NAME: S.PRIYADHARSHINI

ROLL NO.: CB.EN.P2CYS22010

DATE: 20.10.2022

INTERNET PROTOCOL LAB – III

AIM:

To use Wireshark packet sniffer to explore http protocol and it's fields.

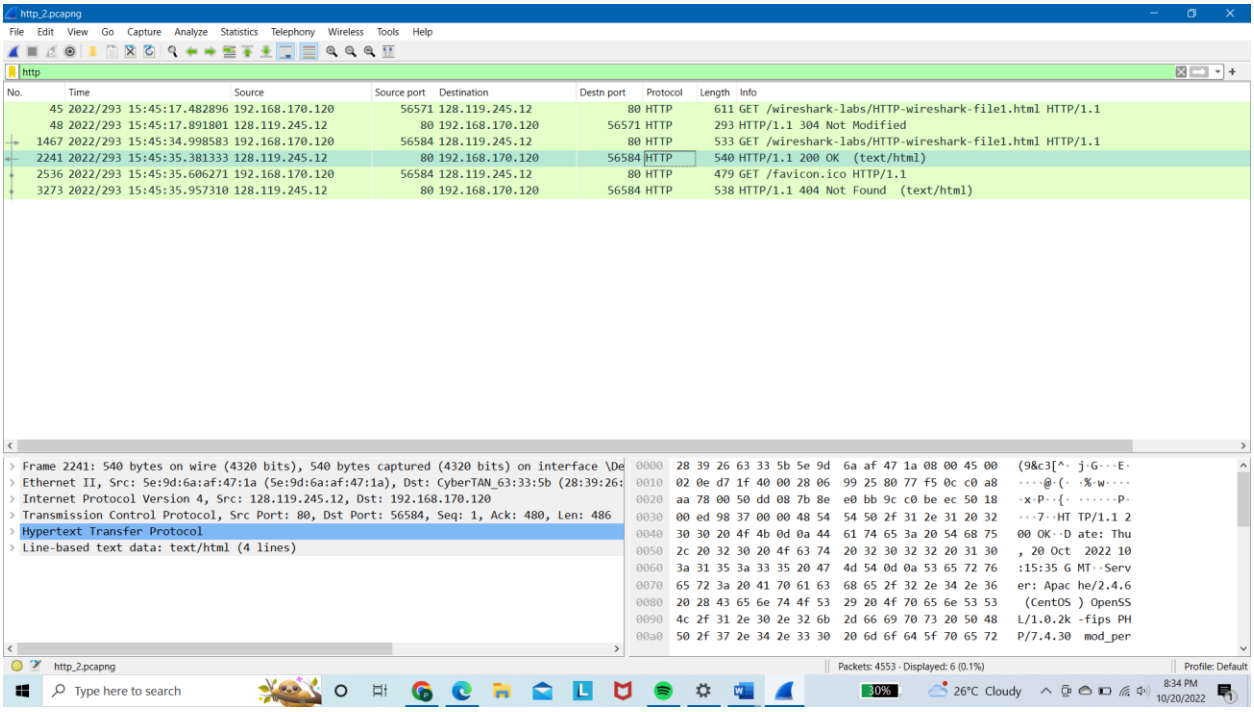
TOOLS REQUIRED:

Wireshark

PROCEDURE:

1. First clear the cache of the browser.
2. Open wireshark and start capturing the packets.
3. Now navigate to the given webpage.
4. Stop the capture in wireshark and search http in display filter. With the contents displayed the information of the packets can be analyzed.

