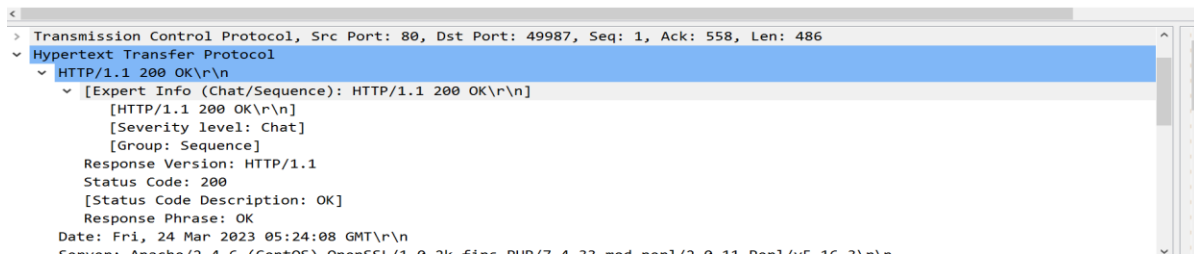
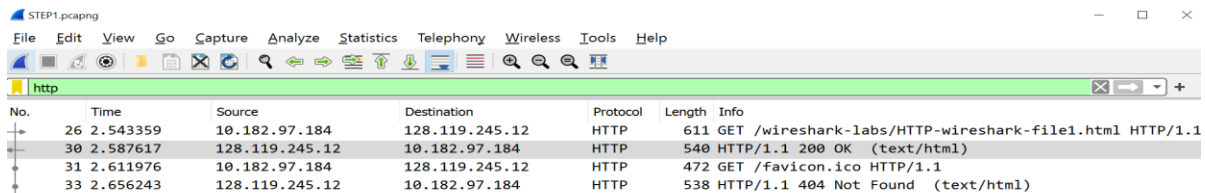
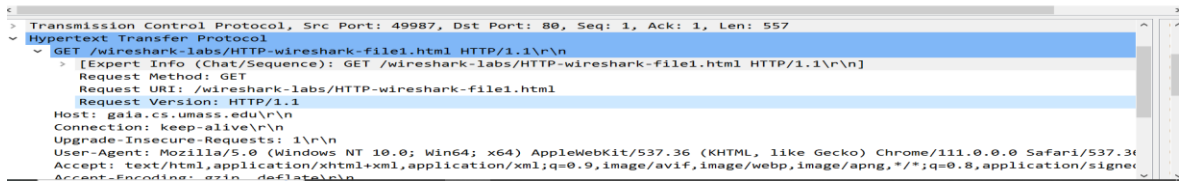
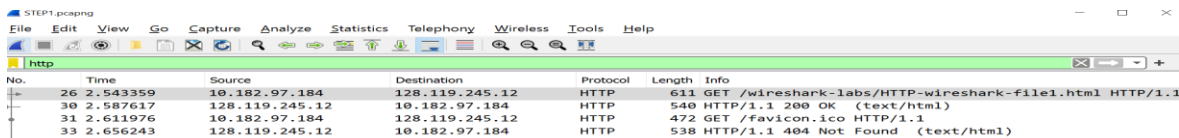
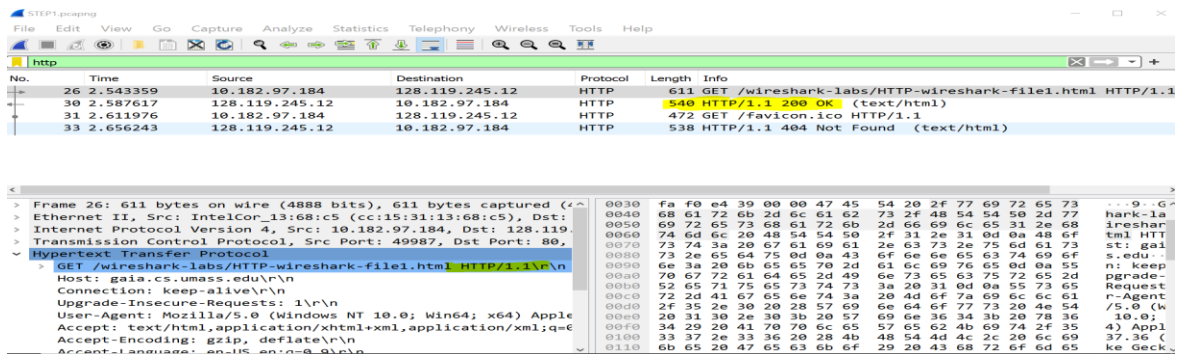


CSE4344/5344 – Project 2 (Spring 2023) Wireshark Lab: HTTP

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?

