21CY681 - INTERNET PROTOCOL LAB – III

Name: Ramya Ajay **Date: 26th October 2022**

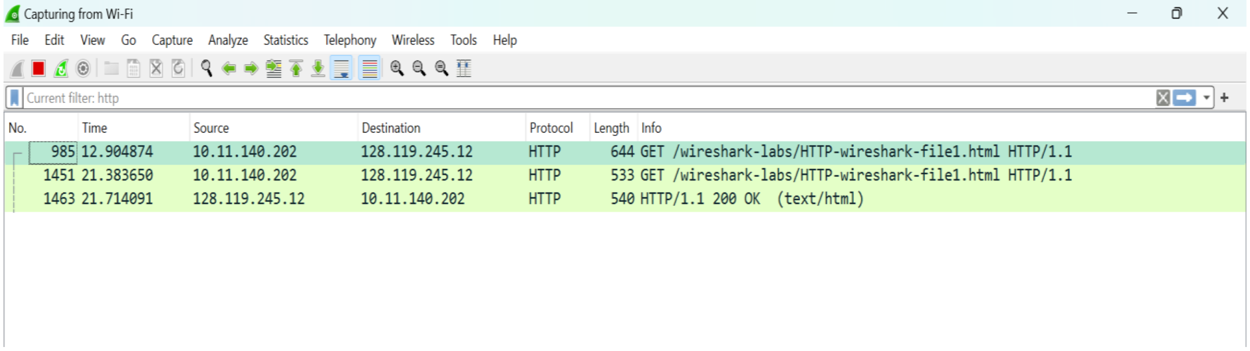
Roll No: CB. EN.P2CYS22004

AIM: ANALYSE VARIOUS HTTP PACKETS AND PROTOCOL USING WIRESHARK

1)Questions:

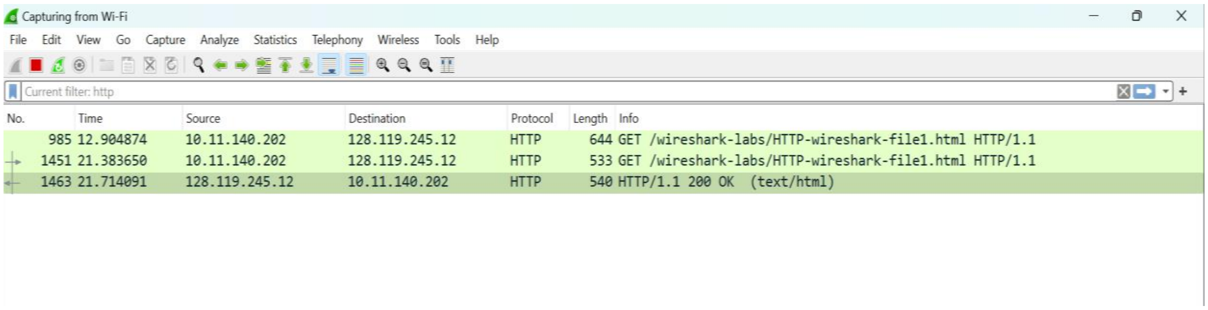
Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is theserver running?

Ans:My browser is running HTTP version 1.1.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
985	12.904874	10.11.140.202	128.119.245.12	HTTP	644	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1451	21.383650	10.11.140.202	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1463	21.714091	128.119.245.12	10.11.140.202	HTTP	540	HTTP/1.1 200 OK (text/html)

