21CY681 - INTERNET PROTOCOL LAB - III

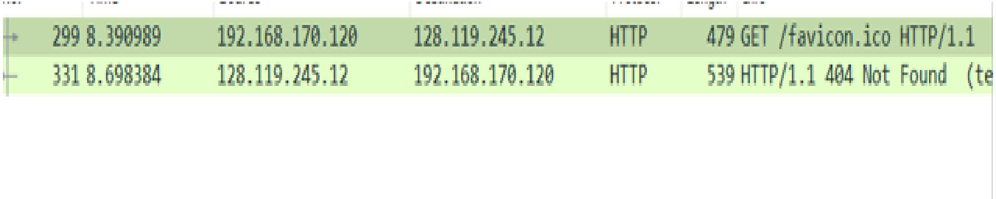
Name: Meera E Thimothy Date: 22nd October 2022

Assignment Topic: To USE WIRESHARK AND ANALYSE VARIOUS HTTP PACKETS AND PROTOCOL

Register Number: CB. EN. P2CYS22002

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

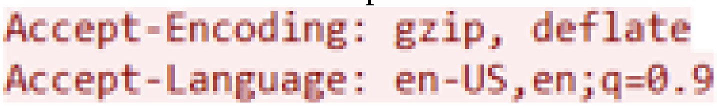
Browser is running on HTTP version 1.1 and the server has version 1.1.



```
299 8.390989   192.168.170.120   128.119.245.12    HTTP   479 GET /favicon.ico HTTP/1.1
331 8.698384   128.119.245.12    192.168.170.120   HTTP   539 HTTP/1.1 404 Not Found  (te
```

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

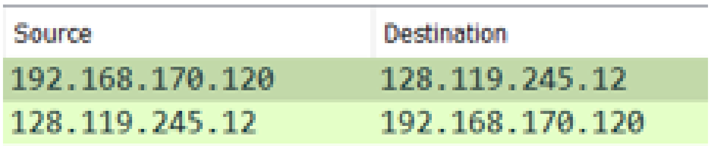
It indicates that it can accept en-US.



```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

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

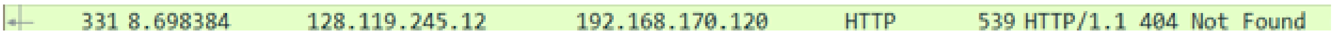
My IP address is 192.168.170.120 and the server is 128.119.245.12



Source	Destination
192.168.170.120	128.119.245.12
128.119.245.12	192.168.170.120

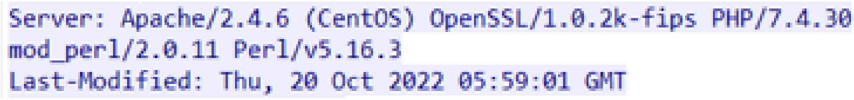
4. What is the status code returned from the server to your browser?

Status code: 404 Not Found



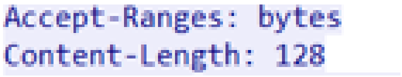
```
331 8.698384    128.119.245.12    192.168.170.120    HTTP    539 HTTP/1.1 404 Not Found
```

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



