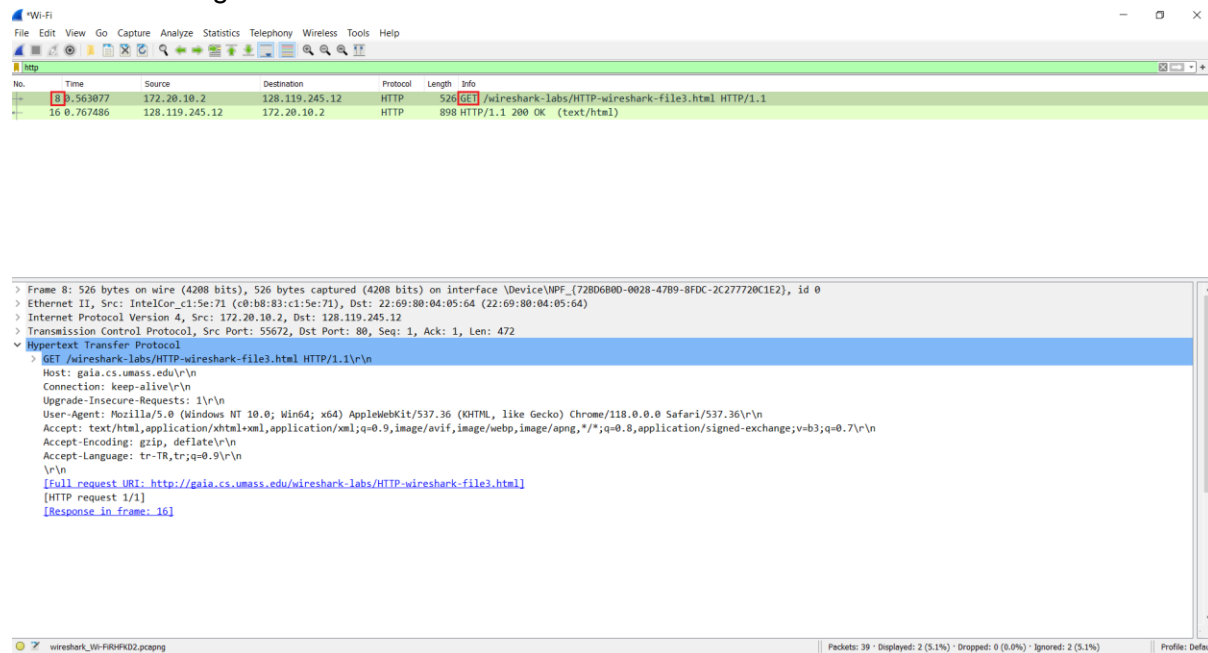


Figure 10

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

The packet that contains the status code and phrase associated with the response to the HTTP GET Request is 16.