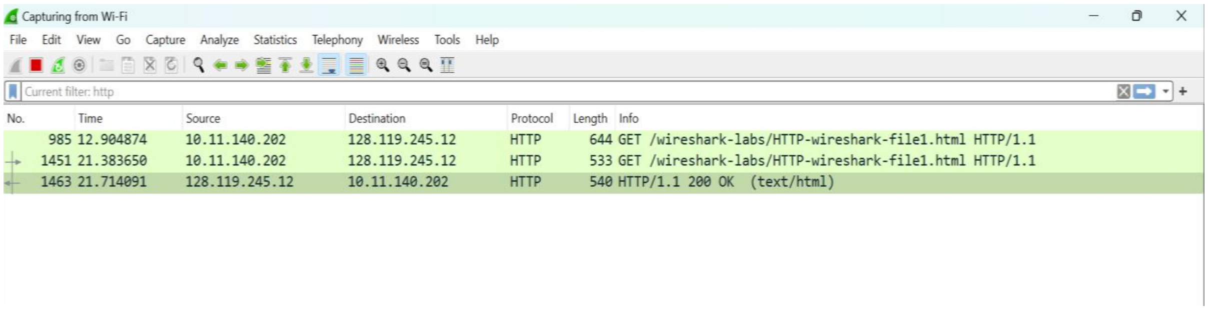
What languages (if any) do your browser indicate that it can accept to theserver? 3.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
985	12.904874	10.11.140.202	128.119.245.12	HTTP	644	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1451	21.383650	10.11.140.202	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1463	21.714091	128.119.245.12	10.11.140.202	HTTP	540	HTTP/1.1 200 OK (text/html)

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

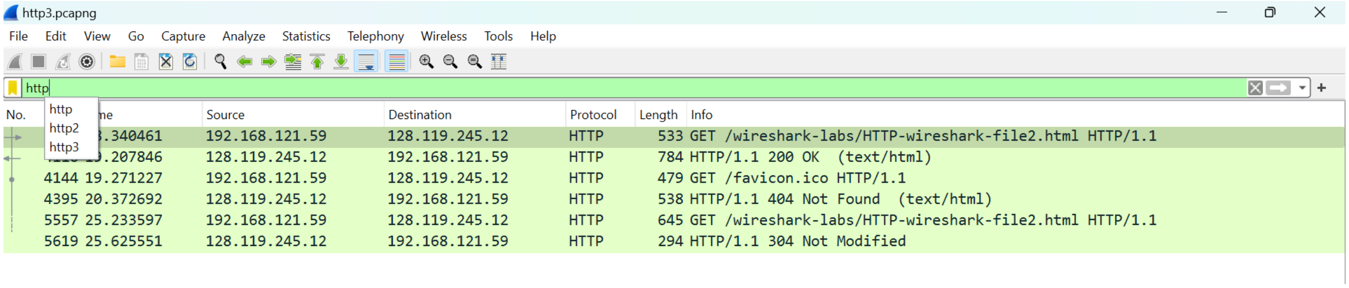
Answer: 10.11.140.202


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
985	12.904874	10.11.140.202	128.119.245.12	HTTP	644	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1451	21.383650	10.11.140.202	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1463	21.714091	128.119.245.12	10.11.140.202	HTTP	540	HTTP/1.1 200 OK (text/html)

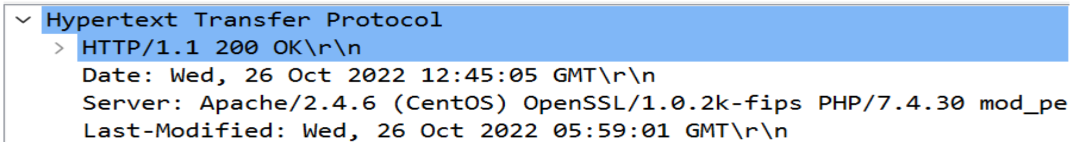
What is the status code returned from the server to your browser?