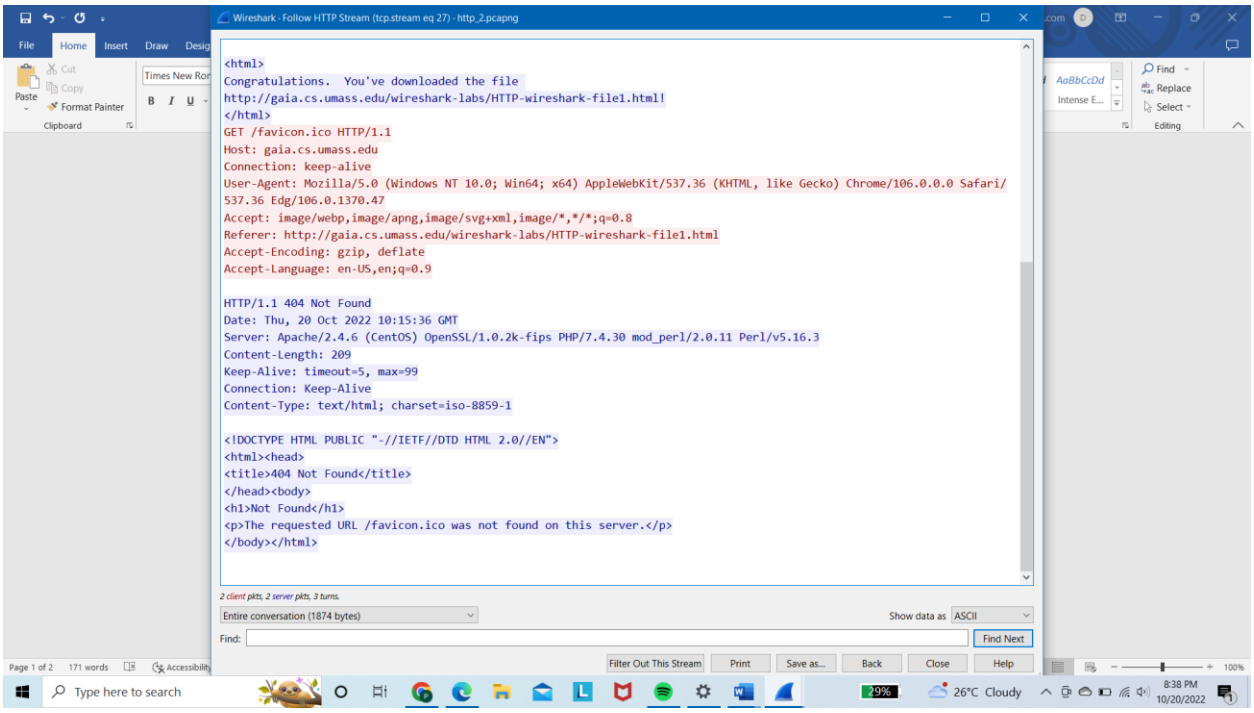
1. file1.html



Questions:

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

The HTTP version of the browser is 1.1. The HTTP version of the server is Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3



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

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

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

No.	Time	Source	Source port	Destination	Destn port	Protocol	Length	Info
45	2022/293 15:45:17.482896	192.168.170.120	56571	128.119.245.12	80	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
48	2022/293 15:45:17.891801	128.119.245.12	80	192.168.170.120	56571	HTTP	293	HTTP/1.1 304 Not Modified
1467	2022/293 15:45:34.998583	192.168.170.120	56584	128.119.245.12	80	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2241	2022/293 15:45:35.381333	128.119.245.12	80	192.168.170.120	56584	HTTP	540	HTTP/1.1 200 OK (text/html)
2536	2022/293 15:45:35.606271	192.168.170.120	56584	128.119.245.12	80	HTTP	479	GET /favicon.ico HTTP/1.1
3273	2022/293 15:45:35.957310	128.119.245.12	80	192.168.170.120	56584	HTTP	538	HTTP/1.1 404 Not Found (text/html)