Wireshark packet capture showing an HTTP GET request. The packet details pane highlights the 'Accept-Language' header.

```
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; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 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=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "80-5f78af92f7965"\r\n
If-Modified-Since: Thu, 23 Mar 2023 05:59:01 GMT\r\n
\r\n
```

Accept language is listed in HTTP get message.

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

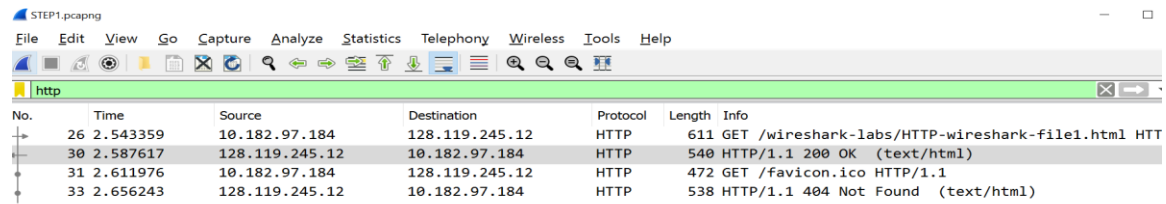
Wireshark packet capture showing an HTTP GET request. The packet details pane highlights the 'Internet Protocol Version 4' header.

```
> Frame 26: 611 bytes on wire (4888 bits), 611 bytes captured (4888 bits) on interface \Device\NPF_{36E86654-3C22-4831-B4F3-6E7...}
> Ethernet II, Src: IntelCor_13:68:c5 (cc:15:31:13:68:c5), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.182.97.184, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 597
    Identification: 0x0d90 (3472)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
```

SRC:10.182.97.184

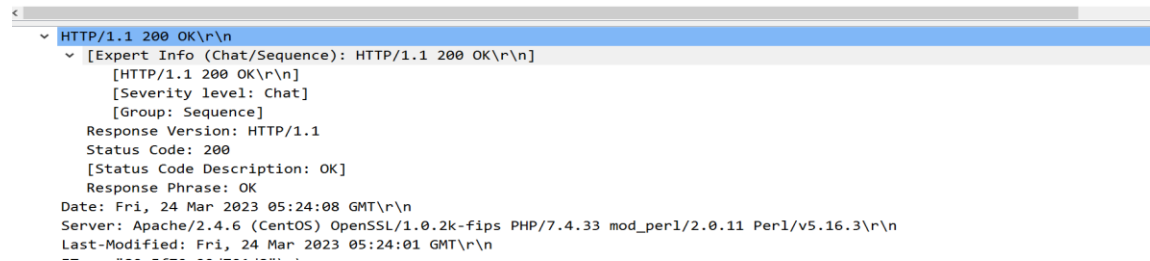
DST:128.119.245.12

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



The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows four packets. Packet 30 is the HTTP 200 OK response. The packet details pane on the right shows the structure of the HTTP response, including the status code 200 and the response phrase 'OK'.

No.	Time	Source	Destination	Protocol	Length	Info
26	2.543359	10.182.97.184	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
30	2.587617	128.119.245.12	10.182.97.184	HTTP	540	HTTP/1.1 200 OK (text/html)
31	2.611976	10.182.97.184	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
33	2.656243	128.119.245.12	10.182.97.184	HTTP	538	HTTP/1.1 404 Not Found (text/html)

