

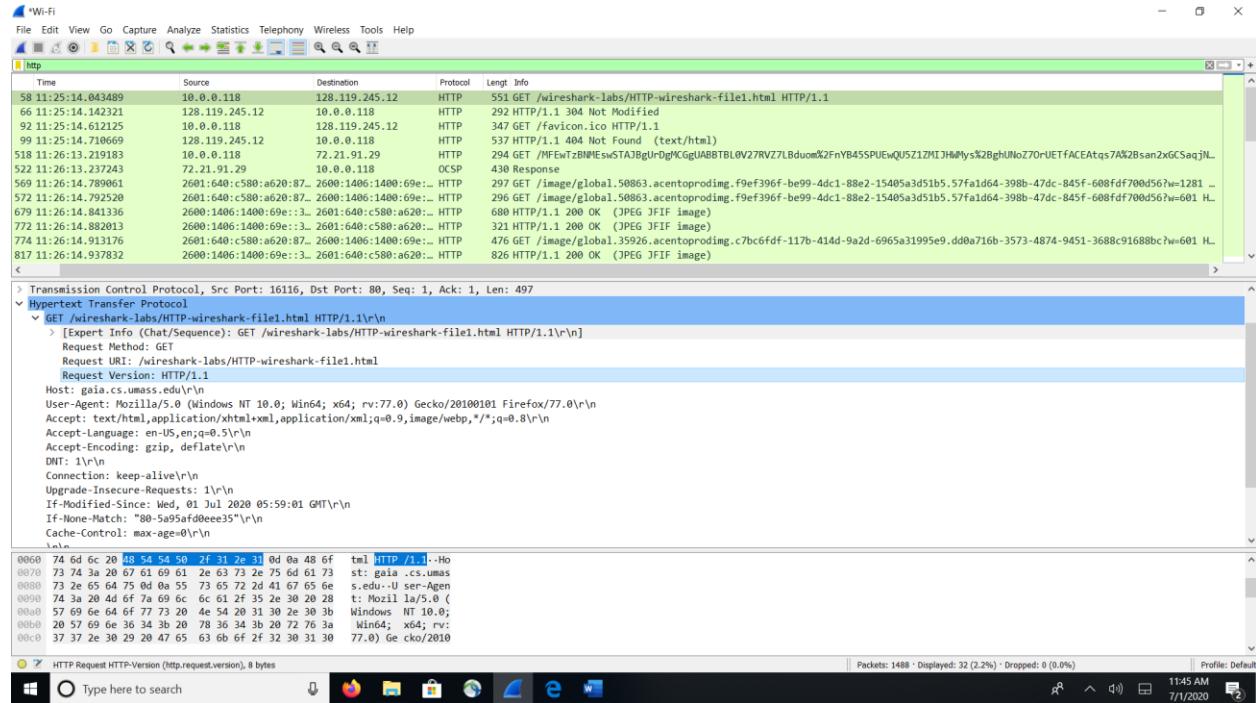
Justin Phillips

cs372 summer2020

lab2

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

Both browser and server are running 1.1



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

the accepted language is en-US

The figure shows a screenshot of the Wireshark application window. The title bar reads "Wi-Fi File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help". The main pane displays a list of network packets. The first few packets are highlighted in green, indicating they are selected. The columns in the packet list are: Time, Source, Destination, Protocol, Length, and Info. The "Info" column contains detailed descriptions of each packet's content, such as "GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1". A vertical scroll bar is visible on the right side of the main pane. Below the main pane, there is a status bar with the text "HTTP Accept Language (http.accept_language), 33 bytes". At the bottom of the screen, the Windows taskbar is visible with icons for File Explorer, Edge browser, and other system tools.

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

ip of my pc is 10.0.0.118 and the server is 128.119.245.12

Wi-Fi File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

http

Time	Source	Destination	Protocol	Length	Info
58 11:25:14.043489	10.0.0.118	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
66 11:25:14.142321	128.119.245.12	10.0.0.118	HTTP	292	HTTP/1.1 304 Not Modified
92 11:25:14.612125	10.0.0.118	128.119.245.12	HTTP	347	GET /favicon.ico HTTP/1.1
99 11:25:14.710669	128.119.245.12	10.0.0.118	HTTP	537	HTTP/1.1 404 Not Found (text/html)
518 11:26:13.219183	10.0.0.118	72.21.91.29	HTTP	299	GET /MFeWzBhMEswSTAjBgUrDgICGigUABTBLOvZ7RvZ7Lbduomk2FnYB45SPUEwQUSZ1ZHJHMy5%2BgHUNoZ7OrUETfACEAtqs7A%2Bsan2x6CsaqjNL
522 11:26:13.237243	72.21.91.29	10.0.0.118	OSCP	430	Response
569 11:26:14.789061	2601:640:c580:a620:87..	2600:1406:1400:69e:..	HTTP	297	GET /image/global_50863.acentropodimg.f9ef396f-be99-acd1-88e2-15405a3d51b5..57fa1d64-398b-47dc-845f-608fd700d56?w=1281 ..
572 11:26:14.792520	2601:640:c580:a620:87..	2600:1406:1400:69e:..	HTTP	299	GET /image/global_50863.acentropodimg.f9ef396f-be99-acd1-88e2-15405a3d51b5..57fa1d64-398b-47dc-845f-608fd700d56?w=601 ..
679 11:26:14.841336	2600:1406:1400:69e:..	2601:640:c580:a620:..	HTTP	688	HTTP/1.1 200 OK (JPEG/JFIF image)
772 11:26:14.882013	2600:1406:1400:69e:..	2601:640:c580:a620:..	HTTP	321	HTTP/1.1 200 OK (JPEG/JFIF image)
774 11:26:14.913176	2601:640:c580:a620:87..	2600:1406:1400:69e:..	HTTP	476	GET /image/global_35926.acentropodimg.c7bc6fdf-117b-414d-9a2d-6965a31995e.9dd0a716b-3573-4874-9451-3688c91688bc?w=601 ..
817 11:26:14.937832	2600:1406:1400:69e:..	2601:640:c580:a620:..	HTTP	826	HTTP/1.1 200 OK (JPEG/JFIF image)

< http://www.wireshark.org/doc/whatis/wireshark.html>

> Frame 58: 551 bytes on wire (4408 bits), 551 bytes captured on interface \Device\NP_{9FB3850A-CC7B-4B6E-8776-C7A0C6A2CFCA}, id 0

> Ethernet II, Src: Intel Cor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)

> Internet Protocol Version 4, Src: 10.0.0.118, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 16116, Dst Port: 80, Seq: 1, Ack: 1, Len: 497

+ 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: gaias.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

DNT: 1\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

TCP Model: TCPv4-Model\r\n

00090 3c b7 4b e7 bb 82 e4 a7 09 2f 04 09 06 9c 06 < K . . . / . . .