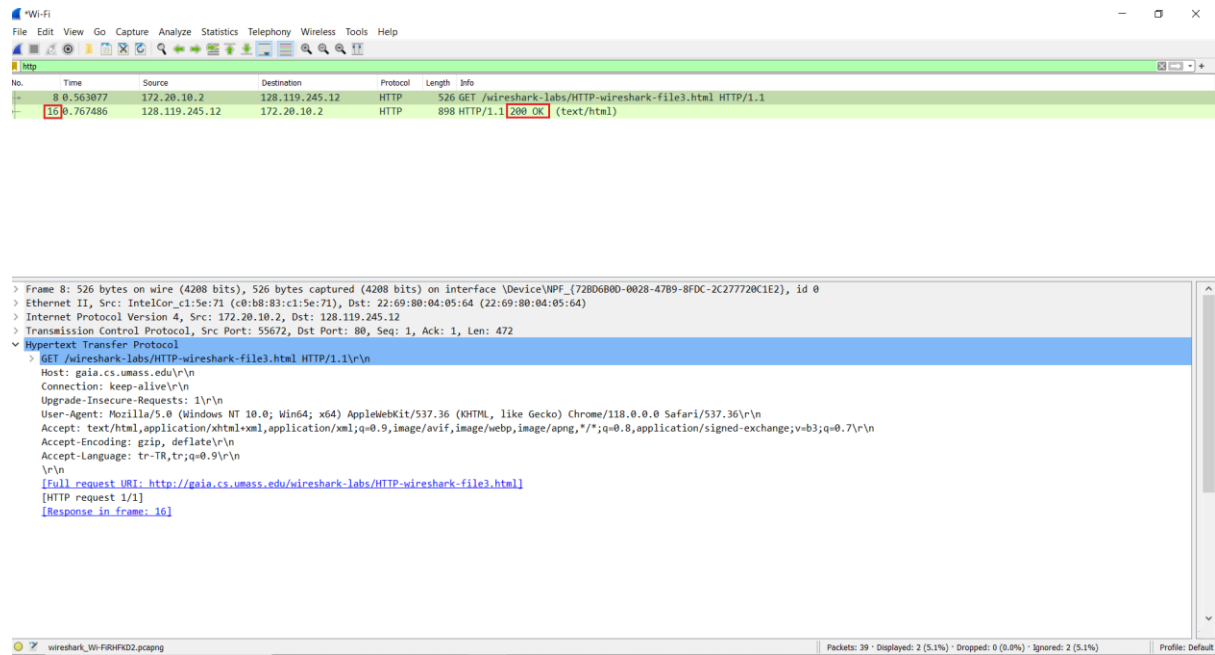


Figure 11

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

HTTP 200: OK

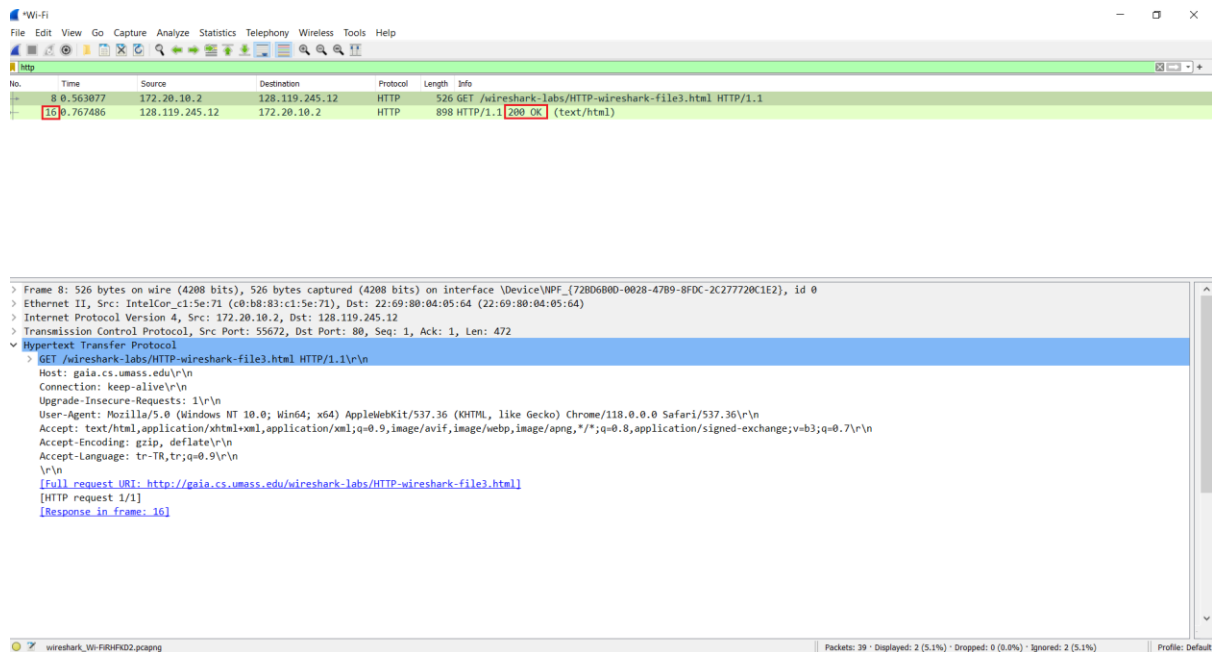


Figure 12

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