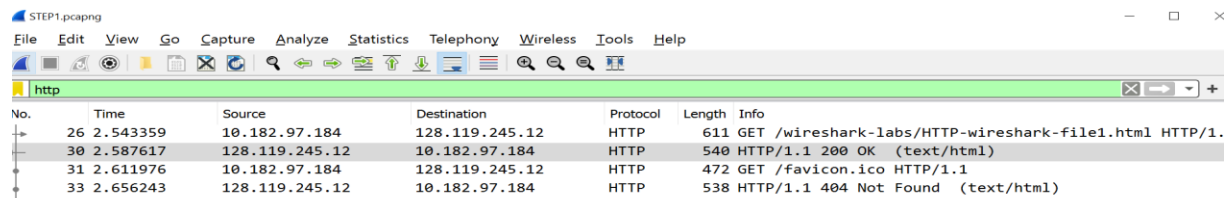


The screenshot shows the packet details pane for the selected HTTP 200 OK packet. The pane is expanded to show the 'Response' section, which includes the status code 200 and the response phrase 'OK'. The 'Date' field shows 'Fri, 24 Mar 2023 05:24:08 GMT'.

```
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 24 Mar 2023 05:24:08 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, 24 Mar 2023 05:24:01 GMT\r\n
-- .....
```

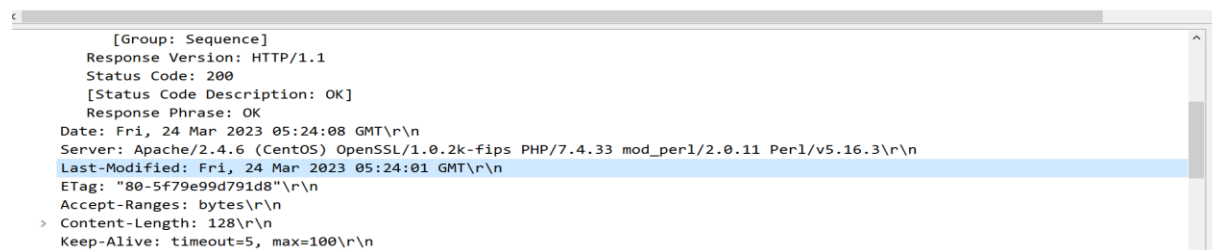
Status code is 200

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



The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows four packets. Packet 30 is the HTTP 200 OK response. The packet details pane on the right shows the structure of the HTTP response, including the status code 200 and the response phrase 'OK'.

No.	Time	Source	Destination	Protocol	Length	Info
26	2.543359	10.182.97.184	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
30	2.587617	128.119.245.12	10.182.97.184	HTTP	540	HTTP/1.1 200 OK (text/html)
31	2.611976	10.182.97.184	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
33	2.656243	128.119.245.12	10.182.97.184	HTTP	538	HTTP/1.1 404 Not Found (text/html)



The screenshot shows the packet details pane for the selected HTTP 200 OK packet. The pane is expanded to show the 'Response' section, which includes the status code 200 and the response phrase 'OK'. The 'Date' field shows 'Fri, 24 Mar 2023 05:24:08 GMT'. The 'Last-Modified' field shows 'Fri, 24 Mar 2023 05:24:01 GMT'.

```
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 24 Mar 2023 05:24:08 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, 24 Mar 2023 05:24:01 GMT\r\n
Etag: "80-5f79e99d791d8"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
```

Last Modified from the http Ok message.

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

The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows four packets. Packet 30 is the HTTP 200 OK response. The packet details pane on the right shows the response structure, including the Content-Length header set to 128.

No.	Time	Source	Destination	Protocol	Length	Info
26	2.543359	10.182.97.184	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
30	2.587617	128.119.245.12	10.182.97.184	HTTP	540	HTTP/1.1 200 OK (text/html)
31	2.611976	10.182.97.184	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
33	2.656243	128.119.245.12	10.182.97.184	HTTP	538	HTTP/1.1 404 Not Found (text/html)

