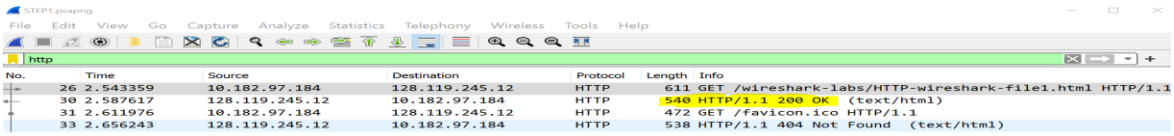
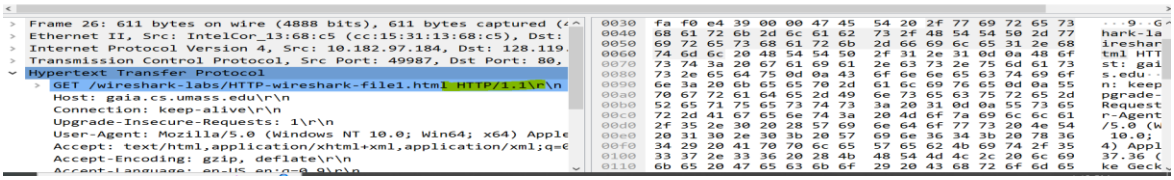
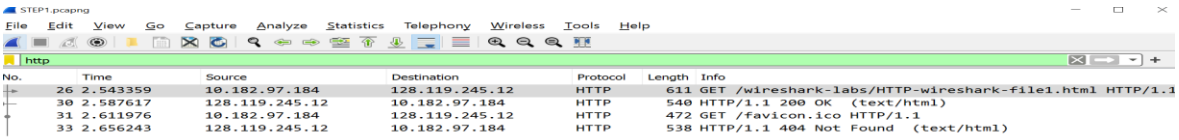
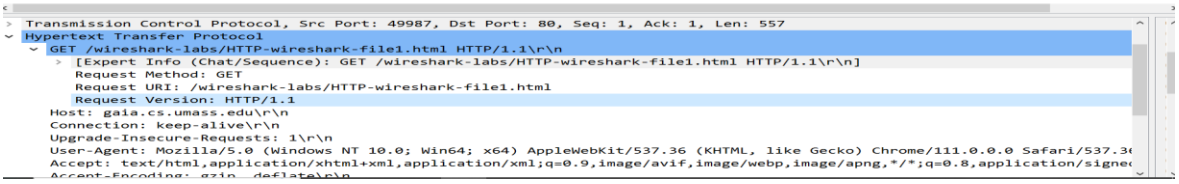
CSE4344/5344 – Project 2 (Spring 2023) Wireshark Lab: HTTP

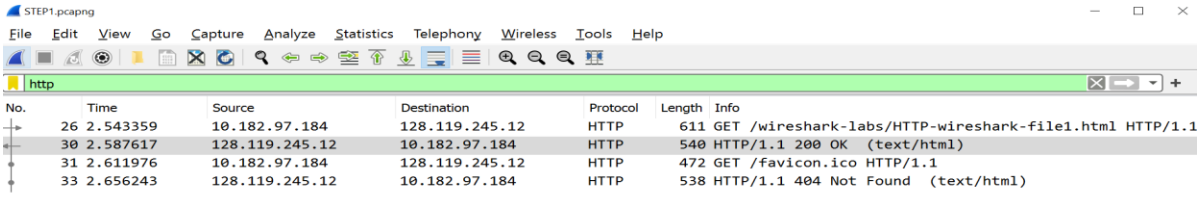
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

