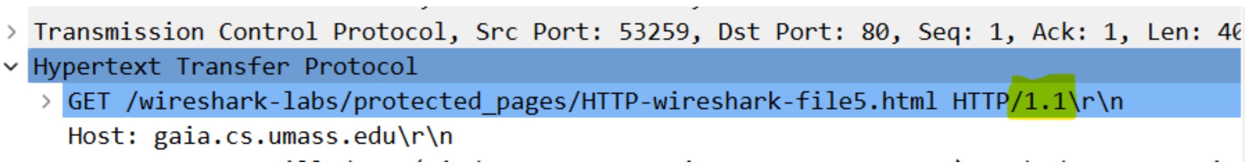
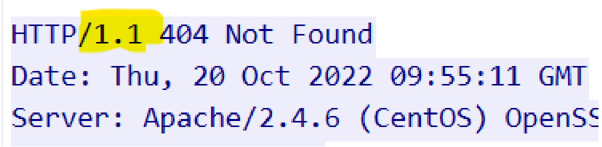
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?



```
> Transmission Control Protocol, Src Port: 53259, Dst Port: 80, Seq: 1, Ack: 1, Len: 4
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
```

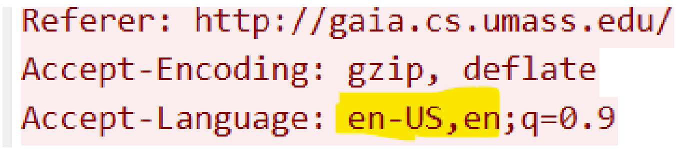
HTTP version is **1.1**



```
HTTP/1.1 404 Not Found
Date: Thu, 20 Oct 2022 09:55:11 GMT
Server: Apache/2.4.6 (CentOS) OpenSS
```

HTTP server is running in **v1.1**

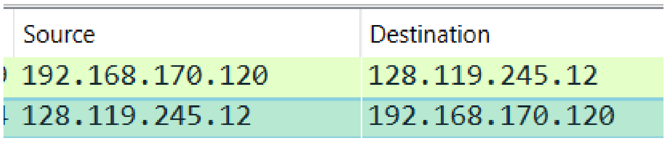
2. What languages (if any) do your browser indicate that it can accept to the server?



```
Referer: http://gaia.cs.umass.edu/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Language : **en-US**

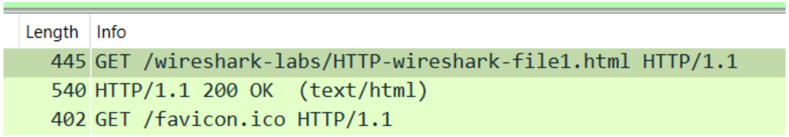
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?



Source	Destination
192.168.170.120	128.119.245.12
128.119.245.12	192.168.170.120

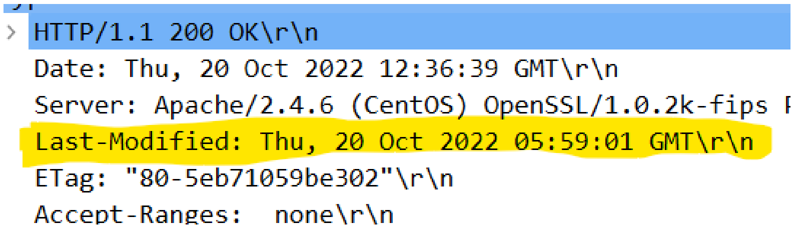
IP Address : 192.168.170.120
Server Address : 128.119.245.12

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



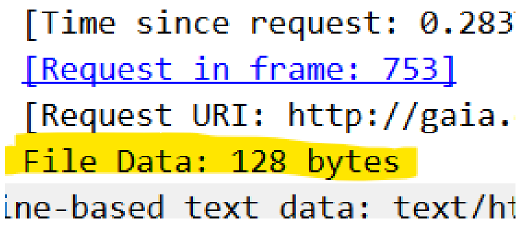
Length	Info
445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
540	HTTP/1.1 200 OK (text/html)
402	GET /favicon.ico HTTP/1.1

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