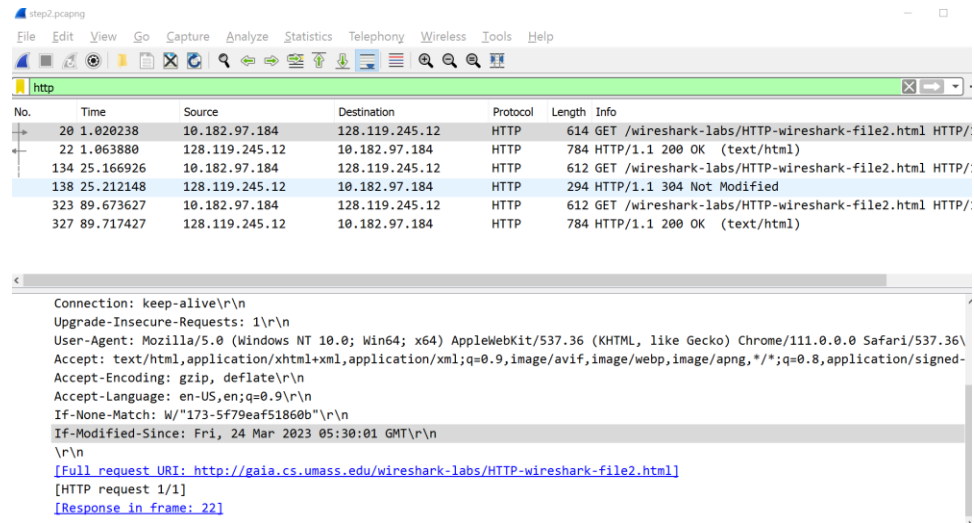
Response Phrase: OK
Date: Fri, 24 Mar 2023 05:24:08 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 24 Mar 2023 05:24:01 GMT\r\n
ETag: "80-5f79e99d791d8"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]

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.

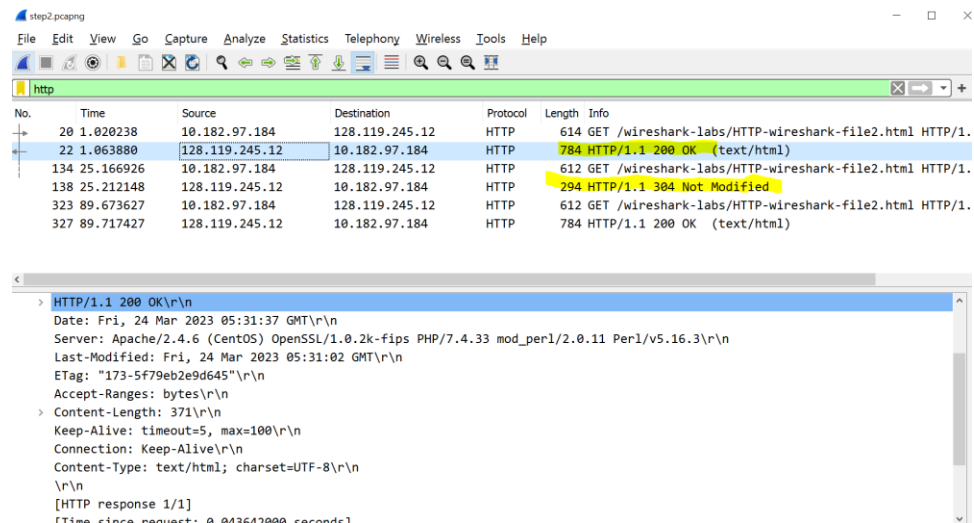
No such packet found.

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?