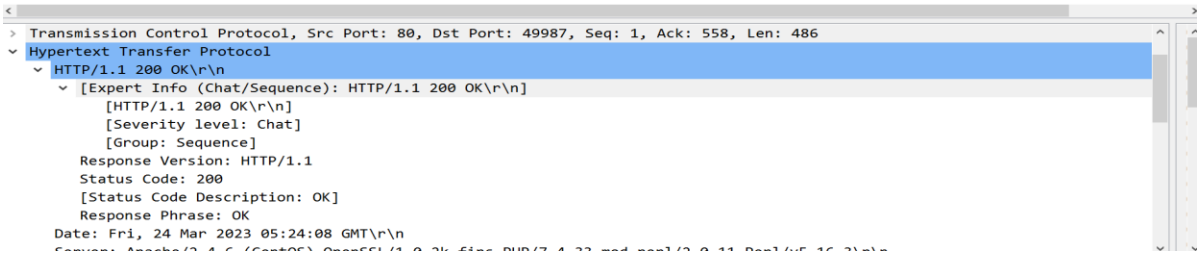






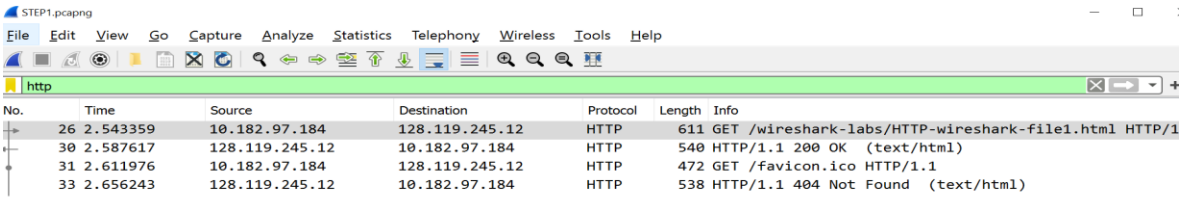


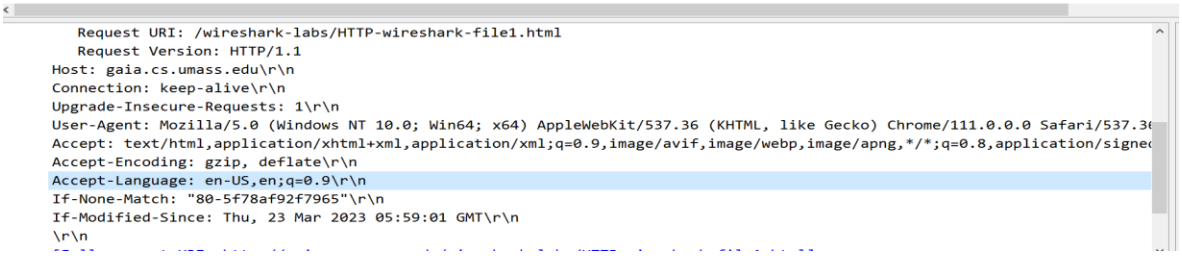




Browser and Server are running on HTML version 1.1

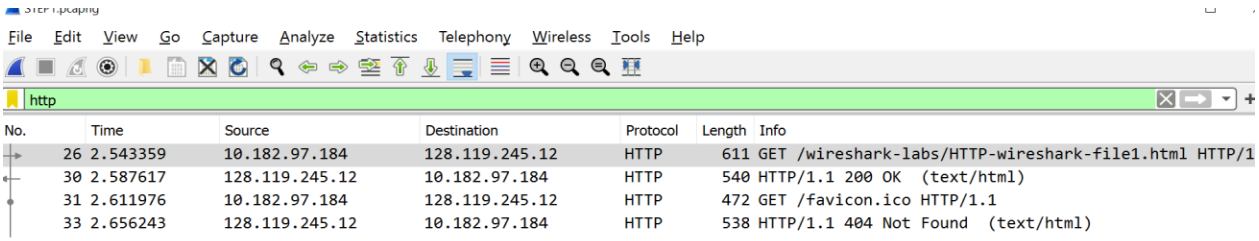
2. What languages (if any) does your browser indicate that it can accept to the server?

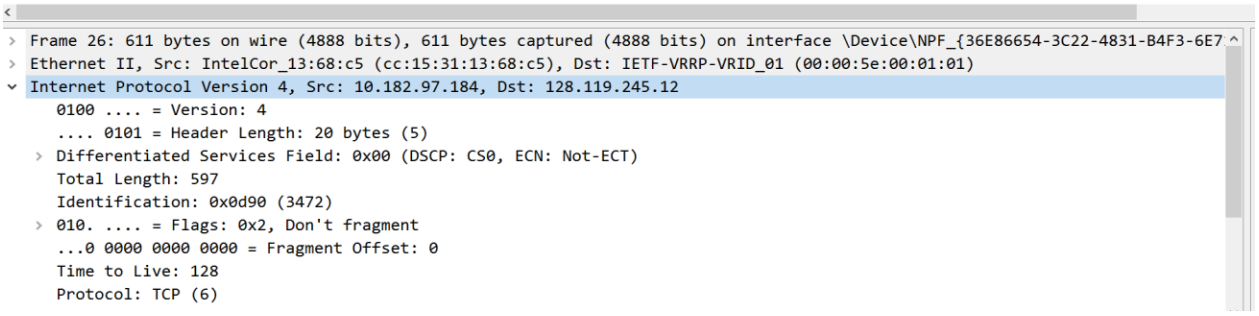




Accept language is listed in HTTP get message.