```
> HTTP/1.1 200 OK\r\n
  Date: Thu, 20 Oct 2022 12:36:39 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips P
  Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT\r\n
  ETag: "80-5eb71059be302"\r\n
  Accept-Ranges:  none\r\n
```

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



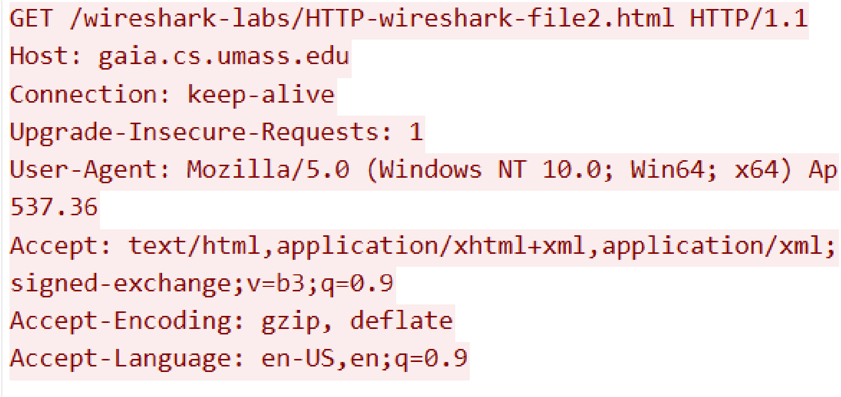
```
 [Time since request: 0.283
 [Request in frame: 753]
 [Request URI: http://gaia.
 File Data: 128 bytes
ine-based text data: text/ht
```

128 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

No

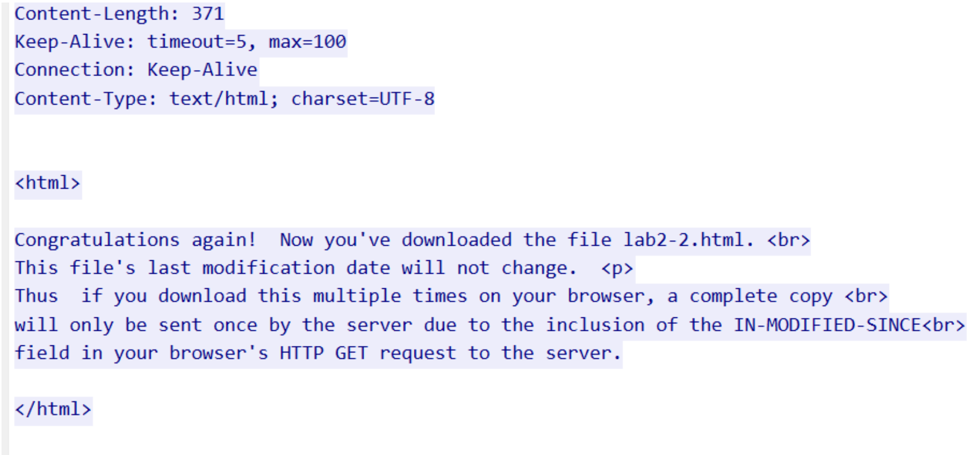
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?



```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
537.36
Accept: text/html,application/xhtml+xml,application/xml;
signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