IP address of computer : 192.168.170.120

IP address of server : 128.119.245.12

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

Status code : 304 - Not Modified

200 - OK

404 - Not Found

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

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 20 Oct 2022 10:15:35 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.
  Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT\r\n
  ETag: "80-5eb71059be302"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 128\r\n
```

This field can be used to check for malicious packets in the network.

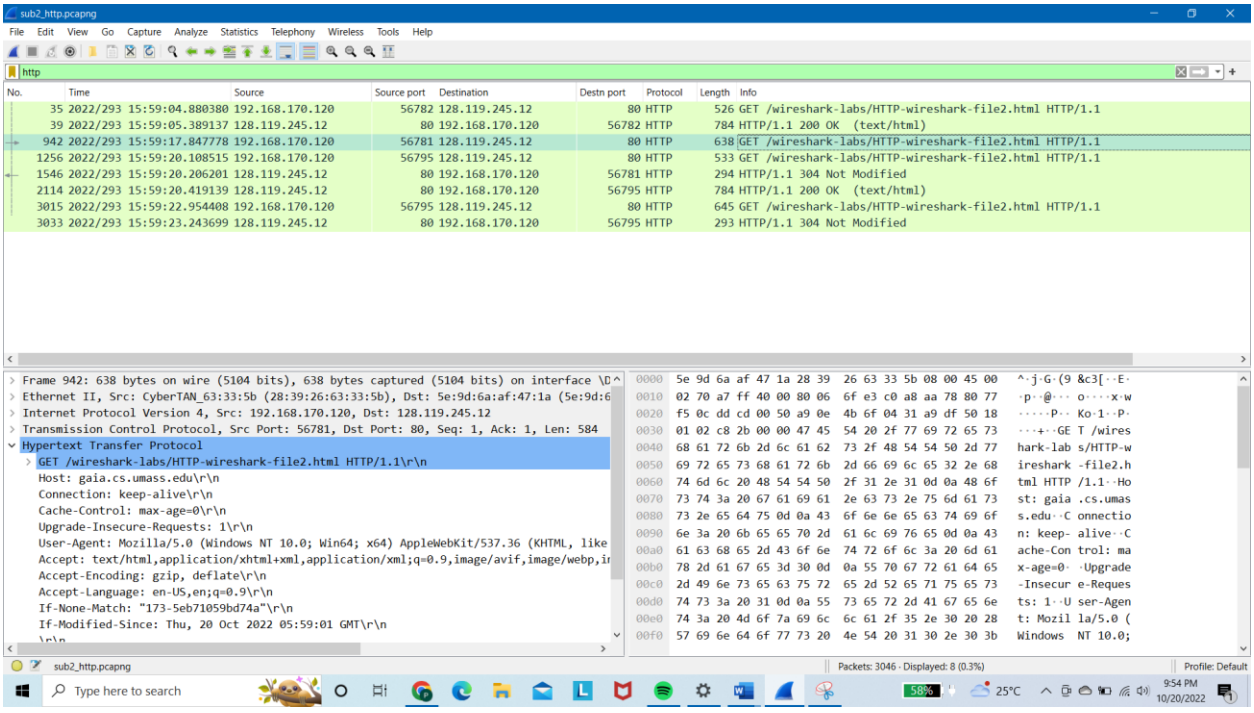
6. How many bytes of content are being returned to your browser?

Content – Length : 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.

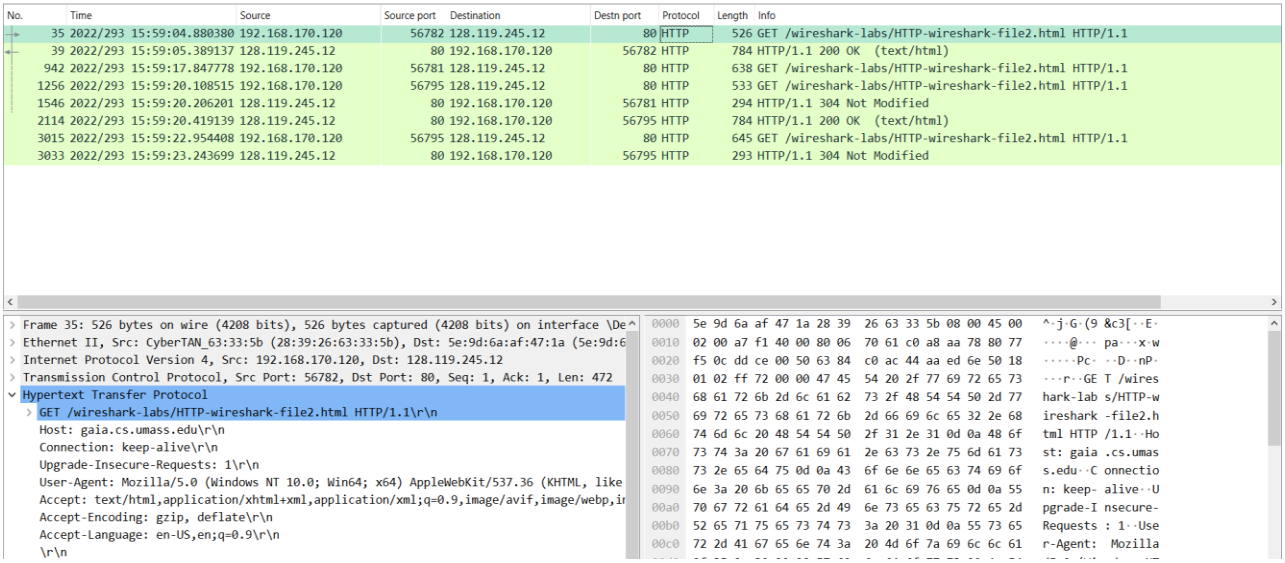
No headers.

2. file2.html



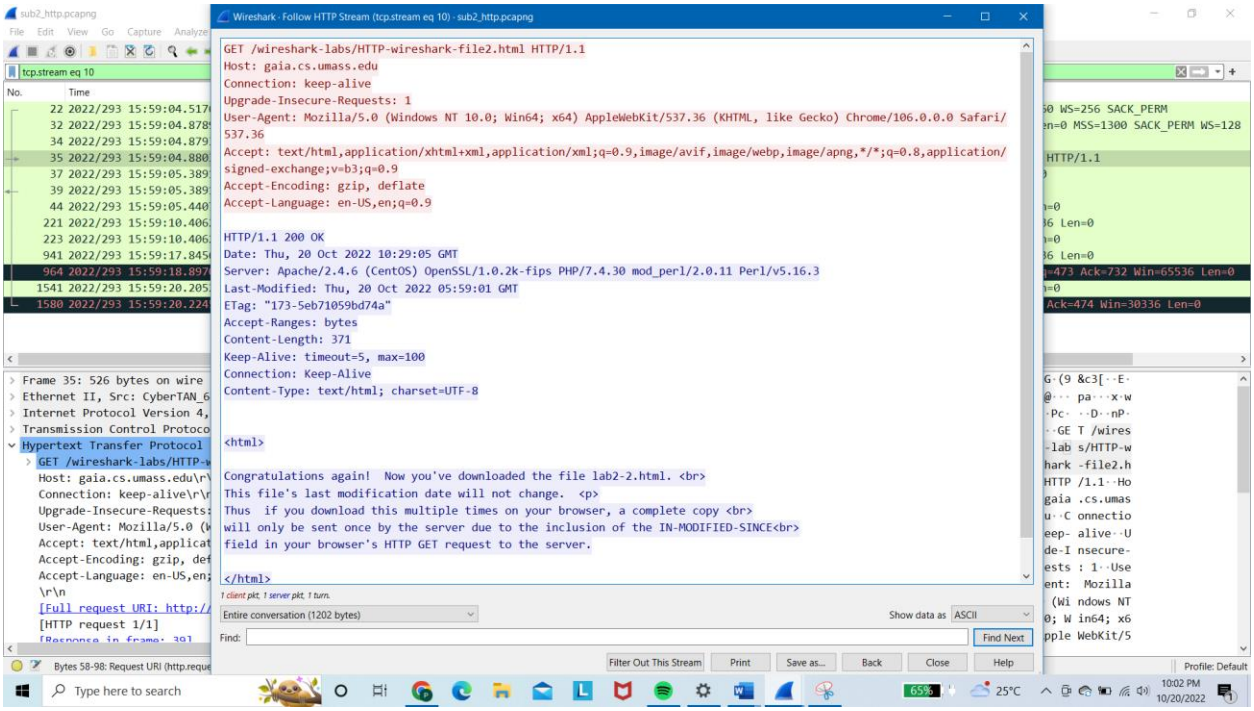
Questions:

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?



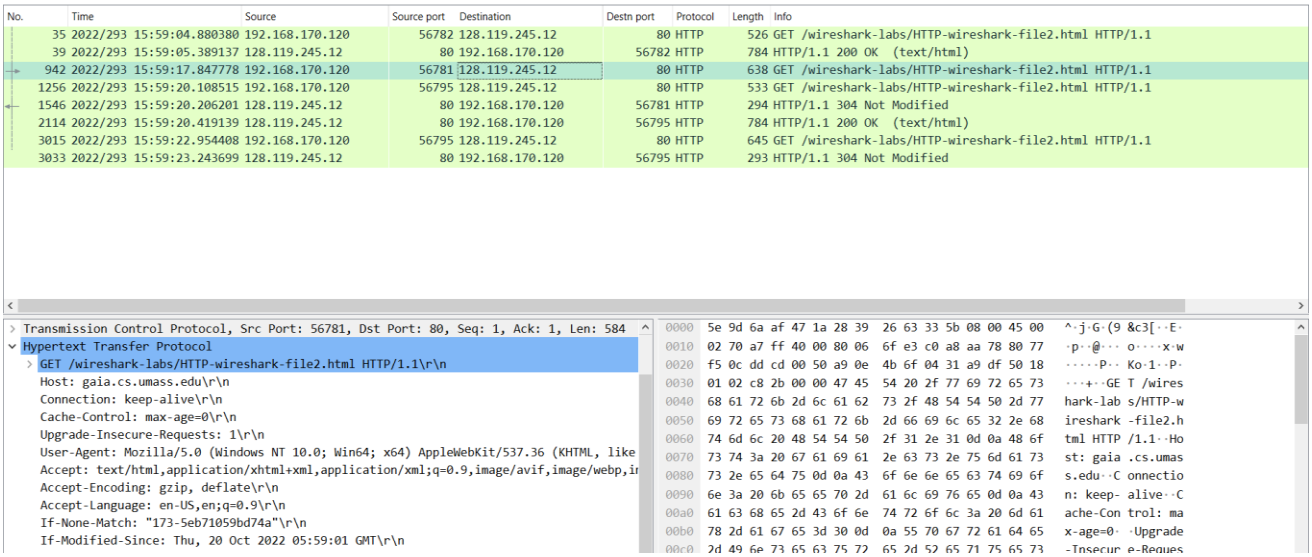
For the first HTTP GET request, the field IF-MODIFIED-SINCE is not present.

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