0010 02 19 60 c9 40 00 40 06 58 1c 00 00 78 00 77 < R . . X . . . v .

0020 f5 02 3e 4f 00 50 f5 b8 e6 c4 0b b9 e6 8a 50 18 < P . . . P .

0030 02 01 31 88 00 07 47 45 54 20 2f 77 69 72 65 73 < . 1 . GE T /w ires

0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s /HTTP-w

0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h

0060 74 6d 6c 20 48 54 50 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1 - Ho

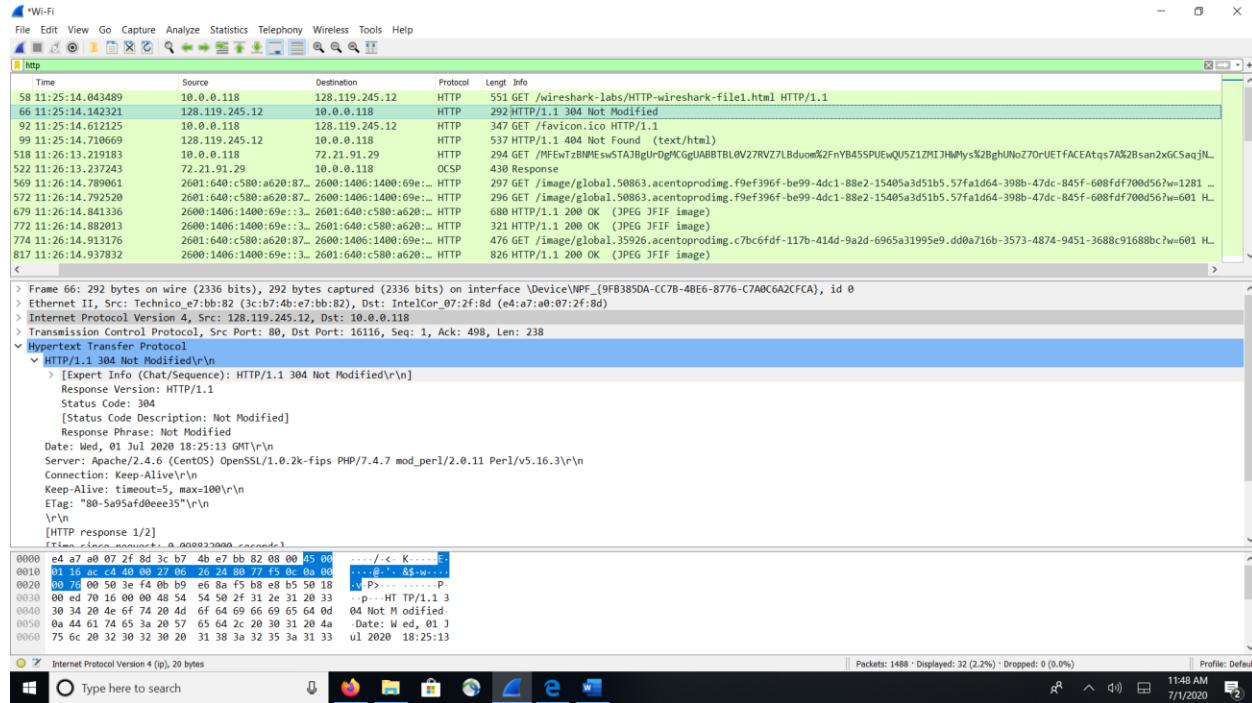
Internet Protocol Version 4 (ip), 20 bytes

Packets: 1488 · Displayed: 32 (2.2%) · Dropped: 0 (0.0%)

Type here to search

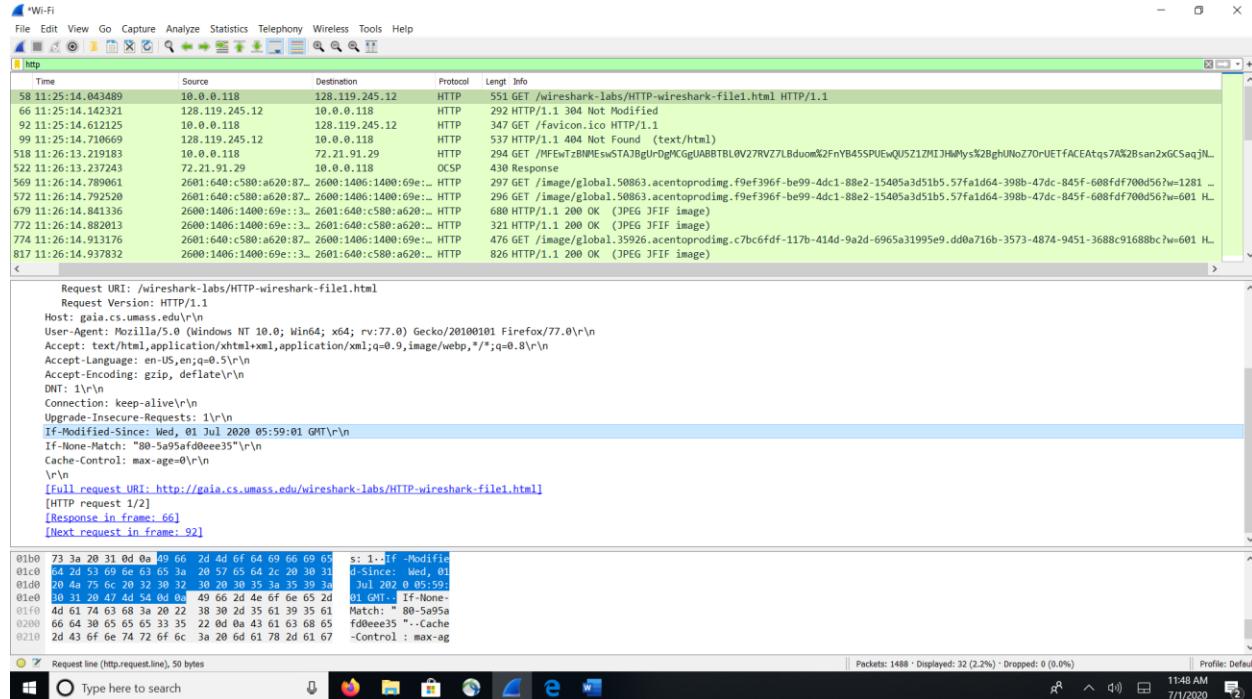
4. What is the status code returned from the server to your browser?