4 TCP Segments are needed for the response.

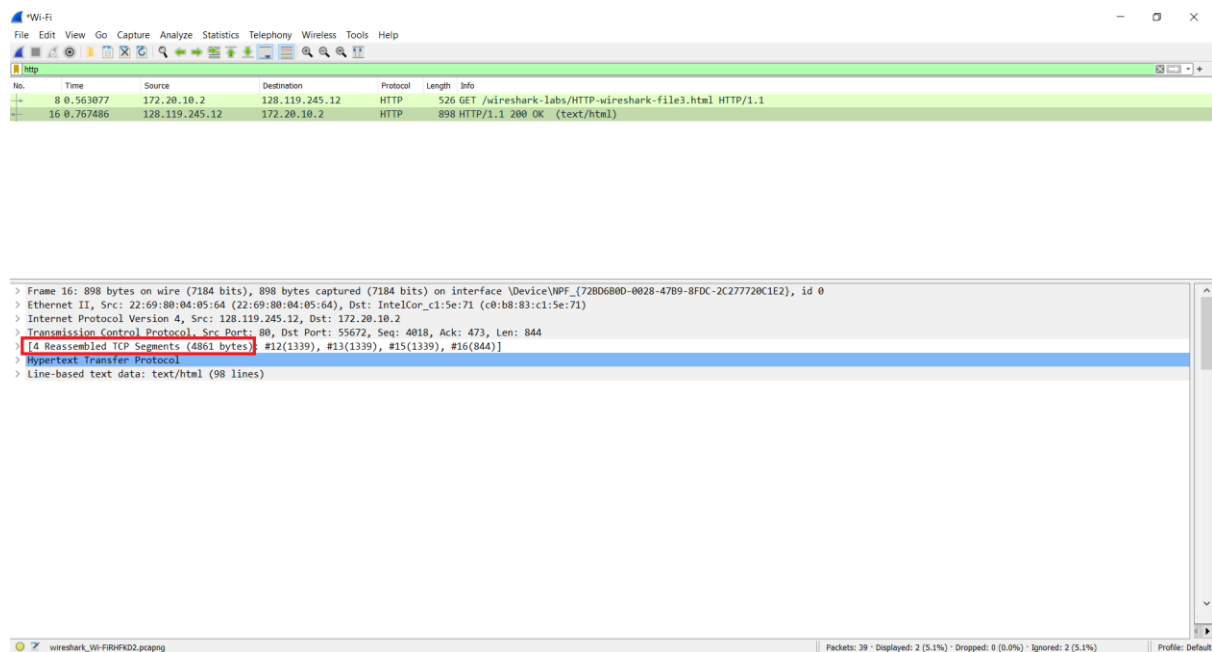


Figure 13

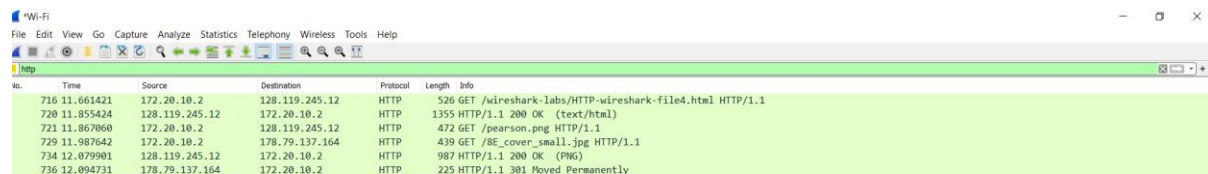
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

The browser sent 3 HTTP GET requests.