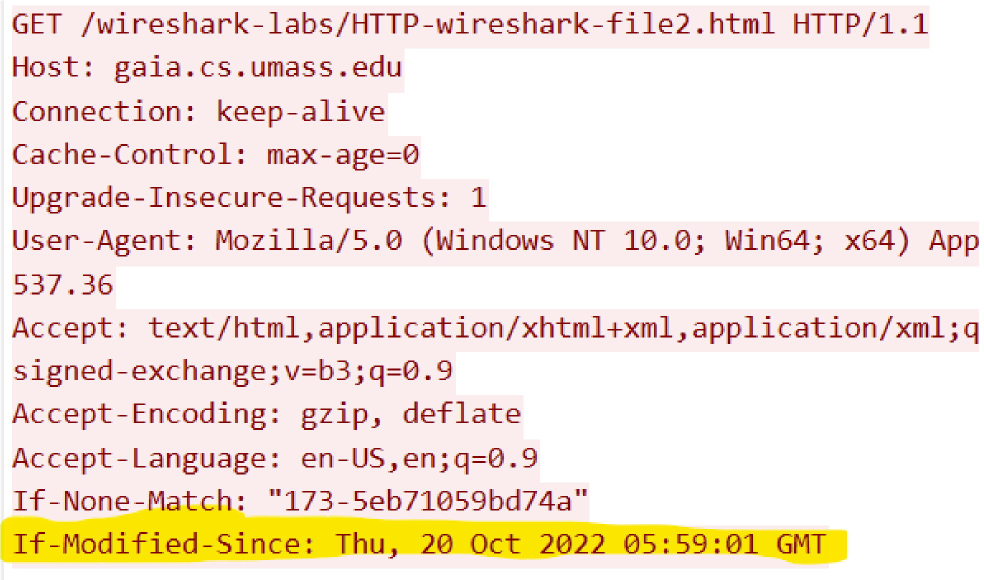
No

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



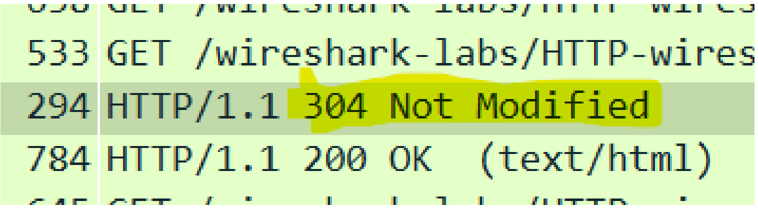
```
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<html>

Congratulations again!  Now you've downloaded the file lab2-2.html. <br>
This file's last modification date will not change.  <p>
Thus  if you download this multiple times on your browser, a complete copy <br>
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
field in your browser's HTTP GET request to the server.

</html>
```

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? What information follows the "IF-MODIFIED?SINCE:" header?



```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
537.36
Accept: text/html,application/xhtml+xml,application/xml;q
signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "173-5eb71059bd74a"
If-Modified-Since: Thu, 20 Oct 2022 05:59:01 GMT
```

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET?



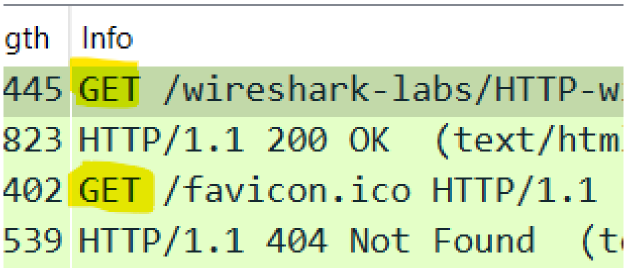
```
533 GET /wireshark-labs/HTTP-wires
294 HTTP/1.1 304 Not Modified
784 HTTP/1.1 200 OK  (text/html)
```

Status Code = 304 , Phrase is : Not Modified

Did the server explicitly return the file's contents?

No , the server didn't returned the file contents because at the time of second GET request, the file is not modifed thus not returning file's contents.

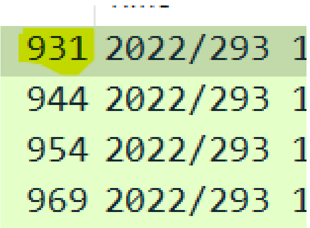
12. How many HTTP GET request messages did your browser send?



```
gth  Info
445  GET /wireshark-labs/HTTP-w
823  HTTP/1.1 200 OK  (text/htm
402  GET /favicon.ico HTTP/1.1
539  HTTP/1.1 404 Not Found  (t
```

2 HTTP GET request messages.

Which packet number in the trace contains the GET message for the Bill or Rights?