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

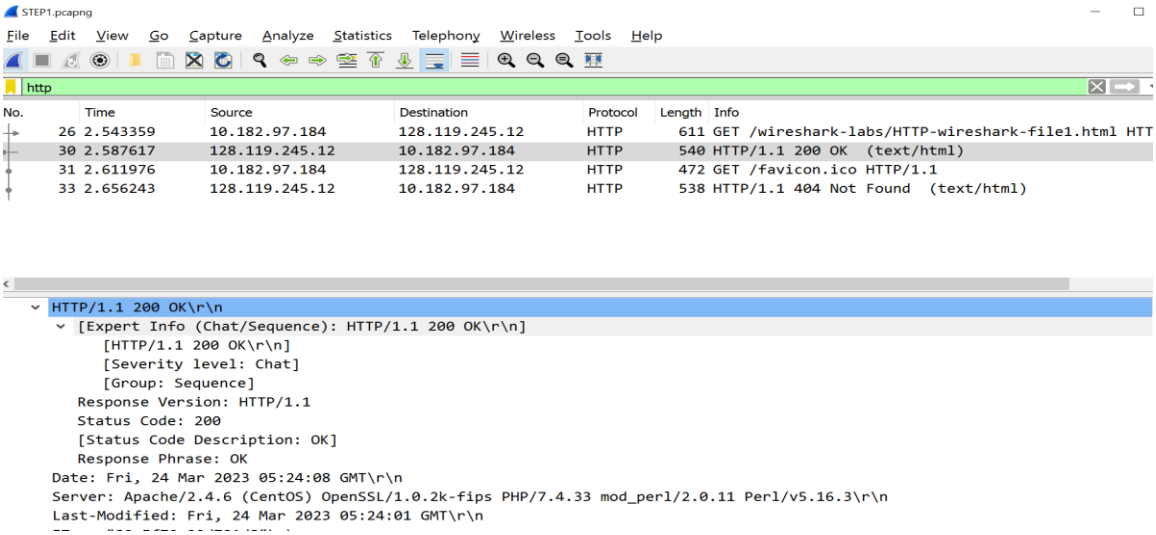




SRC:10.182.97.184

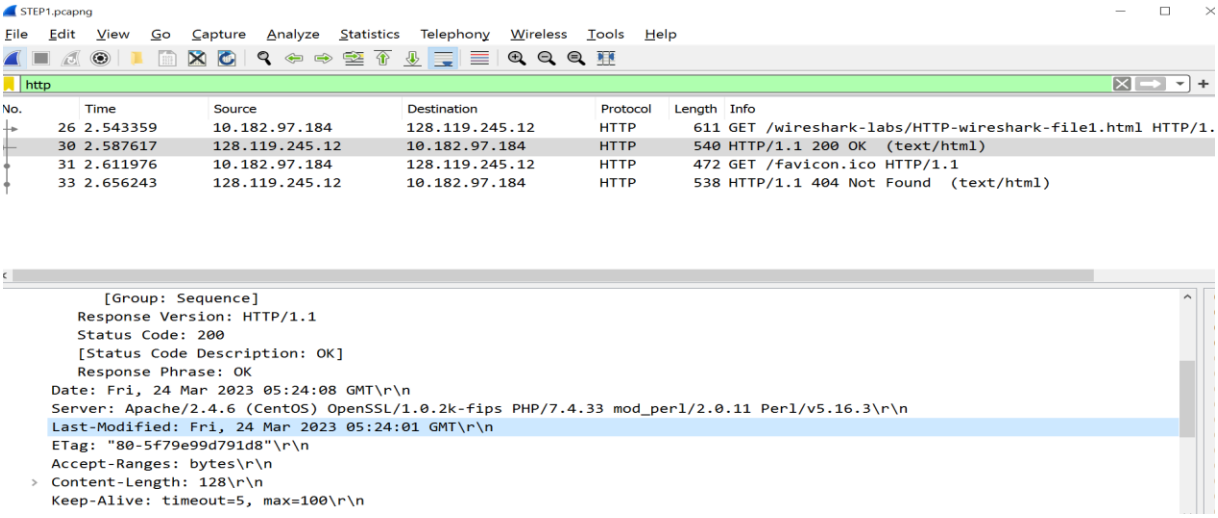
DST:128.119.245.12

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



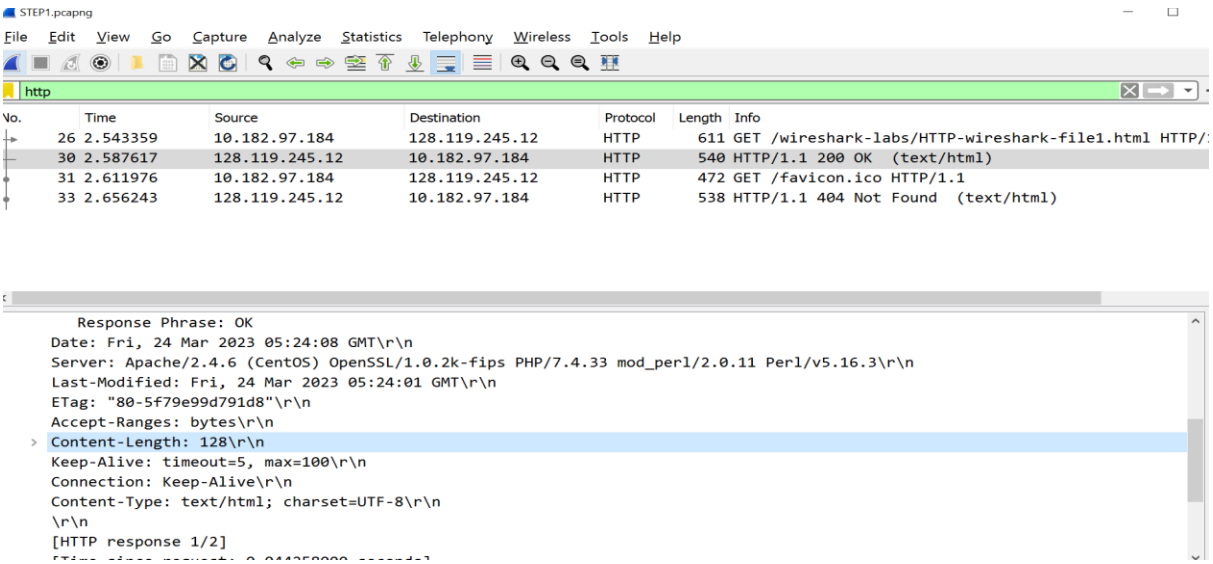
Status code is 200

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