For the first HTTP GET request the server's response shows the contents of the html file. It can be displayed by right clicking on the packet data and click follow and selecting HTTP stream. It displays the packet content.

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-MODIFIEDSINCE:" header?

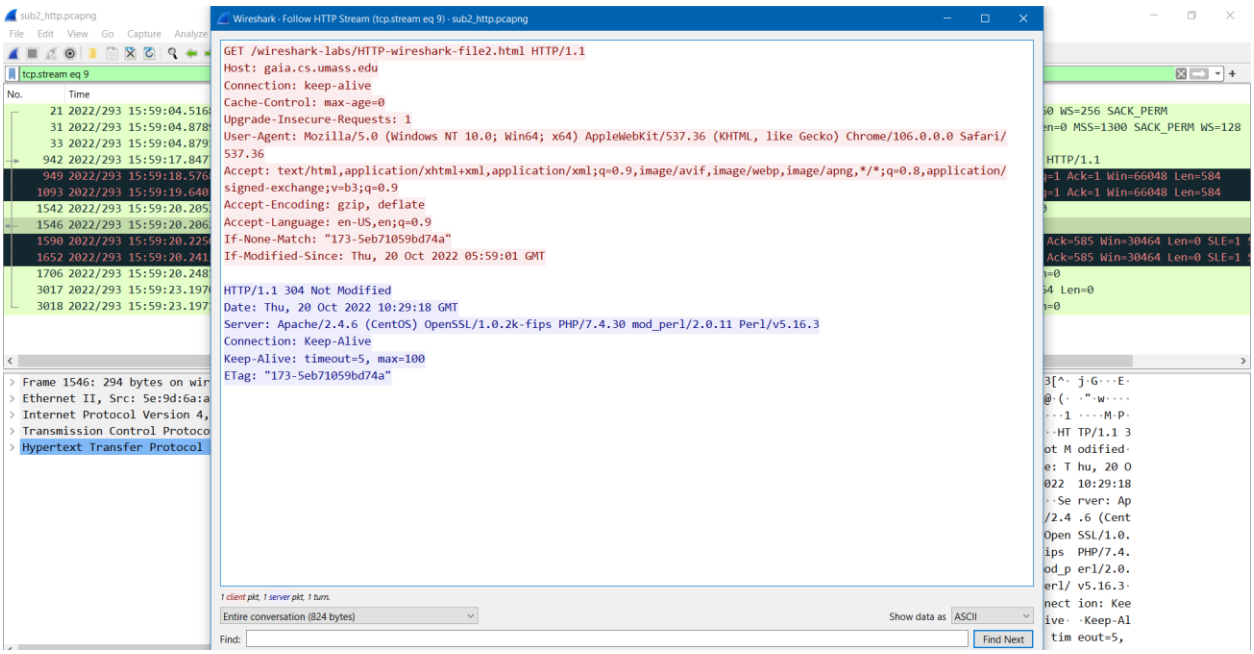


For the second HTTP GET request the field IF-MODIFIED-SINCE is present. This contains, 'If-Modified-Since: Thu, 20 Oct 2022 05:59:01 GMT\r\n'.

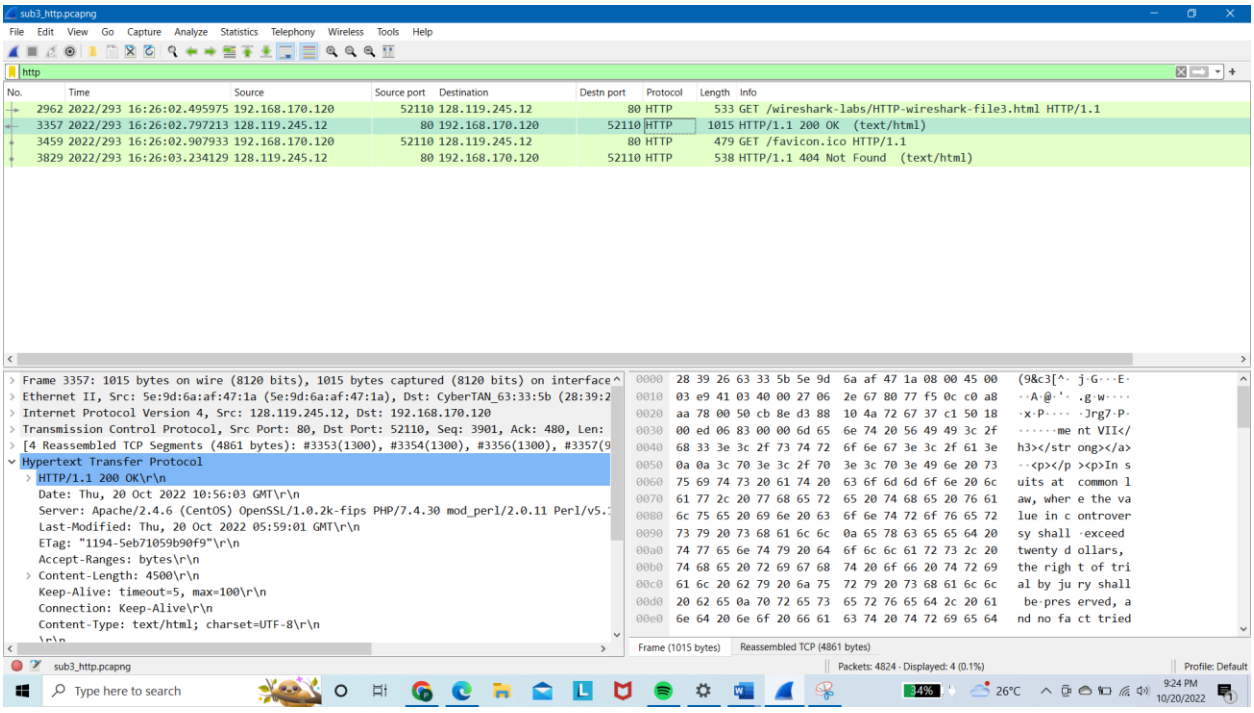
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the file's contents? Explain.

Status code: 304

Phrase: Not Modified, Here the content was not modified so it does not display the contents of the file.


Wireshark · Follow HTTP Stream (tcp.stream eq 9) · sub2_http.pcapng
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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
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
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
HTTP/1.1 304 Not Modified
Date: Thu, 20 Oct 2022 10:29:18 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "173-5eb71059bd74a"
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (824 bytes)
Show data as ASCII
Find:
Find Next

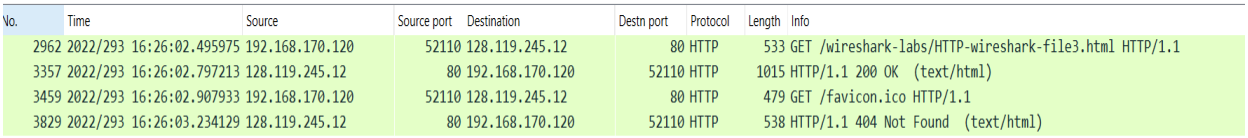
3. file3.html