304 not modified



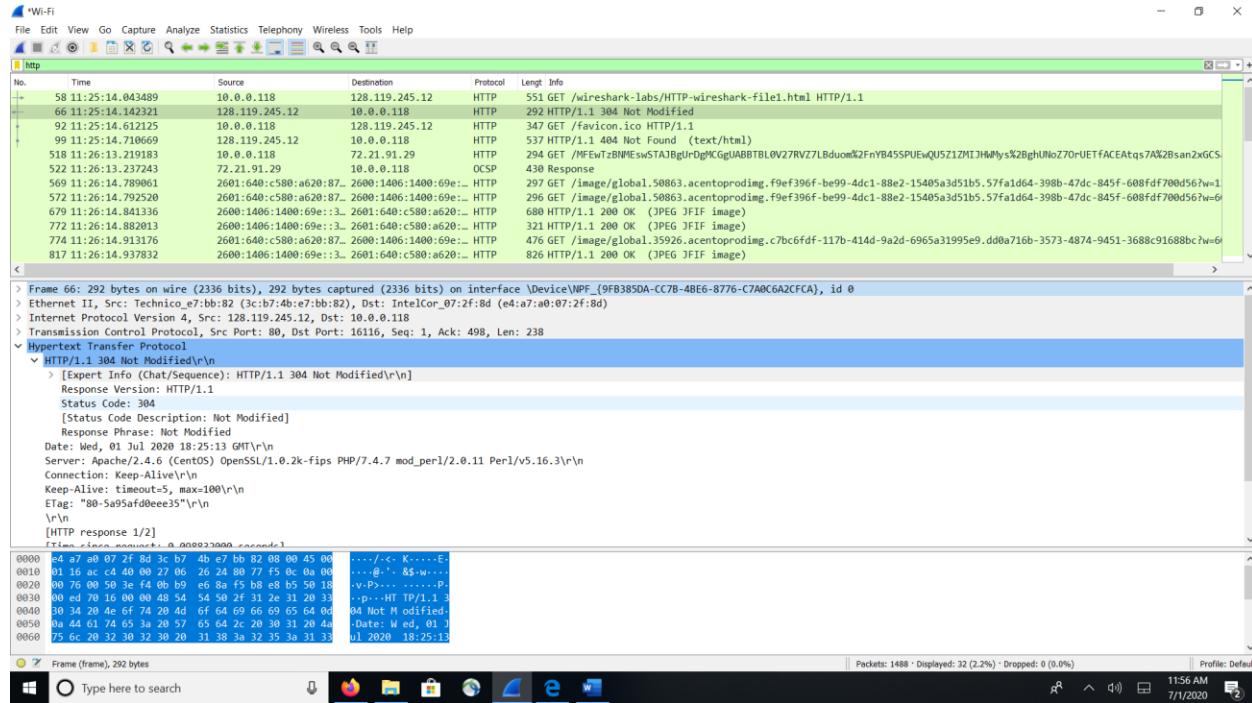
5. When was the HTML file that you are retrieving last modified at the server?

If-Modified-Since: Wed, 01 Jul 2020 05:59:01 GMT\r\n



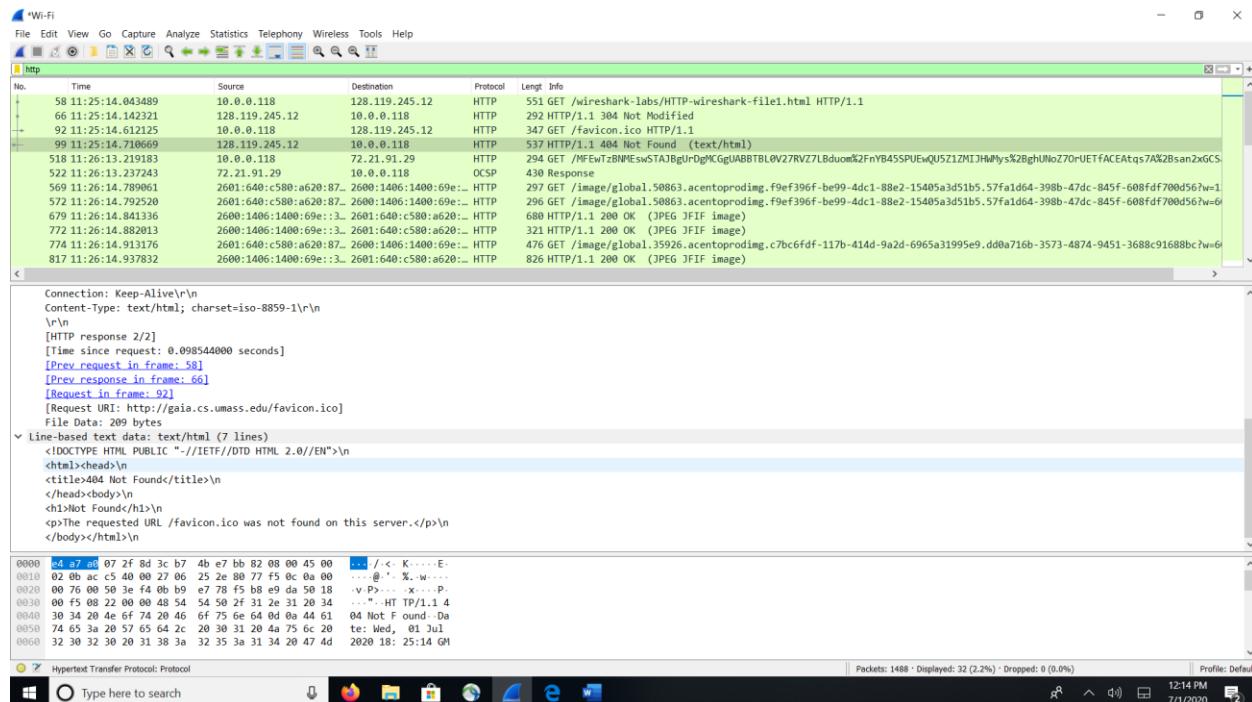
6. How many bytes of content are being returned to your browser?