Answer: 304 -Not Modified


http3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3

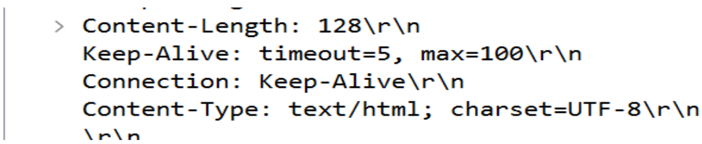
```
No.   me          Source           Destination      Protocol  Length Info
      3.340461    192.168.121.59   128.119.245.12   HTTP       533 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
      .207846     128.119.245.12   192.168.121.59   HTTP       784 HTTP/1.1 200 OK  (text/html)
4144 19.271227    192.168.121.59   128.119.245.12   HTTP       479 GET /favicon.ico HTTP/1.1
4395 20.372692    128.119.245.12   192.168.121.59   HTTP       538 HTTP/1.1 404 Not Found  (text/html)
5557 25.233597    192.168.121.59   128.119.245.12   HTTP       645 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
5619 25.625551    128.119.245.12   192.168.121.59   HTTP       294 HTTP/1.1 304 Not Modified
```

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: Wed, 26 Oct 2022 12:45:05 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_pe
  Last-Modified: Wed, 26 Oct 2022 05:59:01 GMT\r\n
```

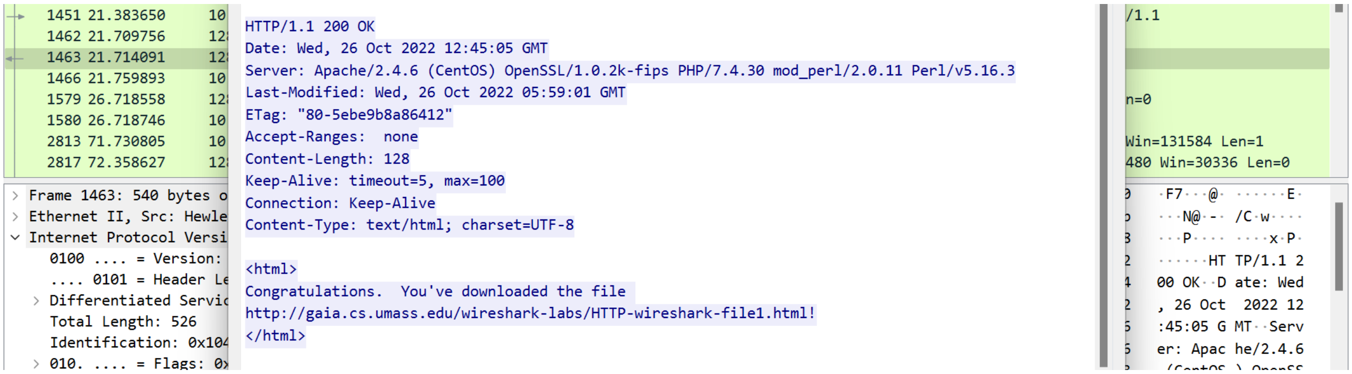
How many bytes of content are being returned to your browser?



```
  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
```

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.

Ans: No new data is displayed.



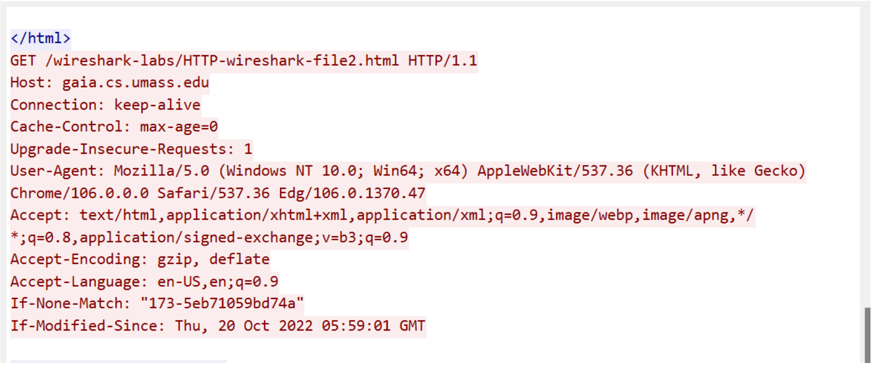
```
1451 21.383650   10
1462 21.709756   12
1463 21.714091   12
1466 21.759893   10
1579 26.718558   12
1580 26.718746   10
2813 71.730805   10
2817 72.358627   12