Last Modifies from the http Ok message.

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

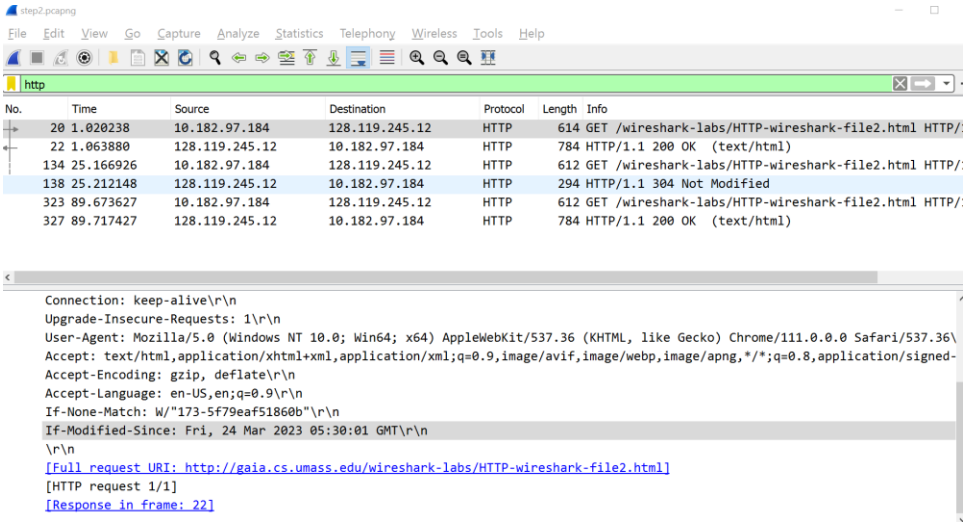


This can be checked from the HTTP ok message content-length

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.

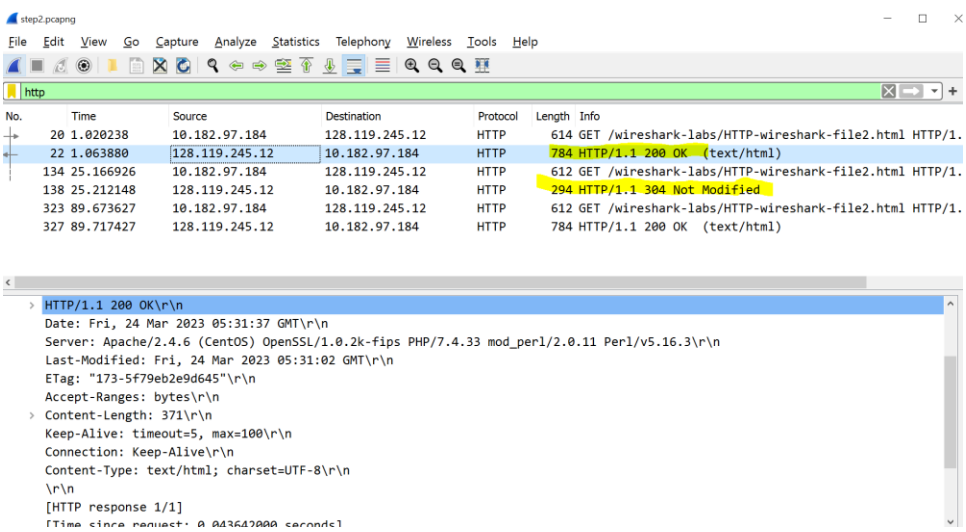
No such packet found.