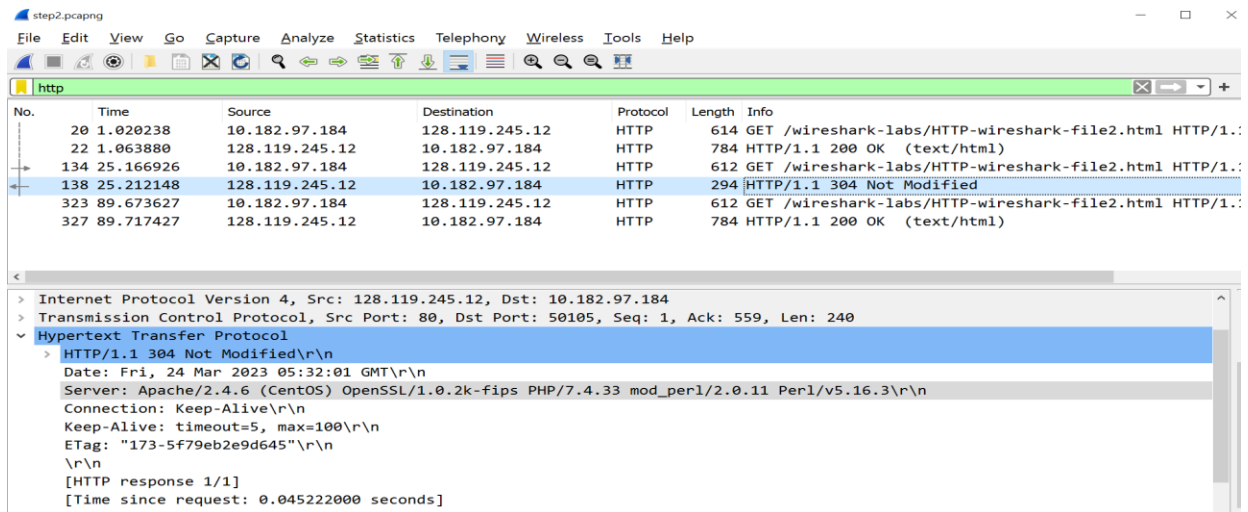
Yes

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



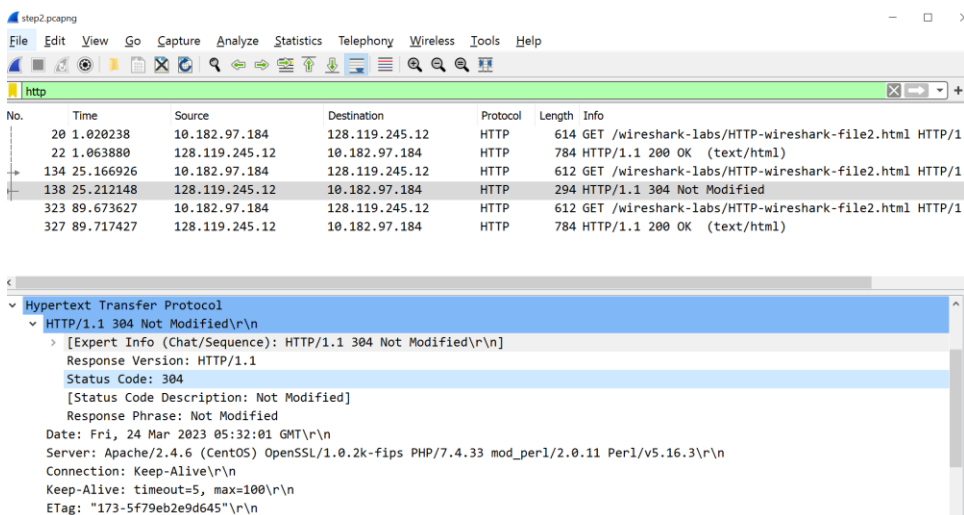
The HTTP OK at 1.063880 and 25.166926 with Not Modified can help us differentiate between the modified and not modified file.

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?

The screenshot shows the Wireshark interface with a packet capture named 'step3.pcapng'. The packet list pane shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
39	3.133766	10.182.97.184	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
46	3.186134	128.119.245.12	10.182.97.184	HTTP	697	HTTP/1.1 200 OK (text/html)

The packet details pane for packet 39 shows the following structure:

- Flags: 0x018 (PSH, ACK)
- Window: 64240
- [Calculated window size: 64240]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0xe3e4 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (472 bytes)
- Hypertext Transfer Protocol**
 - GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n**

The packet bytes pane shows the raw data in hexadecimal and ASCII.

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?

The screenshot shows the Wireshark interface with the same packet capture. The packet list pane shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
39	3.133766	10.182.97.184	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
46	3.186134	128.119.245.12	10.182.97.184	HTTP	697	HTTP/1.1 200 OK (text/html)

The packet details pane for packet 46 shows the following structure:

- Flags: 0x018 (PSH, ACK)
- Window: 64240
- [Calculated window size: 64240]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0xe3e4 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (472 bytes)
- Hypertext Transfer Protocol**
 - HTTP/1.1 200 OK (text/html)**

The packet bytes pane shows the raw data in hexadecimal and ASCII.