sub3_http.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Source port Destination Destn port Protocol Length Info
2962 2022/293 16:26:02.495975 192.168.170.120 52110 128.119.245.12 80 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3357 2022/293 16:26:02.797213 128.119.245.12 80 192.168.170.120 52110 HTTP 1015 HTTP/1.1 200 OK (text/html)
3459 2022/293 16:26:02.907933 192.168.170.120 52110 128.119.245.12 80 HTTP 479 GET /favicon.ico HTTP/1.1
3829 2022/293 16:26:03.234129 128.119.245.12 80 192.168.170.120 52110 HTTP 538 HTTP/1.1 404 Not Found (text/html)
Frame 3357: 1015 bytes on wire (8120 bits), 1015 bytes captured (8120 bits) on interface
Ethernet II, Src: 5e:9d:6a:af:47:1a (5e:9d:6a:af:47:1a), Dst: CyberTAN_63:33:5b (28:39:2
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.170.120
Transmission Control Protocol, Src Port: 80, Dst Port: 52110, Seq: 3901, Ack: 480, Len:
[4 Reassembled TCP Segments (4861 bytes): #3353(1300), #3354(1300), #3356(1300), #3357(9
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 20 Oct 2022 10:56:03 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.
Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT\r\n
ETag: "1194-5eb71059b90f9"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 4500\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