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?



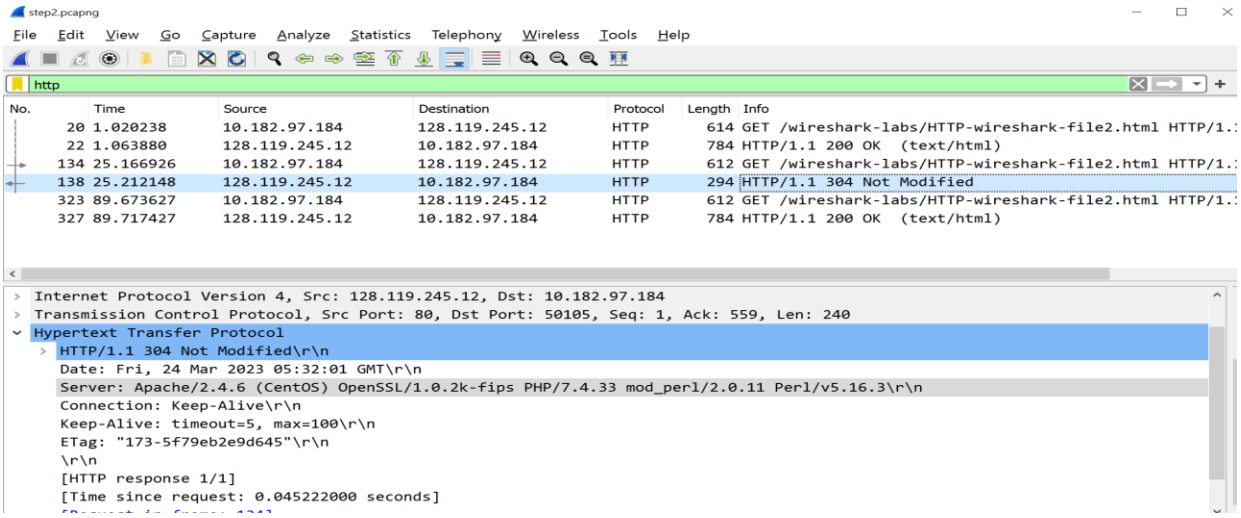
Yes

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



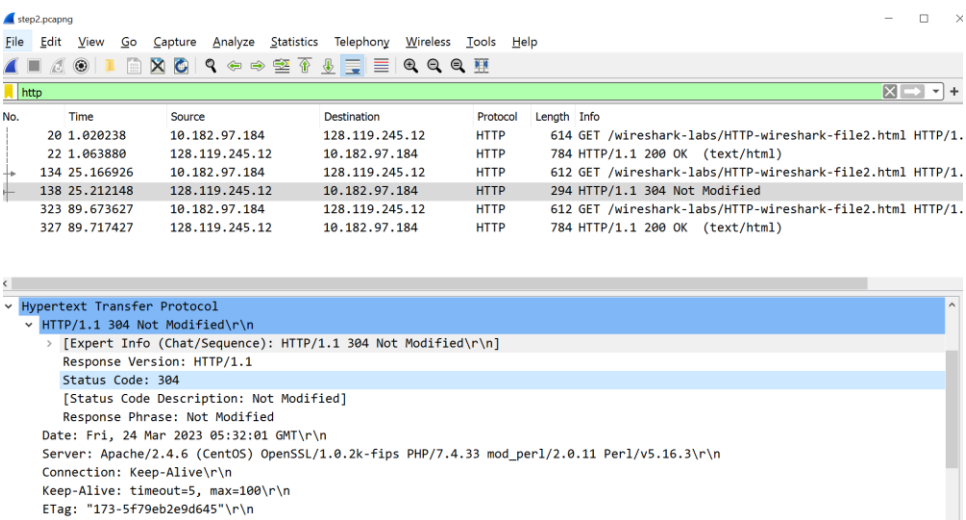
The HTTP OK at 1.063880 and 25.166926 with Not Modified can help us differentiate between the modified and not modified file.