```
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30
mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT
```

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



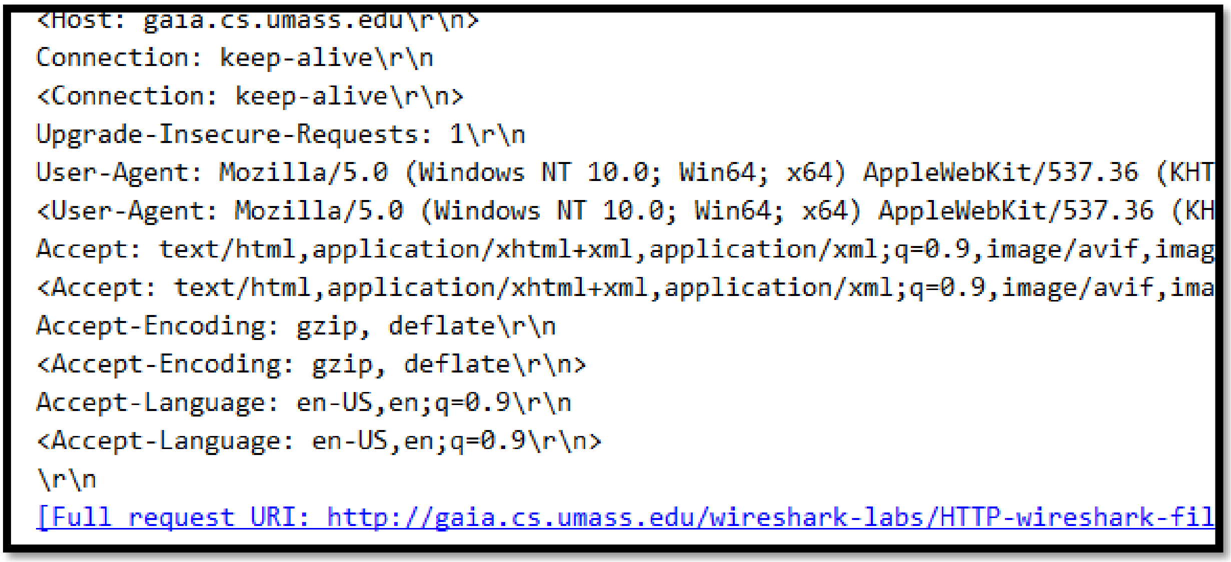
```
Accept-Ranges: bytes
Content-Length: 128
```

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, there is no header within data.

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?

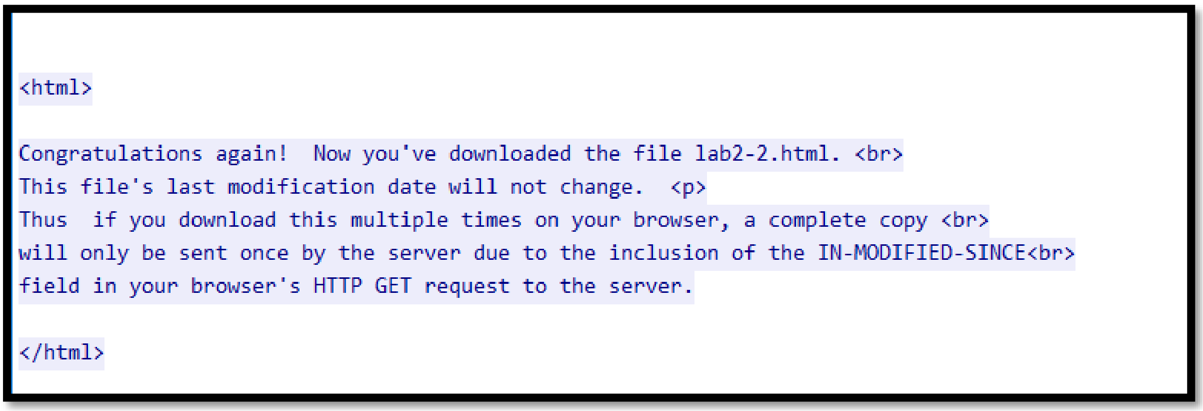
NO, there is no “ IF MODIFIED –SINCE “ line in the HTTP GET.