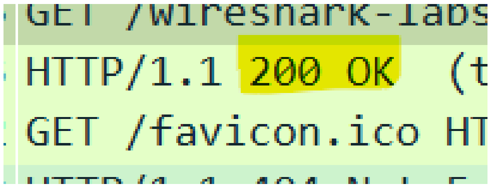
```
931 2022/293 1
944 2022/293 1
954 2022/293 1
969 2022/293 1
```

First Packet (Packet No: 931)

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

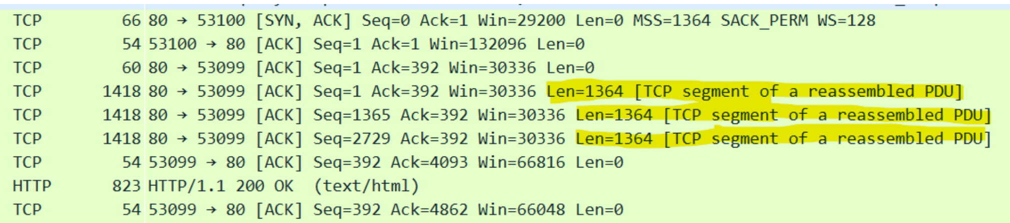
Second Packet (Packet No : 944)

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



```
GET /wireshark-labs
HTTP/1.1 200 OK  (t
GET /favicon.ico HT
```

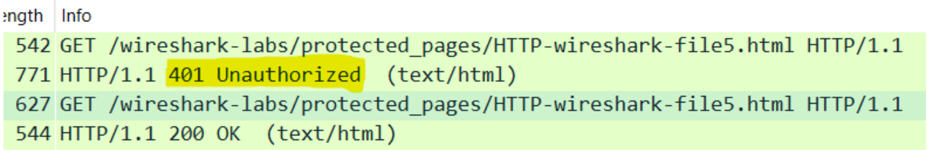
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?



```
TCP         66 80 → 53100 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1364 SACK_PERM WS=128
TCP         54 53100 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
TCP         60 80 → 53099 [ACK] Seq=1 Ack=392 Win=30336 Len=0
TCP       1418 80 → 53099 [ACK] Seq=1 Ack=392 Win=30336 Len=1364 [TCP segment of a reassembled PDU]
TCP       1418 80 → 53099 [ACK] Seq=1365 Ack=392 Win=30336 Len=1364 [TCP segment of a reassembled PDU]
TCP       1418 80 → 53099 [ACK] Seq=2729 Ack=392 Win=30336 Len=1364 [TCP segment of a reassembled PDU]
TCP         54 53099 → 80 [ACK] Seq=392 Ack=4093 Win=66816 Len=0
HTTP       823 HTTP/1.1 200 OK  (text/html)
TCP         54 53099 → 80 [ACK] Seq=392 Ack=4862 Win=66048 Len=0
```

It depends upon the size of the file. In this case , it is 3 TCP segments.

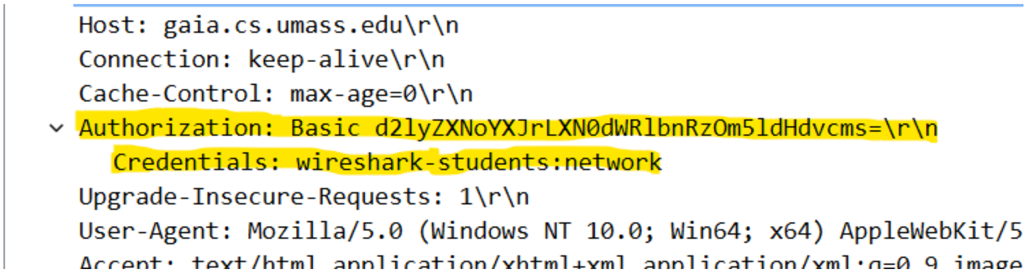
16. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?



```
ength Info
  542 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  771 HTTP/1.1 401 Unauthorized  (text/html)
  627 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  544 HTTP/1.1 200 OK  (text/html)
```

Server's response is : 401 Unauthorized

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



```
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
⌄ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
```

The new field added is : Authorization field

<u>Result</u> :- Thus , exploring web application protocols using protocol analyzer is done successfully.