First address: 128.119.245.13 to get the content of the page (html)
“http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html”

Second Address: 129.119.245.12 to get the Pearson logo
“http://gaia.cs.umass.edu/pearson.png”

Third Address: 178.79.137.164 to get the book cover image.
“http://kurose.cslash.net/8E_cover_small.jpg”

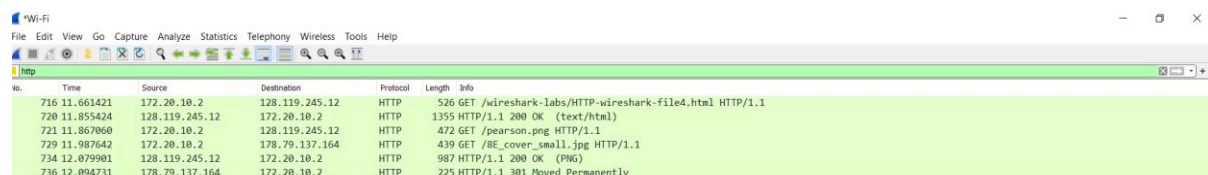


A screenshot of the Wireshark network protocol analyzer. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The first three packets are HTTP GET requests. The first packet is from 172.20.10.2 to 128.119.245.12, requesting /wireshark-labs/HTTP-wireshark-file4.html. The second packet is from 172.20.10.2 to 128.119.245.12, requesting /pearson.png. The third packet is from 172.20.10.2 to 178.79.137.164, requesting /8E_cover_small.jpg. The fourth packet is an HTTP 200 OK response from 178.79.137.164 to 172.20.10.2. The fifth packet is an HTTP 301 Moved Permanently response from 178.79.137.164 to 172.20.10.2.

No.	Time	Source	Destination	Protocol	Length	Info
716	11.661421	172.20.10.2	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
720	11.855424	128.119.245.12	172.20.10.2	HTTP	1355	HTTP/1.1 200 OK (text/html)
721	11.867060	172.20.10.2	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
729	11.987642	172.20.10.2	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
734	12.079901	128.119.245.12	172.20.10.2	HTTP	987	HTTP/1.1 200 OK (PNG)
736	12.094731	178.79.137.164	172.20.10.2	HTTP	225	HTTP/1.1 301 Moved Permanently

Figure 14

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.



A screenshot of the Wireshark network protocol analyzer. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The first three packets are HTTP GET requests. The first packet is from 172.20.10.2 to 128.119.245.12, requesting /wireshark-labs/HTTP-wireshark-file4.html. The second packet is from 172.20.10.2 to 128.119.245.12, requesting /pearson.png. The third packet is from 172.20.10.2 to 178.79.137.164, requesting /8E_cover_small.jpg. The fourth packet is an HTTP 200 OK response from 178.79.137.164 to 172.20.10.2. The fifth packet is an HTTP 301 Moved Permanently response from 178.79.137.164 to 172.20.10.2.

No.	Time	Source	Destination	Protocol	Length	Info
716	11.661421	172.20.10.2	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
720	11.855424	128.119.245.12	172.20.10.2	HTTP	1355	HTTP/1.1 200 OK (text/html)
721	11.867060	172.20.10.2	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
729	11.987642	172.20.10.2	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
734	12.079901	128.119.245.12	172.20.10.2	HTTP	987	HTTP/1.1 200 OK (PNG)
736	12.094731	178.79.137.164	172.20.10.2	HTTP	225	HTTP/1.1 301 Moved Permanently

Figure 15

They were downloaded **in parallel** because the browser doesn't wait for the first image's response, it makes a request for other image before getting the first.