46 Packet number is the response for http get request.

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

The screenshot shows the Wireshark interface with a packet capture of an HTTP response. The packet list at the top shows two packets: a GET request (No. 39) and an HTTP/1.1 200 OK response (No. 46). The selected packet (No. 46) is expanded in the packet details pane, showing the response structure: HTTP/1.1 200 OK\r\n, with status code 200 and response phrase OK. The packet bytes pane shows the raw data of the response, starting with 7d 78 88 f3 00 00 3c 61 20 6e 61 6d 65 3d 21.

No.	Time	Source	Destination	Protocol	Length	Info
39	3.133766	10.182.97.184	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
46	3.186134	128.119.245.12	10.182.97.184	HTTP	697	HTTP/1.1 200 OK (text/html)

Packet details for packet 46:

- HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
- Date: Fri, 24 Mar 2023 05:36:21 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.4.6
- Last-Modified: Fri, 24 Mar 2023 05:36:01 GMT\r\n
- ETag: "1194-5f79ec4c5a9e6"\r\n

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?

The screenshot shows the Wireshark interface with a packet capture of a TCP segment. The packet list at the top shows two packets: a GET request (No. 39) and an HTTP/1.1 200 OK response (No. 46). The selected packet (No. 46) is expanded in the packet details pane, showing the response structure: HTTP/1.1 200 OK\r\n, with status code 200 and response phrase OK. The packet bytes pane shows the raw data of the response, starting with 7d 78 88 f3 00 00 3c 61 20 6e 61 6d 65 3d 21.

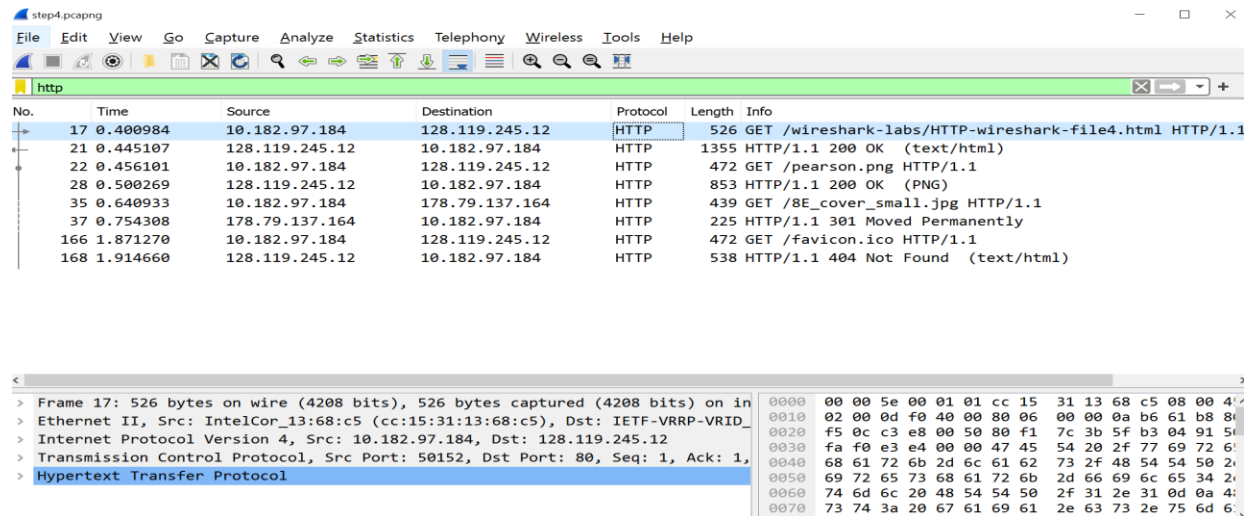
No.	Time	Source	Destination	Protocol	Length	Info
39	3.133766	10.182.97.184	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
46	3.186134	128.119.245.12	10.182.97.184	HTTP	697	HTTP/1.1 200 OK (text/html)

Packet details for packet 46:

- Flags: 0x018 (PSH, ACK)
- Window: 32120
- [Calculated window size: 32120]
- Window size scaling factor: -2 (no window scaling used)
- Checksum: 0x88f3 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (643 bytes)
- TCP segment data (643 bytes)

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?