0000 28 39 26 63 33 5b 5e 9d 6a af 47 1a 08 00 45 00 (9&c3[^· j·G···E·
0010 03 e9 41 03 40 00 27 06 2e 67 80 77 f5 0c c0 a8 ··A·@·'· .g·w····
0020 aa 78 00 50 cb 8e d3 88 10 4a 72 67 37 c1 50 18 ·x·P···· ·Jrg7·P·
0030 00 ed 06 83 00 00 6d 65 6e 74 20 56 49 49 3c 2f ·····me nt VII</
0040 68 33 3e 3c 2f 73 74 72 6f 6e 67 3e 3c 2f 61 3e h3></str ong>
0050 0a 0a 3c 70 3e 3c 2f 70 3e 3c 70 3e 49 6e 20 73 ·· In s
0060 75 69 74 73 20 61 74 20 63 6f 6d 6d 6f 6e 20 6c uits at common l
0070 61 77 2c 20 77 68 65 72 65 20 74 68 65 20 76 61 aw, wher e the va
0080 6c 75 65 20 69 6e 20 63 6f 6e 74 72 6f 76 65 72 lue in c ontrover
0090 73 79 20 73 68 61 6c 6c 0a 65 78 63 65 65 64 20 sy shall ·exceed
00a0 74 77 65 6e 74 79 20 64 6f 6c 6c 61 72 73 2c 20 twenty d ollars,
00b0 74 68 65 20 72 69 67 68 74 20 6f 66 20 74 72 69 the righ t of tri
00c0 61 6c 20 62 79 20 6a 75 72 79 20 73 68 61 6c 6c al by ju ry shall
00d0 20 62 65 0a 70 72 65 73 65 72 76 65 64 2c 20 61 be·pres erved, a
00e0 6e 64 20 6e 6f 20 66 61 63 74 20 74 72 69 65 64 nd no fa ct tried
Frame (1015 bytes) Reassembled TCP (4861 bytes)
sub3_http.pcapng
Packets: 4824 · Displayed: 4 (0.1%)
Profile: Default
Type here to search
34%
26°C
9:24 PM
10/20/2022