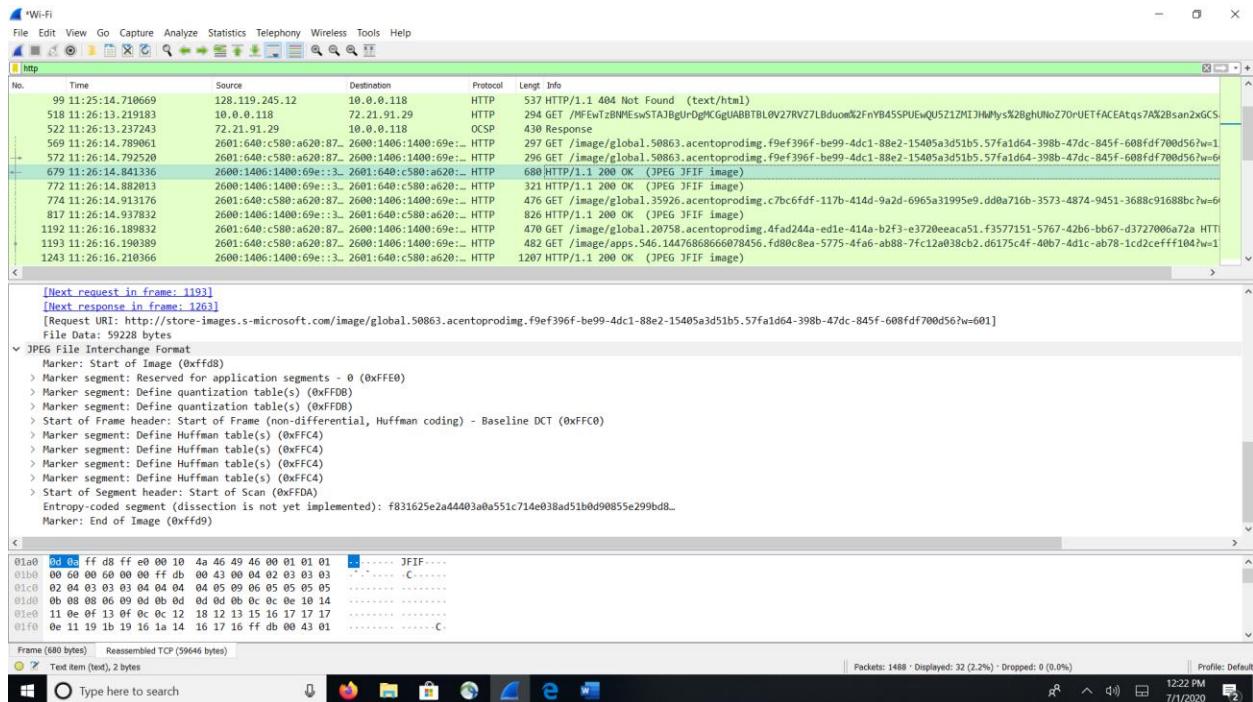
length is 292 bytes



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.

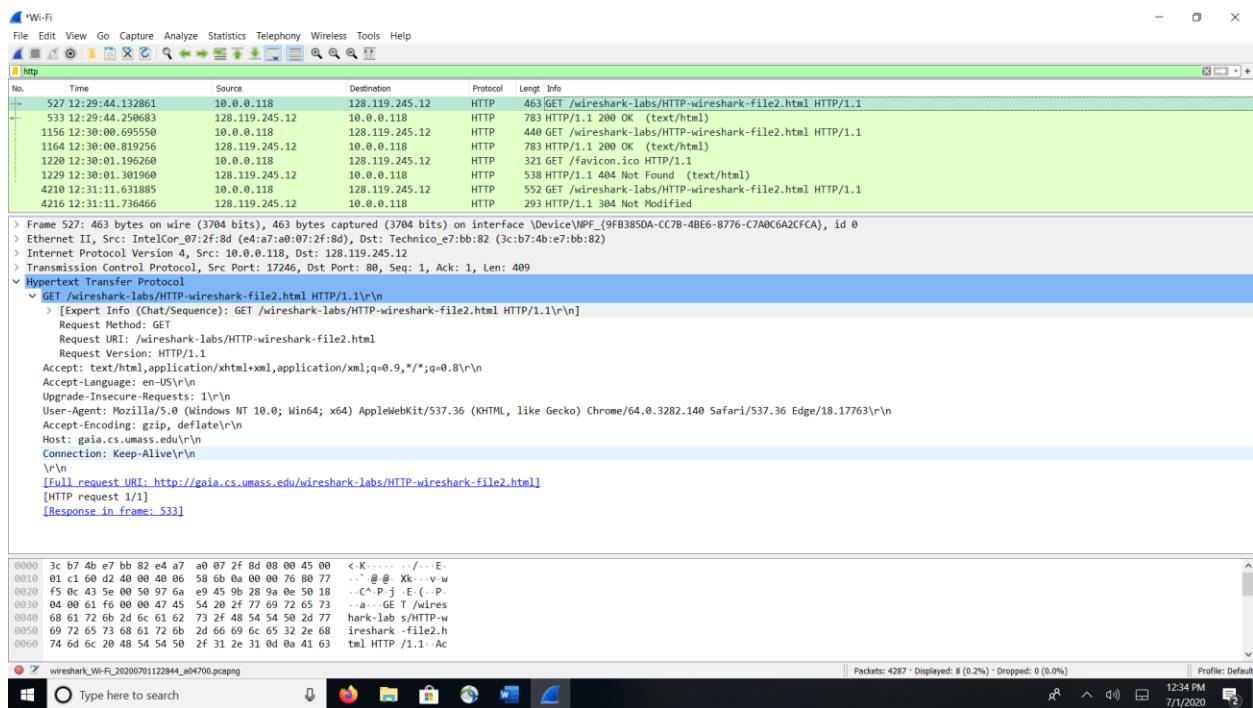
I received a bunch of request for images that I got 200 responses and and html that wasn't found





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 I don't see any if modified



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

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Http

No.	Time	Source	Destination	Protocol	Lengt	Info
527	12:29:44.132861	10.0.0.118	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
533	12:29:44.250683	128.119.245.12	10.0.0.118	HTTP	783	HTTP/1.1 200 OK (text/html)
1156	12:30:00.695550	10.0.0.118	128.119.245.12	HTTP	440	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1164	12:30:00.819256	128.119.245.12	10.0.0.118	HTTP	783	HTTP/1.1 200 OK (text/html)
1220	12:30:01.196260	10.0.0.118	128.119.245.12	HTTP	321	GET /favicon.ico HTTP/1.1
1229	12:30:01.301960	128.119.245.12	10.0.0.118	HTTP	538	HTTP/1.1 404 Not Found (text/html)
4210	12:31:11.631885	10.0.0.118	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4216	12:31:11.736466	128.119.245.12	10.0.0.118	HTTP	293	HTTP/1.1 304 Not Modified

```

Etag: "173-5a95af0d0ede95"\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: 0.117822000 seconds
[Request in frame: 527]
[Request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[File Data: 371 bytes]

▼ Line-based text data: text/html (10 lines)
\b
<html>\n
<head>\n
</head>\n
<body>\n
  Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
  This file's last modification date will not change. <br>\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.<br>\n
</body>\n
</html>\n