```
<Host: gaia.cs.umass.edu\r\n>
Connection: keep-alive\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 (KHT
<User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
<Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
Accept-Encoding: gzip, deflate\r\n
<Accept-Encoding: gzip, deflate\r\n>
Accept-Language: en-US,en;q=0.9\r\n
<Accept-Language: en-US,en;q=0.9\r\n>
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-fil
```

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

Yes, the server explicitly return the contents of the file.



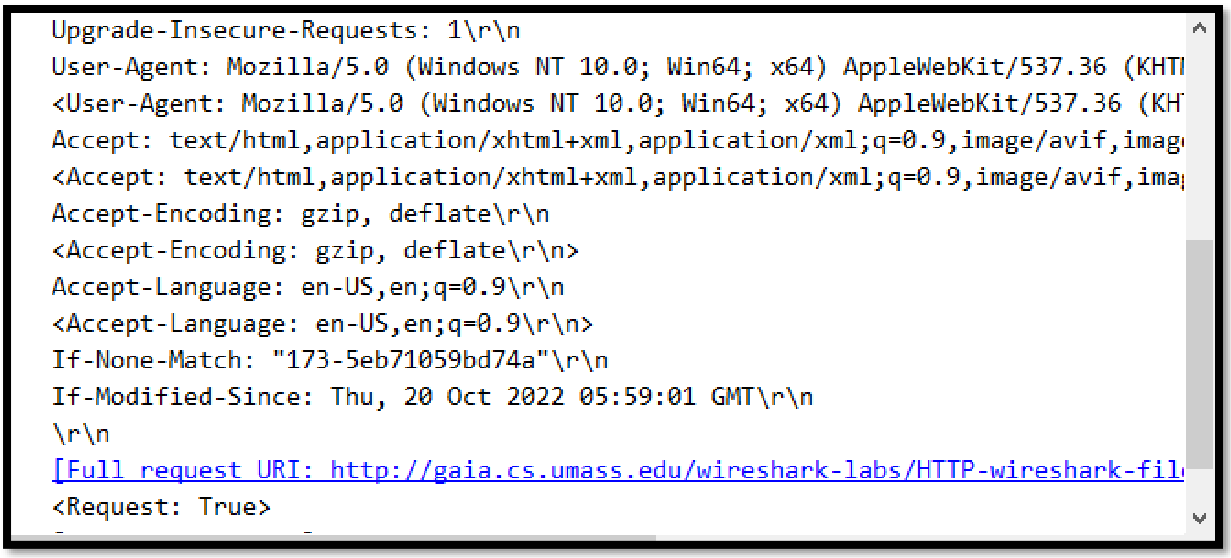
```
<html>

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?

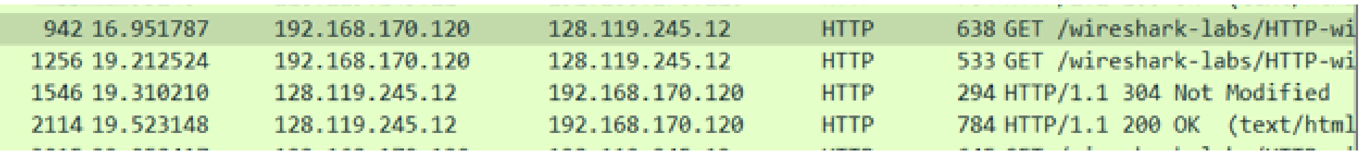
Yes, “if modified since” is visible.



```
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
<User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
<Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
Accept-Encoding: gzip, deflate\r\n
<Accept-Encoding: gzip, deflate\r\n>
Accept-Language: en-US,en;q=0.9\r\n
<Accept-Language: en-US,en;q=0.9\r\n>
If-None-Match: "173-5eb71059bd74a"\r\n
If-Modified-Since: Thu, 20 Oct 2022 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-fil
<Request: True>
```

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 file’s contents? Explain.