Questions:

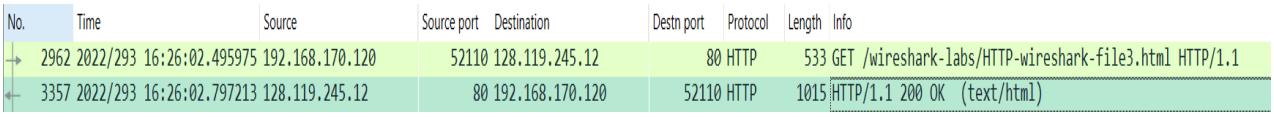
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

There are 2 GET request message.



No.	Time	Source	Source port	Destination	Destn port	Protocol	Length	Info
2962	2022/293 16:26:02.495975	192.168.170.120	52110	128.119.245.12	80	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3357	2022/293 16:26:02.797213	128.119.245.12	80	192.168.170.120	52110	HTTP	1015	HTTP/1.1 200 OK (text/html)
3459	2022/293 16:26:02.907933	192.168.170.120	52110	128.119.245.12	80	HTTP	479	GET /favicon.ico HTTP/1.1
3829	2022/293 16:26:03.234129	128.119.245.12	80	192.168.170.120	52110	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?



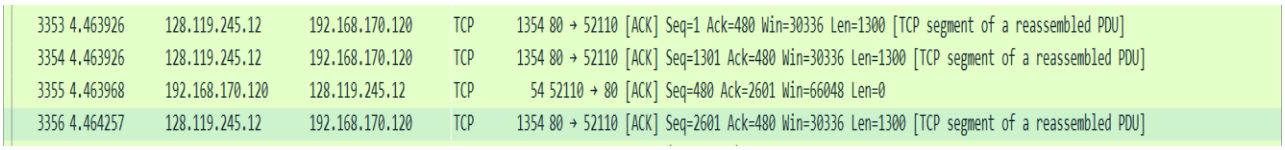
No.	Time	Source	Source port	Destination	Destn port	Protocol	Length	Info
2962	2022/293 16:26:02.495975	192.168.170.120	52110	128.119.245.12	80	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3357	2022/293 16:26:02.797213	128.119.245.12	80	192.168.170.120	52110	HTTP	1015	HTTP/1.1 200 OK (text/html)

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

Status code: 200

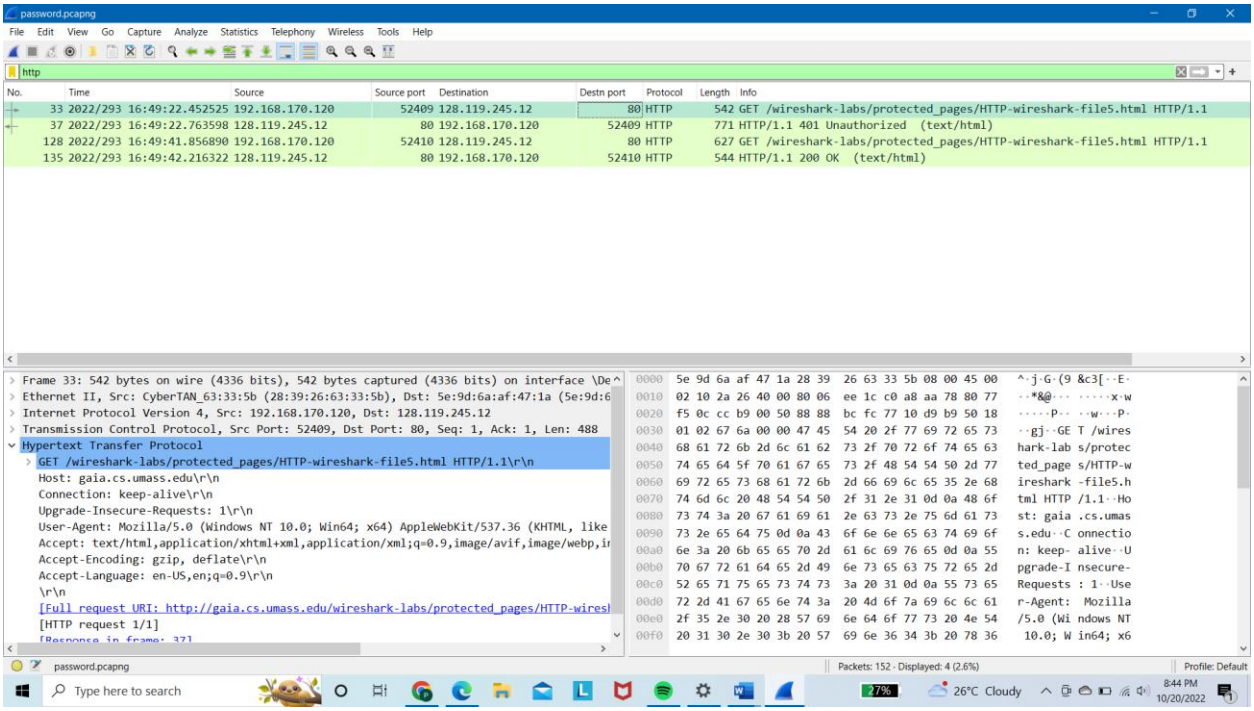
Phrase: OK

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



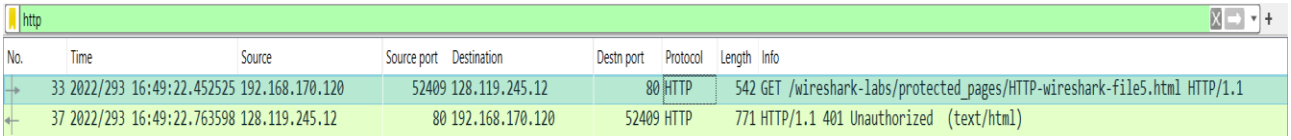