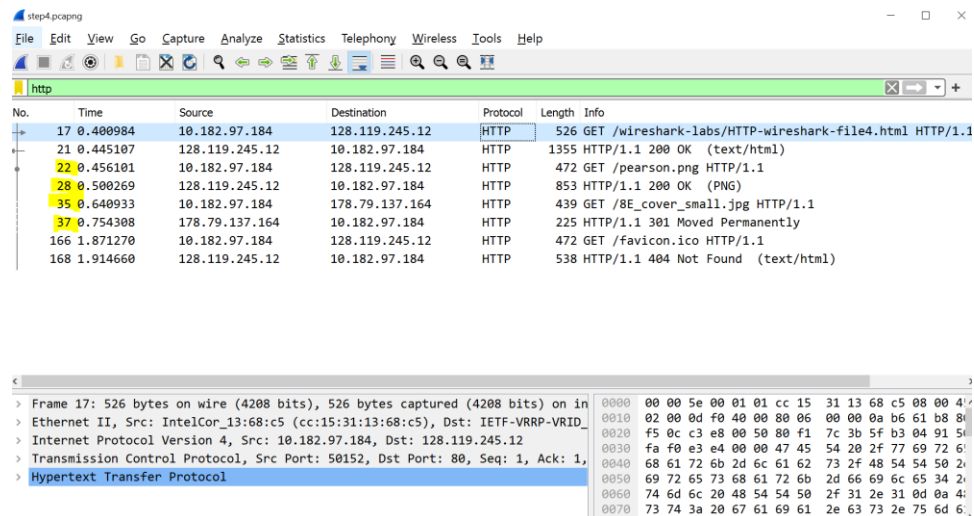
The screenshot shows a Wireshark capture of HTTP traffic. The packet list on the left shows several GET requests to 10.182.97.184. The packet details on the right show the structure of the HTTP GET request for /wireshark-labs/HTTP-wireshark-file4.html.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.400984	10.182.97.184	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
21	0.445107	128.119.245.12	10.182.97.184	HTTP	1355	HTTP/1.1 200 OK (text/html)
22	0.456101	10.182.97.184	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
28	0.500269	128.119.245.12	10.182.97.184	HTTP	853	HTTP/1.1 200 OK (PNG)
35	0.640933	10.182.97.184	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
37	0.754308	178.79.137.164	10.182.97.184	HTTP	225	HTTP/1.1 301 Moved Permanently
166	1.871270	10.182.97.184	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
168	1.914660	128.119.245.12	10.182.97.184	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 17: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
 Ethernet II, Src: IntelCor_13:68:c5 (cc:15:31:13:68:c5), Dst: IETF-VRRP-VRID_...
 Internet Protocol Version 4, Src: 10.182.97.184, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 50152, Dst Port: 80, Seq: 1, Ack: 1, Win: 0, Len: 0
 Hypertext Transfer Protocol

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.



The screenshot shows a Wireshark capture of HTTP traffic. The packet list on the left shows two GET requests for images (pearson.png and 8E_cover_small.jpg) sent to 10.182.97.184. The packet details on the right show the structure of the HTTP GET request for /wireshark-labs/HTTP-wireshark-file4.html.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.400984	10.182.97.184	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
21	0.445107	128.119.245.12	10.182.97.184	HTTP	1355	HTTP/1.1 200 OK (text/html)
22	0.456101	10.182.97.184	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
28	0.500269	128.119.245.12	10.182.97.184	HTTP	853	HTTP/1.1 200 OK (PNG)
35	0.640933	10.182.97.184	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
37	0.754308	178.79.137.164	10.182.97.184	HTTP	225	HTTP/1.1 301 Moved Permanently
166	1.871270	10.182.97.184	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
168	1.914660	128.119.245.12	10.182.97.184	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 17: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
 Ethernet II, Src: IntelCor_13:68:c5 (cc:15:31:13:68:c5), Dst: IETF-VRRP-VRID_...
 Internet Protocol Version 4, Src: 10.182.97.184, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 50152, Dst Port: 80, Seq: 1, Ack: 1, Win: 0, Len: 0
 Hypertext Transfer Protocol

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?

step3-z.pcapng

Io.	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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmcs=\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```

The message has Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmcs=\r\n