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 not Modified in response message

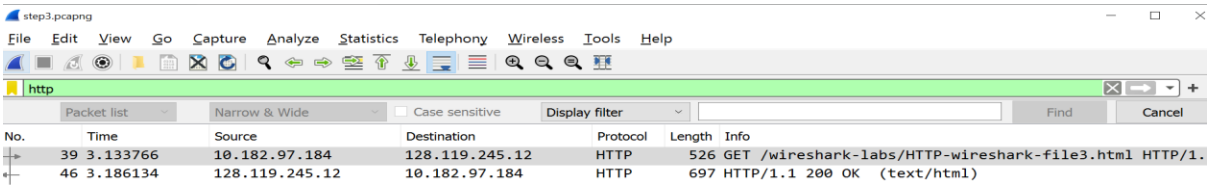
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain

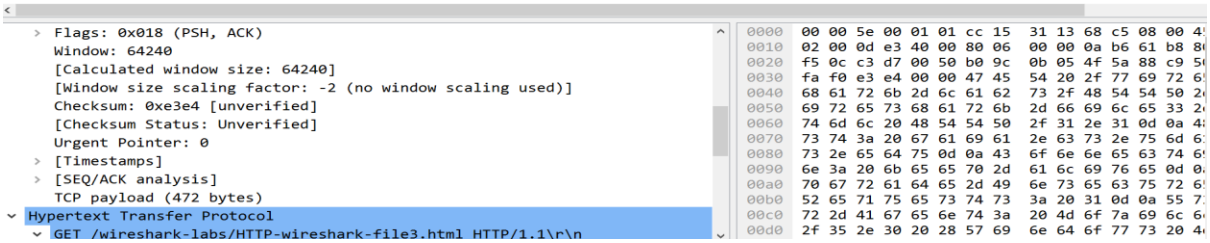


No since the server data was not changed. It replied with a status code of 304 and did not return the data explicitly.

If the status code had been 200 it would have returned the data since it would have been updated. It was a conditional get request.

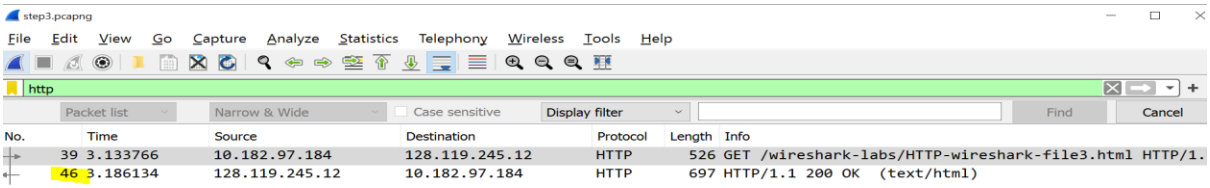
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

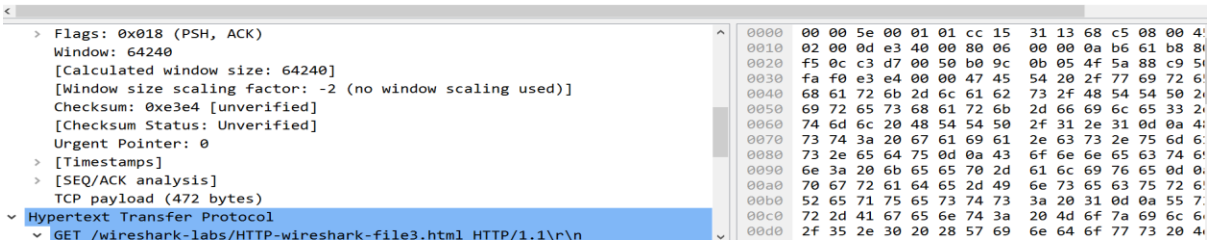




Packet No. -39 is GET message and Only 1 HTTP get request is sent.