```

```

0100 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 0a 3c 68 78 et=UTF-8 ...<.cht
0101 6c 2e 0a 00 43 0f 0c 67 0d 61 74 73 6c 61 67 65 al><.con gratulat
0102 29 6f 6e 20 59 61 67 61 69 6e 21 20 4e 6f 77 ions, age in now
0103 20 70 64 75 27 76 65 20 64 6f 27 6e 6c 6f 61 66 you're download
0104 65 64 20 74 68 65 20 66 69 6c 65 20 6c 61 62 32 ed the file lab2
0105 2d 32 2e 68 74 6d 2e 20 3c 62 72 3e 0a 54 68 -2.html. <br>> Th
0106 69 73 20 66 69 6c 65 27 73 20 6c 61 73 74 20 6d is file's last m
0107 65 64 20 74 68 65 20 66 69 6c 65 20 6c 61 62 32 ed the file lab2
0108 2d 32 2e 68 74 6d 2e 20 3c 62 72 3e 0a 54 68 -2.html. <br>> Th
0109 69 73 20 66 69 6c 65 27 73 20 6c 61 73 74 20 6d is file's last m

```

Packets: 4287 · Displayed: 0 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

12:51 PM 7/1/2020

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?

still do not see an “IF-MODIFIED-SINCE:”

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Http

No.	Time	Source	Destination	Protocol	Lengt	Info
527	12:29:44.132861	10.0.0.118	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
533	12:29:44.250683	128.119.245.12	10.0.0.118	HTTP	783	HTTP/1.1 200 OK (text/html)
1156	12:30:00.695550	10.0.0.118	128.119.245.12	HTTP	440	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1164	12:30:00.819256	128.119.245.12	10.0.0.118	HTTP	783	HTTP/1.1 200 OK (text/html)
1220	12:30:01.196260	10.0.0.118	128.119.245.12	HTTP	321	GET /favicon.ico HTTP/1.1
1229	12:30:01.301960	128.119.245.12	10.0.0.118	HTTP	538	HTTP/1.1 404 Not Found (text/html)
4210	12:31:11.631885	10.0.0.118	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4216	12:31:11.736466	128.119.245.12	10.0.0.118	HTTP	293	HTTP/1.1 304 Not Modified

```

> Internet Protocol Version 4, Src: 10.0.0.118, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 17252, Dst Port: 80, Seq: 1, Ack: 1, Len: 386
▼ 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
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
        Accept-Language: en-US,en;q=0.5\r\n
        Accept-Encoding: gzip, deflate\r\n
        DNT: 1\r\n
        Connection: keep-alive\r\n
        Upgrade-Insecure-Requests: 1\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: 1164]

```

```

0000 3c b7 4b e7 b0 82 e4 a7 a0 07 2f 8d 08 00 45 00 < K..... /...E.
0010 01 aa 60 d8 40 00 40 06 58 7c 0a 00 00 76 80 70 ..@. X...v.w
0020 f5 0c 43 64 00 50 90 a2 bf f4 0e a1 53 02 50 18 ..Cd P...S.P.
0030 02 01 29 c7 00 00 47 45 54 20 2f 77 69 72 65 73 ..) GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 6b 61 72 6b 2d 66 6c 65 32 2e 68 ireshark -file2.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1-Ho

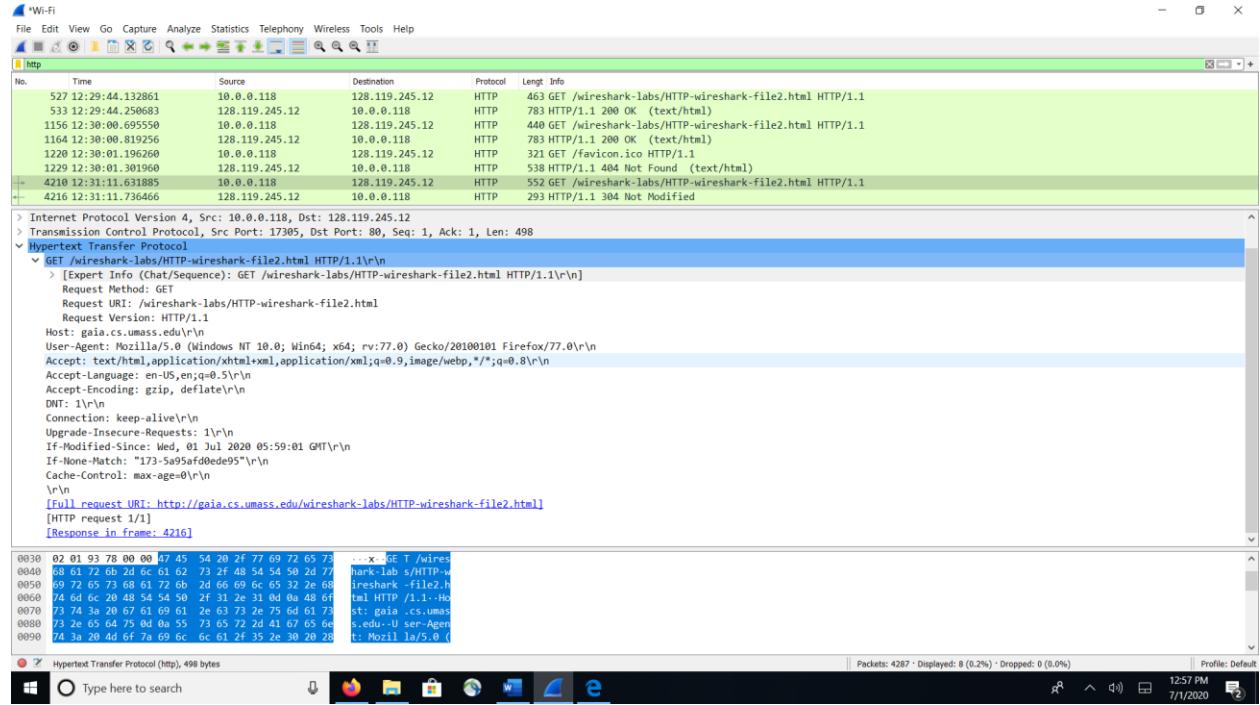
```

Packets: 4287 · Displayed: 0 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