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

HTTP 401: Unauthorized

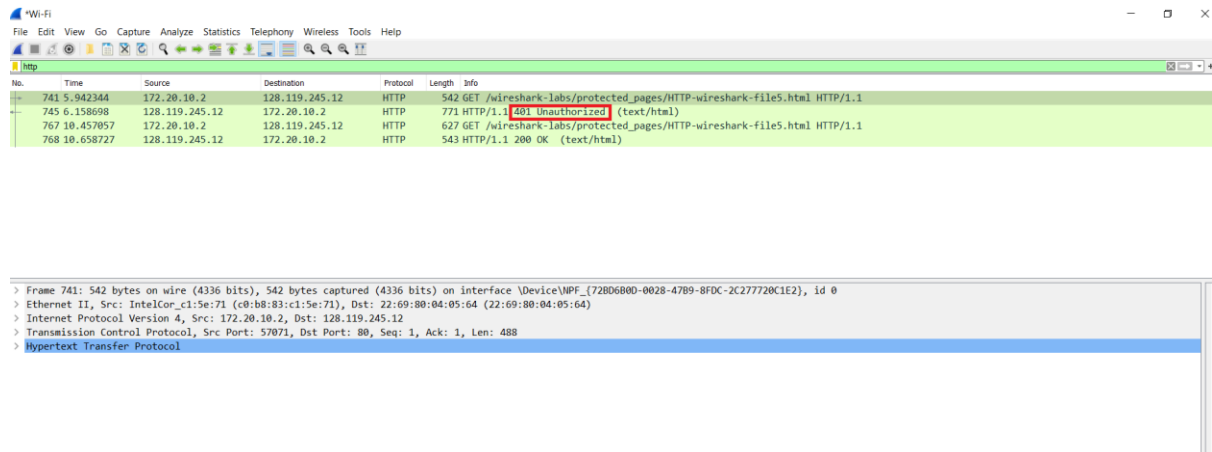


Figure 16

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

Authorization field is included for the second request.

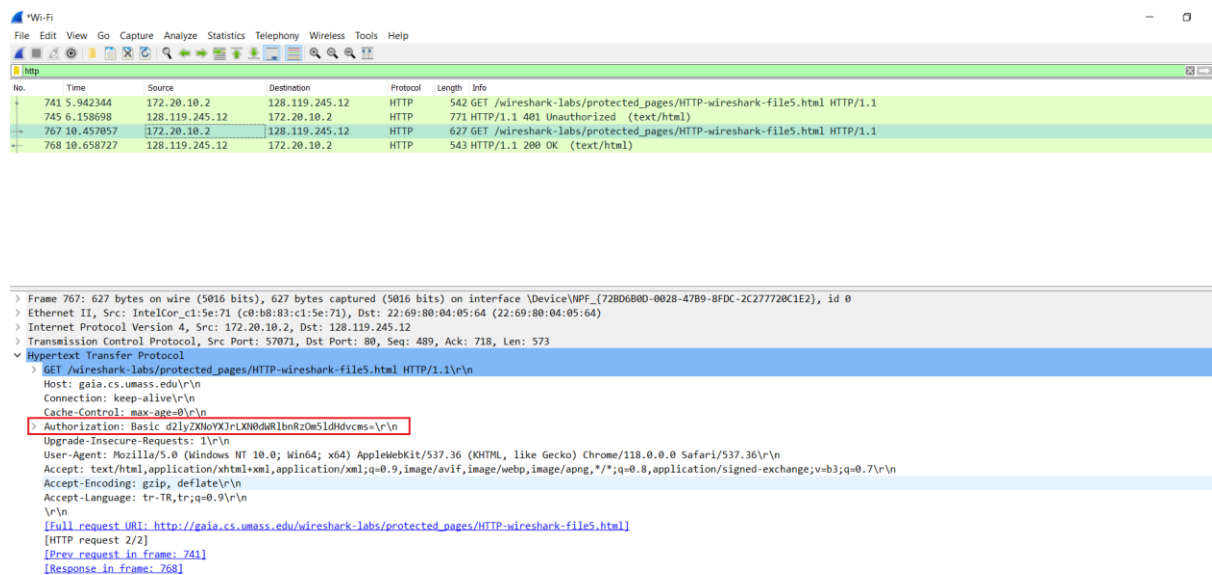


Figure 17