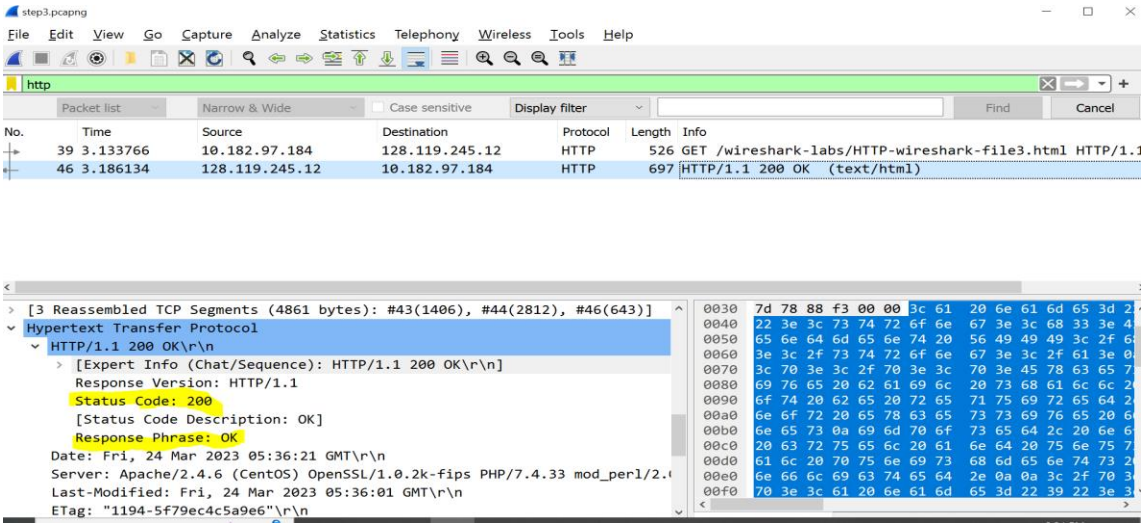
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?





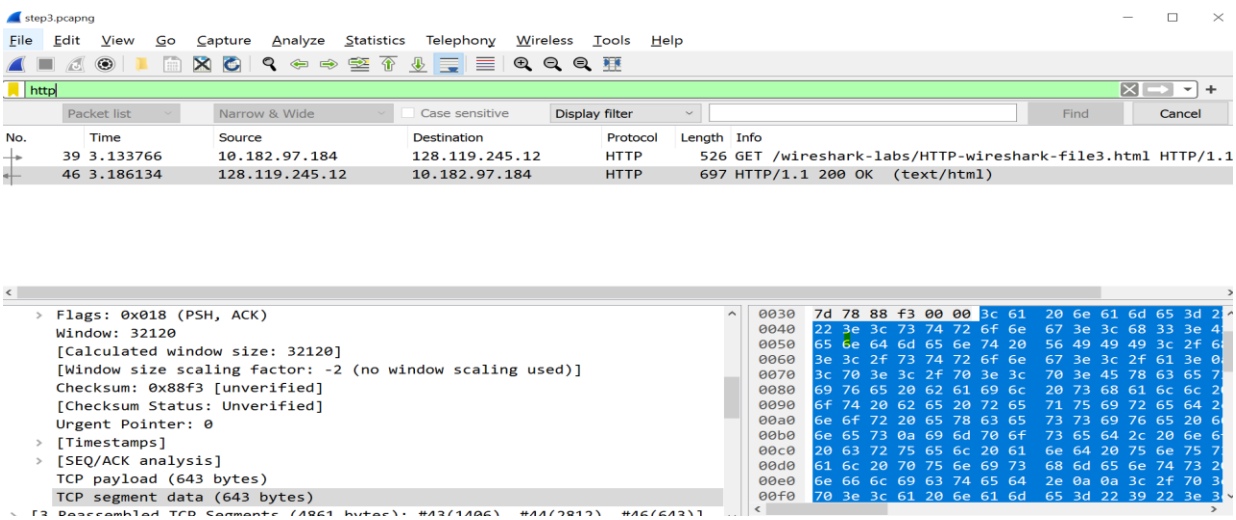
46 Packet number is the response for http get request.

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



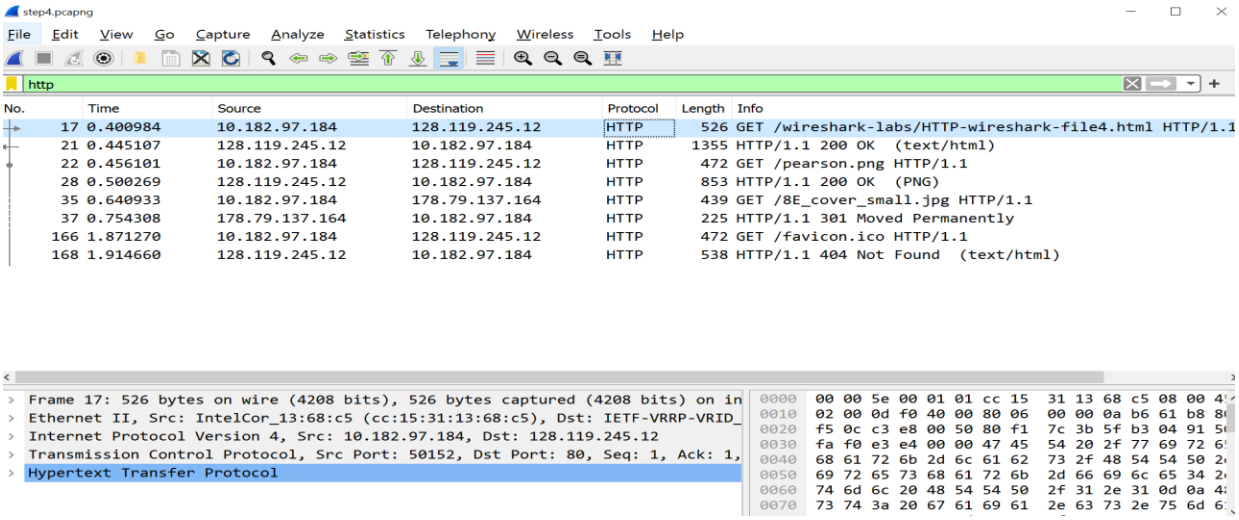
Status code is 200 and response phrase is OK