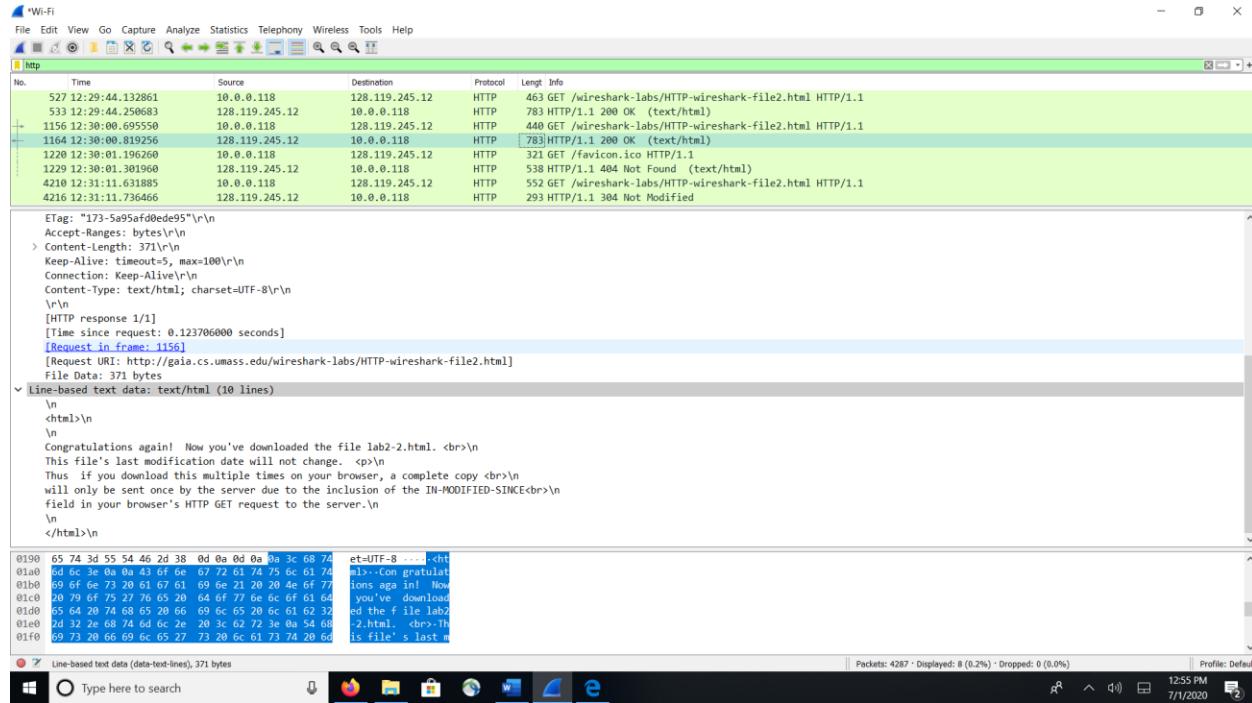
12:53 PM 7/1/2020

for some reason I did get the “IF-MODIFIED-SINCE:” on the 4th get request and the If-Modified-Since:
Wed, 01 Jul 2020 05:59:01 GMT\r\n

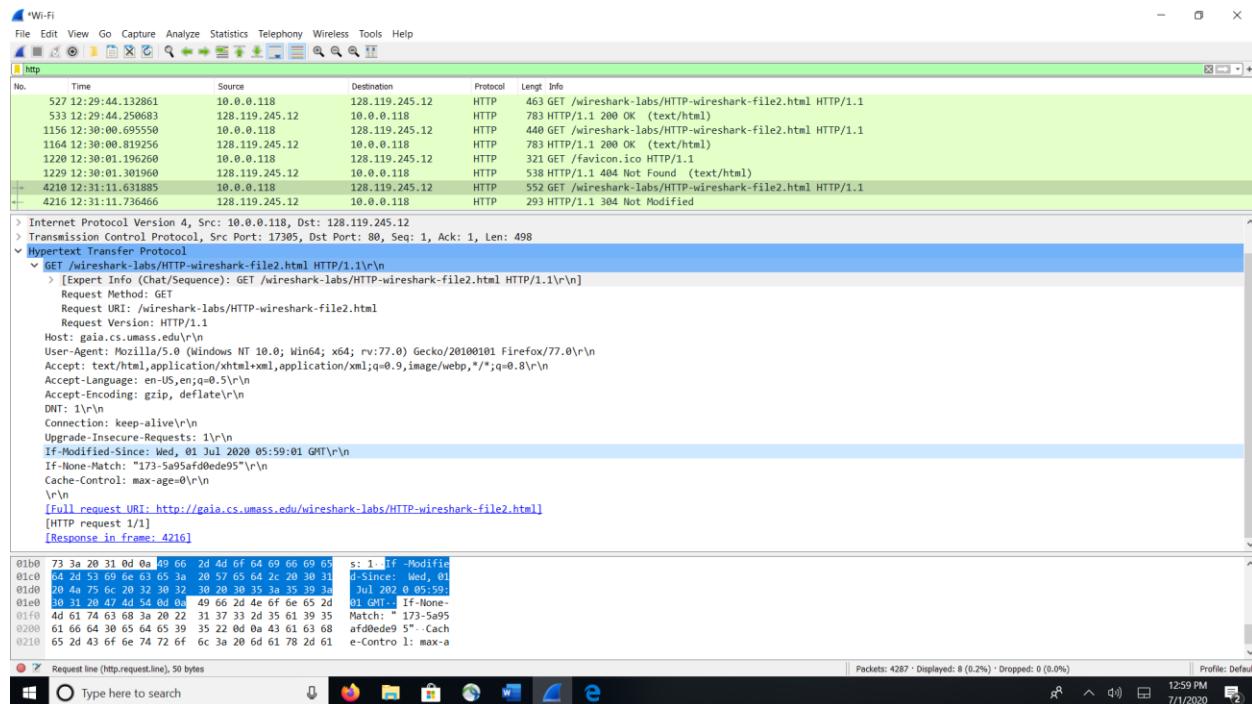


11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The code is a 200 and the response phrase is OK.