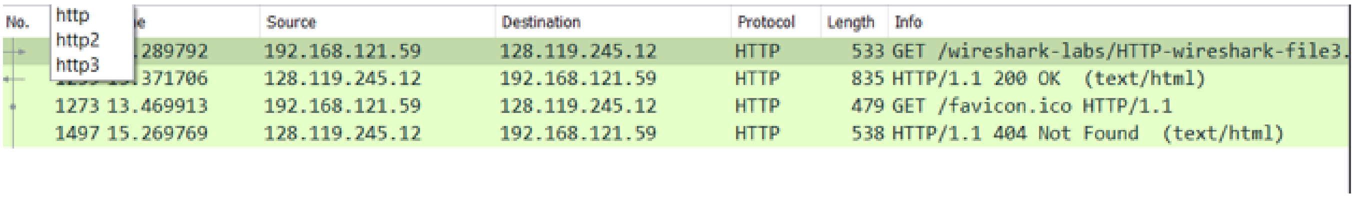
No, the server did not explicitly return the file contents.



```
 942 16.951787   192.168.170.120   128.119.245.12    HTTP    638 GET /wireshark-labs/HTTP-wi
1256 19.212524   192.168.170.120   128.119.245.12    HTTP    533 GET /wireshark-labs/HTTP-wi
1546 19.310210   128.119.245.12    192.168.170.120   HTTP    294 HTTP/1.1 304 Not Modified
2114 19.523148   128.119.245.12    192.168.170.120   HTTP    784 HTTP/1.1 200 OK  (text/html
```

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?

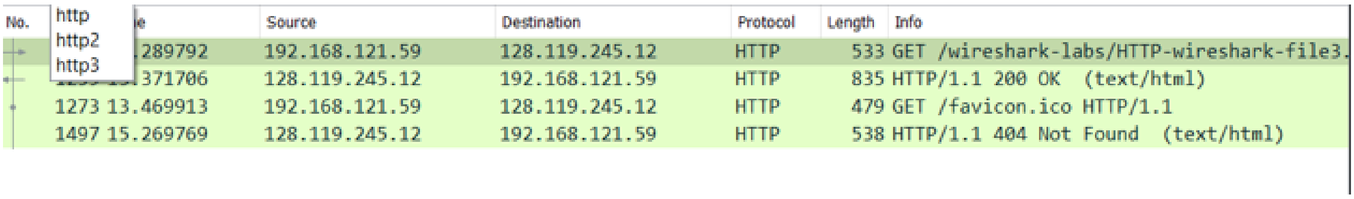
We got 2 get request by using this file. The packet number 1100 in the trace contains the GET message for the bill or rights.



```
No.  http     e        Source            Destination       Protocol  Length Info
     http2    .289792  192.168.121.59    128.119.245.12    HTTP        533 GET /wireshark-labs/HTTP-wireshark-file3.
     http3    .371706  128.119.245.12    192.168.121.59    HTTP        835 HTTP/1.1 200 OK  (text/html)
     1273 13.469913    192.168.121.59    128.119.245.12    HTTP        479 GET /favicon.ico HTTP/1.1
     1497 15.269769    128.119.245.12    192.168.121.59    HTTP        538 HTTP/1.1 404 Not Found  (text/html)
```

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

The packet number 1259 in the trace contains the status code and phrase associated with response to the HTTP GET request.



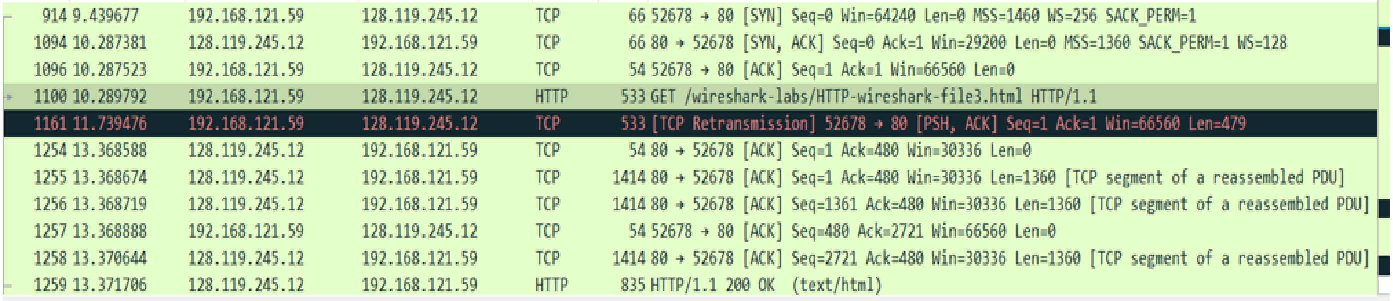
```
No.  http     e        Source            Destination       Protocol  Length Info
     http2    .289792  192.168.121.59    128.119.245.12    HTTP        533 GET /wireshark-labs/HTTP-wireshark-file3.
     http3    .371706  128.119.245.12    192.168.121.59    HTTP        835 HTTP/1.1 200 OK  (text/html)
     1273 13.469913    192.168.121.59    128.119.245.12    HTTP        479 GET /favicon.ico HTTP/1.1
     1497 15.269769    128.119.245.12    192.168.121.59    HTTP        538 HTTP/1.1 404 Not Found  (text/html)
```