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



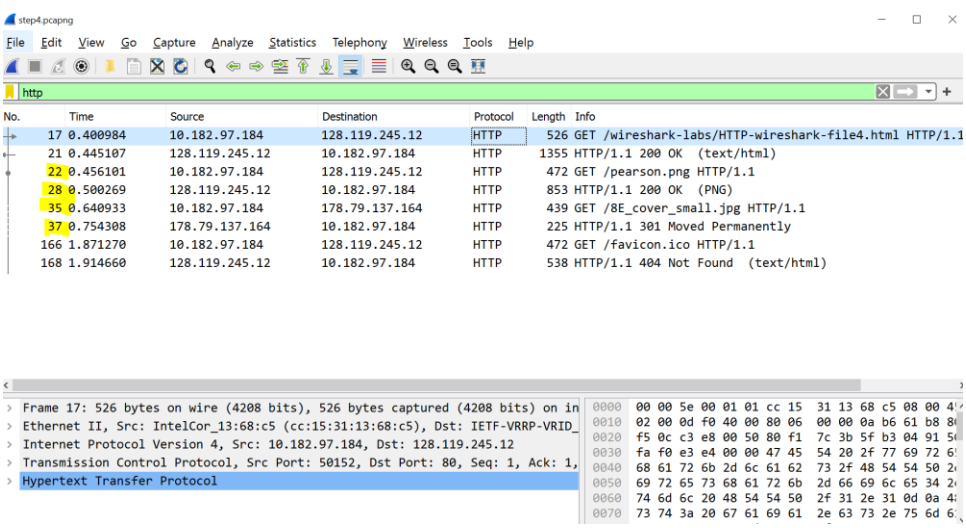
1 HTTP was sent in response to GET request.

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



4 GET request messages were sent to 128.119.245.12.

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.



By checking the TCP ports we can see if our files were downloaded serially or in parallel. In this case the 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.

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

```
> [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
  Response Version: HTTP/1.1
  Status Code: 401
  [Status Code Description: Unauthorized]
  Response Phrase: Unauthorized
Date: Fri, 24 Mar 2023 23:40:28 GMT\r\n
```

Status Code: 401

Response Code: 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?

step5-2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
170	16.138228	192.168.1.20	128.119.245.12	HTTP	544	GET /wireshark-labs/protected_pages/HT
175	16.191450	128.119.245.12	192.168.1.20	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
264	39.149646	192.168.1.20	13.107.4.50	HTTP	300	GET /msdownload/update/v3/static/trust
268	39.157428	13.107.4.50	192.168.1.20	HTTP	585	HTTP/1.1 304 Not Modified
305	44.360460	192.168.1.20	128.119.245.12	HTTP	629	GET /wireshark-labs/protected_pages/HT
335	44.424264	128.119.245.12	192.168.1.20	HTTP	584	HTTP/1.1 404 Not Found (text/html)
352	47.210306	192.168.1.20	13.107.4.50	HTTP	300	GET /msdownload/update/v3/static/trust
355	47.216722	13.107.4.50	192.168.1.20	HTTP	583	HTTP/1.1 304 Not Modified
587	65.520644	192.168.1.20	128.119.245.12	HTTP	603	GET /wireshark-labs/protected_pages/HT
593	65.584949	128.119.245.12	192.168.1.20	HTTP	584	HTTP/1.1 404 Not Found (text/html)

```
> GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
> Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```

```
00b0  0a 41 75 74 68 6f 72 69  7a 6
00c0  42 61 73 69 63 20 64 32  6c 7
00d0  4a 72 4c 58 4e 30 64 57  52 6
00e0  35 6c 64 48 64 76 63 6d  73 3
00f0  61 64 65 2d 49 6e 73 65  63 7
0100  75 65 73 74 73 3a 20 31  0d 0
0110  67 65 6e 74 3a 20 4d 6f  7a 6
```

The message has Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n