Frame 1463: 540 bytes o
Ethernet II, Src: Hewle
Internet Protocol Versi
   0100 .... = Version:
   .... 0101 = Header Le
   Differentiated Servic
   Total Length: 526
   Identification: 0x104
   010. .... = Flags: 0x
```

```
HTTP/1.1 200 OK
Date: Wed, 26 Oct 2022 12:45:05 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
Last-Modified: Wed, 26 Oct 2022 05:59:01 GMT
ETag: "80-5ebe9b8a86412"
Accept-Ranges: none
Content-Length: 128
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
Congratulations.  You've downloaded the file
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!
</html>
```

```
/1.1


n=0

Win=131584 Len=1
480 Win=30336 Len=0

0   ·F7···@·  ······E·
b   ···N@·-·  /C·w····
3   ···P····  ····x·P·
2   ······HT  TP/1.1 2
4   00 OK··D  ate: Wed
2   , 26 Oct   2022 12
5   :45:05 G  MT··Serv
5   er: Apac  he/2.4.6
```

2)Questions:

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



```
</html>
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 Edg/106.0.1370.47
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
```

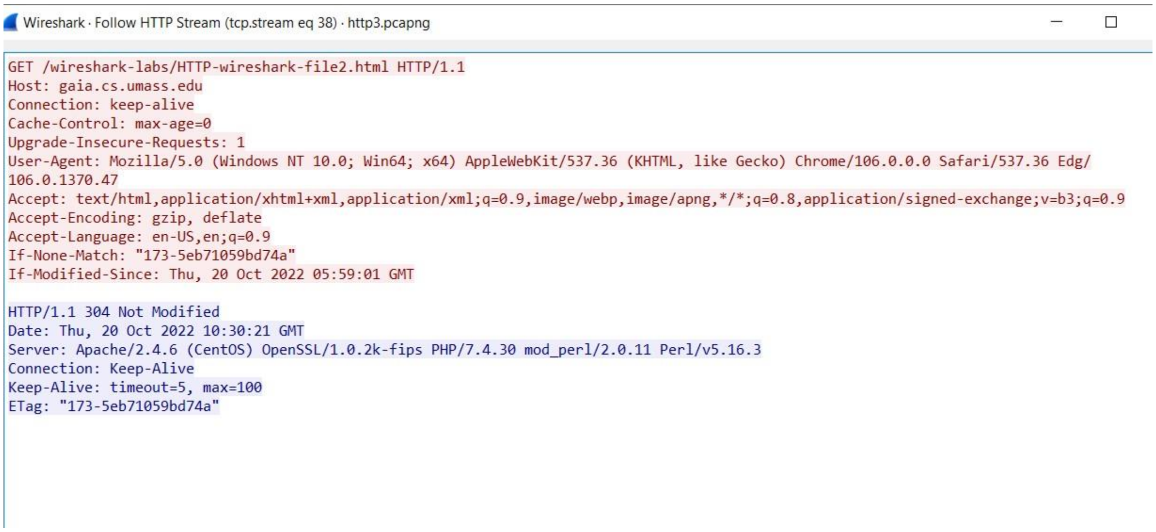
Inspect the contents of the server response. Did the server explicitly returnthe contents of the file? How can you tell?

Ans: Yes, the server explicitly returns the contents of the file because server storescache data while first time loading into the browser and every time use that data while the same request generates redundantly.

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?

Ans:As the server is using the cache data for loading the html file, “IF-MODIFIED-SINCE” will show first time and date value when file was first time run into the browser.

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’scontents? Explain.

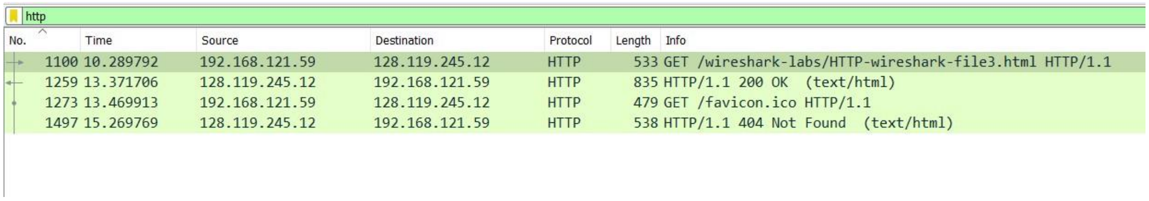

Wireshark · Follow HTTP Stream (tcp.stream eq 38) · http3.pcapng