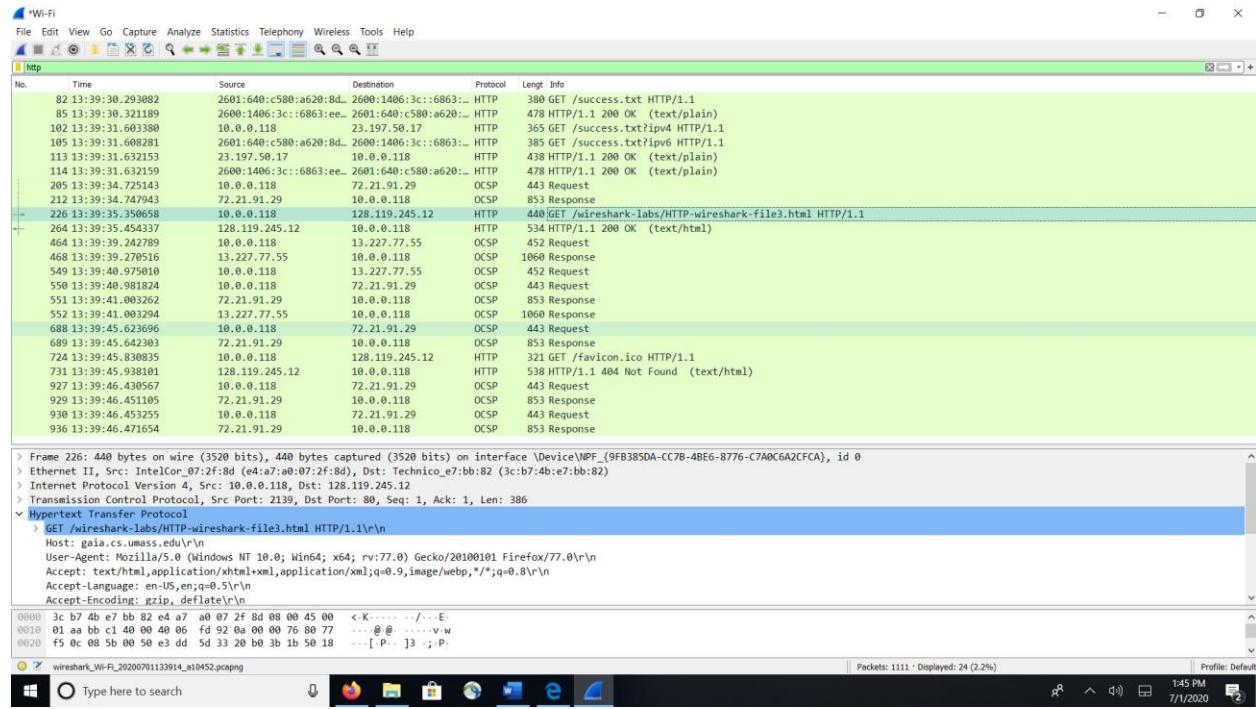


the fourth request was the 304 with a Response Phrase: Not Modified



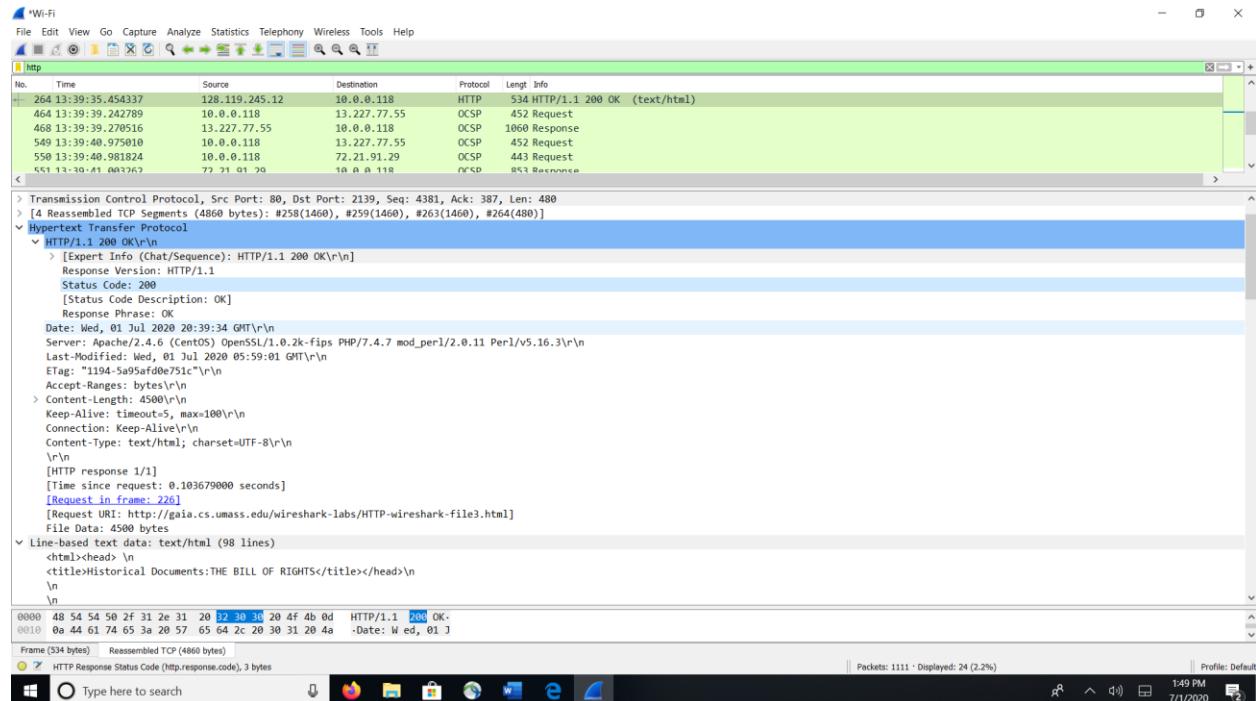
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