3353	4.463926	128.119.245.12	192.168.170.120	TCP	1354	80 → 52110 [ACK] Seq=1 Ack=480 Win=30336 Len=1300 [TCP segment of a reassembled PDU]
3354	4.463926	128.119.245.12	192.168.170.120	TCP	1354	80 → 52110 [ACK] Seq=1301 Ack=480 Win=30336 Len=1300 [TCP segment of a reassembled PDU]
3355	4.463968	192.168.170.120	128.119.245.12	TCP	54	52110 → 80 [ACK] Seq=480 Ack=2601 Win=66048 Len=0
3356	4.464257	128.119.245.12	192.168.170.120	TCP	1354	80 → 52110 [ACK] Seq=2601 Ack=480 Win=30336 Len=1300 [TCP segment of a reassembled PDU]

4. file5.html



Questions:

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

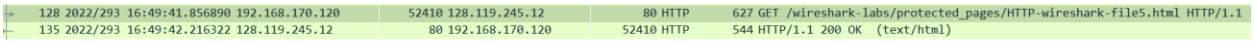


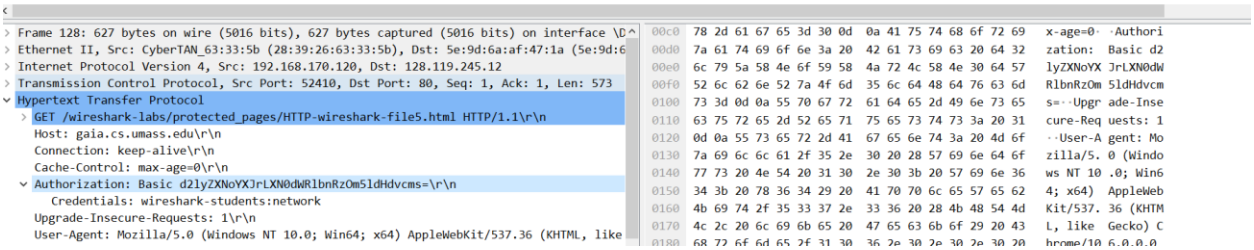
For the initial HTTP GET message the server's response was,

Status code = 401

Phrase = Unauthorized, because when opening the webpage initially it asks for username and password. This status appears because the credentials were not entered.

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





For the second HTTP GET message a new field called Authorization is added, because the user has entered the username and password and gained access to the webpage.

RESULT:

Hence the http protocol and packets were successfully analyzed with Wireshark.