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

Status code -200

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

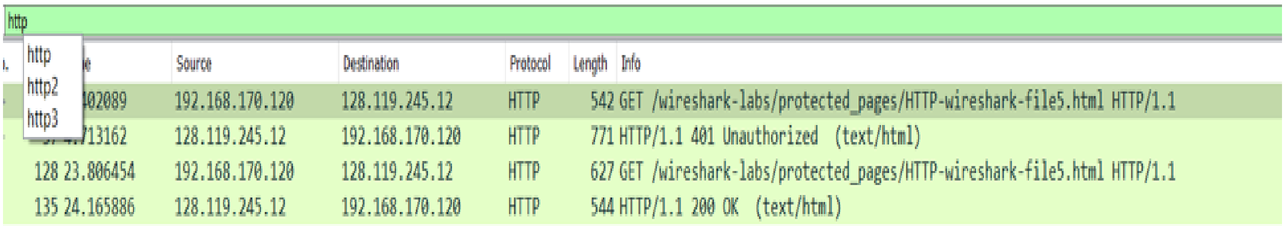


```
 914 9.439677   192.168.121.59   128.119.245.12   TCP     66 52678 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1094 10.287381  128.119.245.12   192.168.121.59   TCP     66 80 → 52678 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=128
1096 10.287523  192.168.121.59   128.119.245.12   TCP     54 52678 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
1100 10.289792  192.168.121.59   128.119.245.12   HTTP   533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1161 11.739476  192.168.121.59   128.119.245.12   TCP    533 [TCP Retransmission] 52678 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66560 Len=479
1254 13.368588  128.119.245.12   192.168.121.59   TCP     54 80 → 52678 [ACK] Seq=1 Ack=480 Win=30336 Len=0
1255 13.368674  128.119.245.12   192.168.121.59   TCP   1414 80 → 52678 [ACK] Seq=1 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
1256 13.368719  128.119.245.12   192.168.121.59   TCP   1414 80 → 52678 [ACK] Seq=1361 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
1257 13.368888  192.168.121.59   128.119.245.12   TCP     54 52678 → 80 [ACK] Seq=480 Ack=2721 Win=66560 Len=0
1258 13.370644  128.119.245.12   192.168.121.59   TCP   1414 80 → 52678 [ACK] Seq=2721 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
1259 13.371706  128.119.245.12   192.168.121.59   HTTP   835 HTTP/1.1 200 OK  (text/html)
```

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

STATUS CODE:401

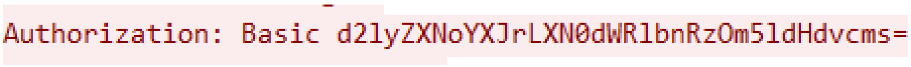
PHRASE: unauthorized



.	e	Source	Destination	Protocol	Length	Info
	402089	192.168.170.120	128.119.245.12	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
	713162	128.119.245.12	192.168.170.120	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
128	23.806454	192.168.170.120	128.119.245.12	HTTP	627	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
135	24.165886	128.119.245.12	192.168.170.120	HTTP	544	HTTP/1.1 200 OK (text/html)

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

Authorization is the new header included in HTTP GET message.



```
Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm51dHdvcms=
```