5 GET requests and 226 is the packet number with the Bill of Rights



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

264 is the packet number

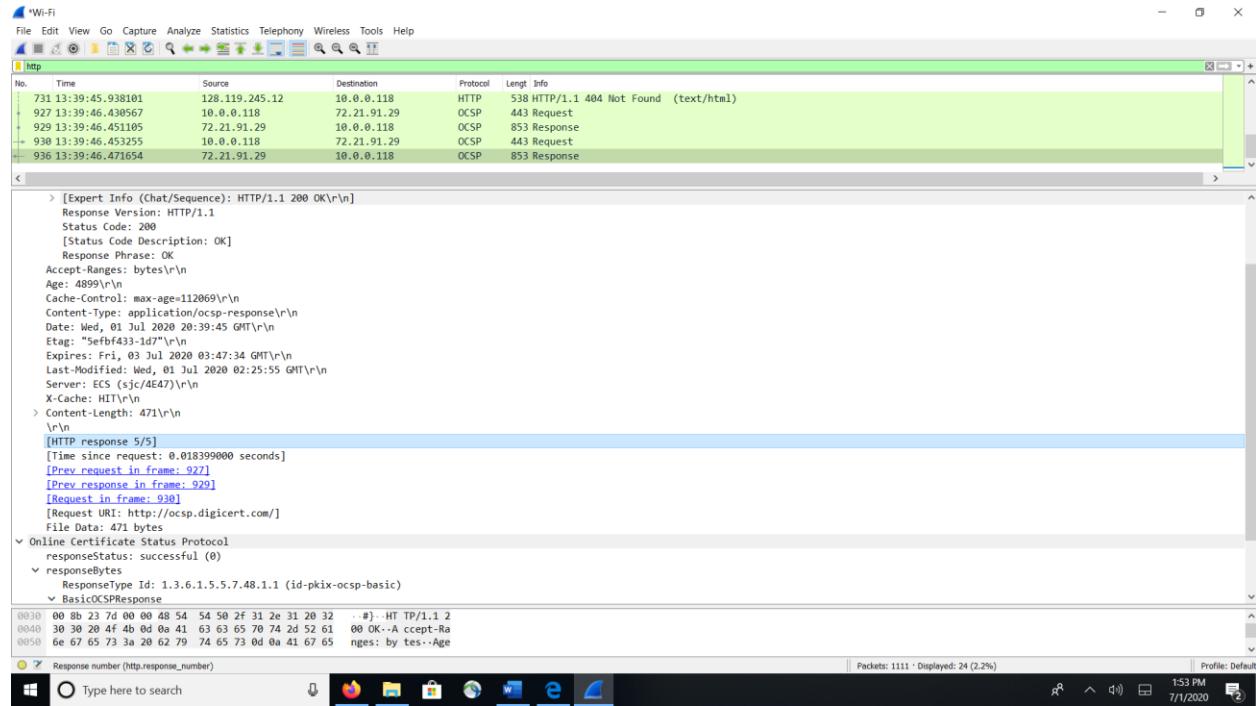


14. What is the status code and phrase in the response?

The code is 200 with a Response Phrase:OK

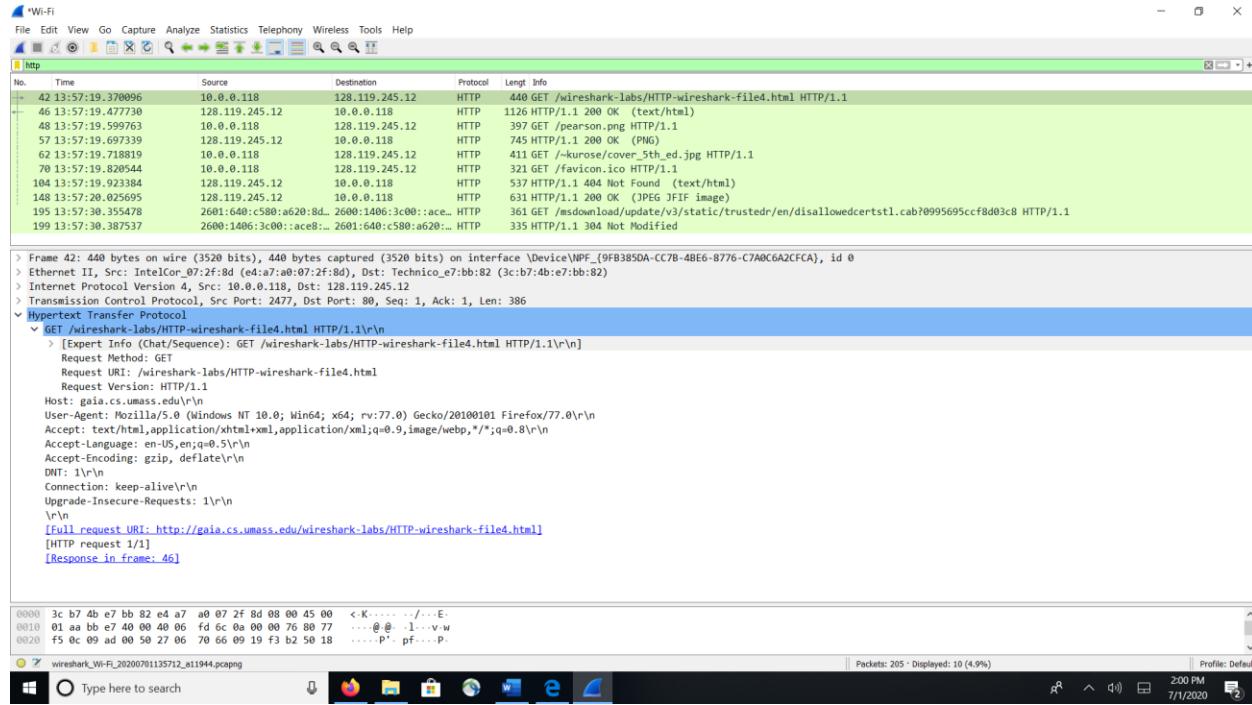
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

5 request/responses were send to get the complete Bill of Rights file



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

three Get request were made to [Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>]

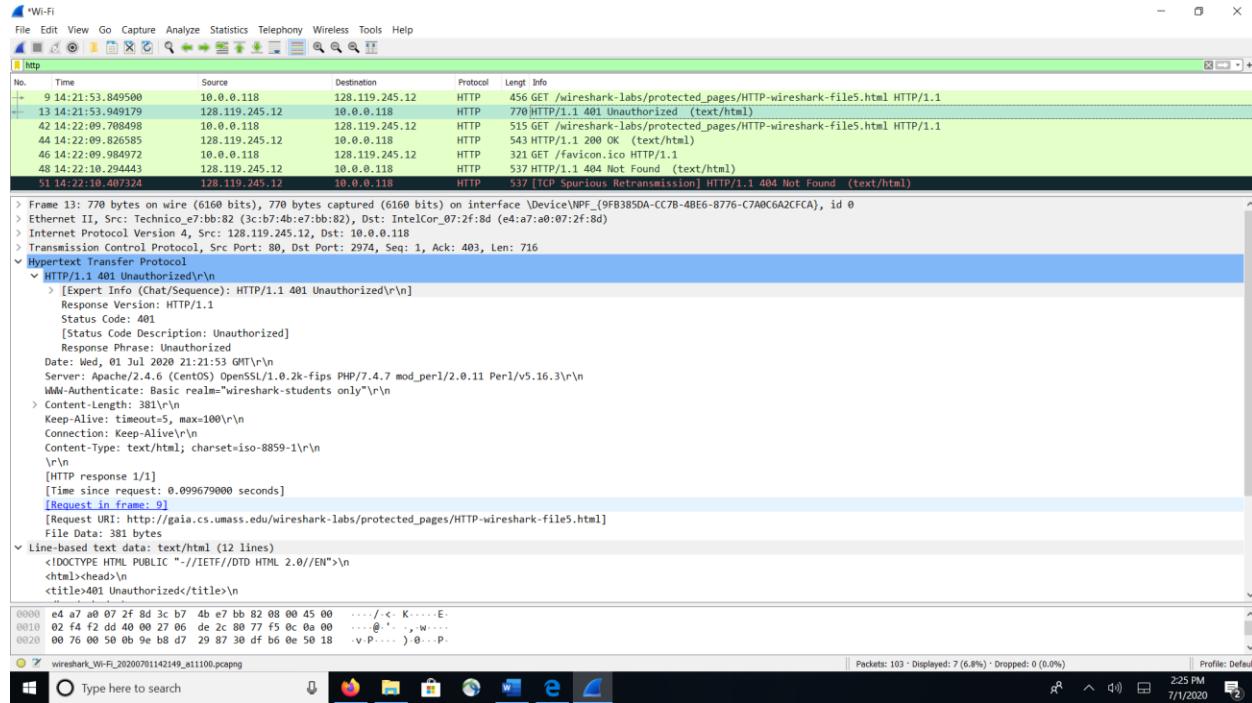


17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

I believe that my browser downloaded the images serially since the first one completed before the other one started.

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

The code and response for the GET request. Status Code: 401, Response 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?

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbzRzOm5ldHdvcms=\r\n