```
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 Edg/
106.0.1370.47
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 10:30:21 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"
```

Ans:Yes, As we have not modified the file the 304-Not Modified code willreturned. And server will explicitly return the file content.

3)Questions:

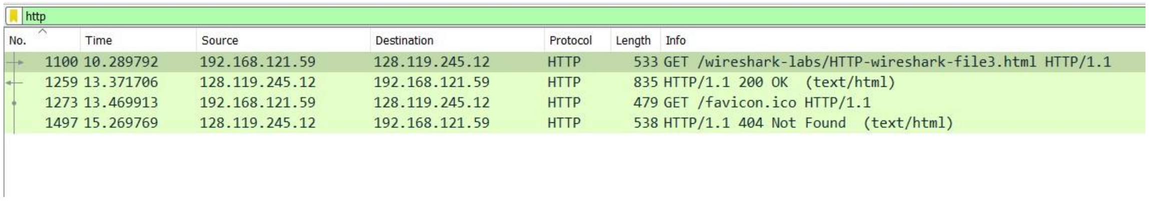
How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?



```
No.   Time       Source           Destination      Protocol  Length  Info
1100 10.289792   192.168.121.59   128.119.245.12   HTTP        533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1259 13.371706   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)
```

Ans:We are getting here two http requests. The first packet in the trace contains the GET message for the Bill or Rights.

Which packet number in the trace contains the status code and phraseassociated with the response to the HTTP GET request?


http

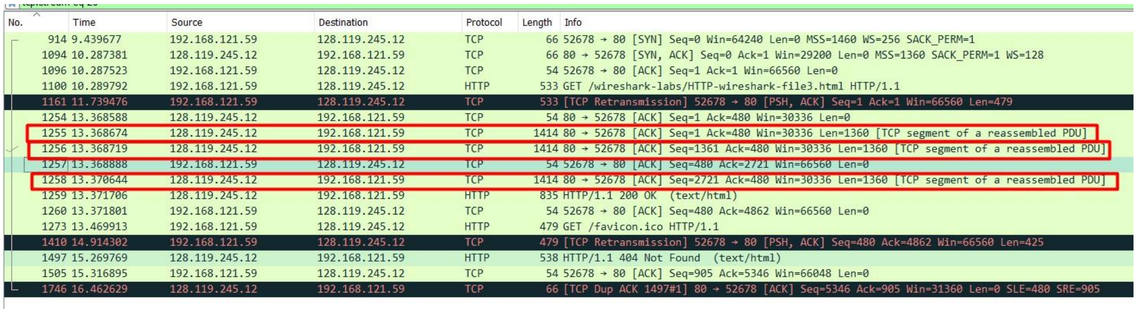
```
No.   Time       Source           Destination      Protocol  Length  Info
1100 10.289792   192.168.121.59   128.119.245.12   HTTP        533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1259 13.371706   128.119.245.12   192.168.121.59   HTTP        835 HTTP/1.1 200 OK  (text/html)
1273 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)
```

The second packet in the trace contains the status code 200 and phrase OKwith the response to the HTTP GET request.

What is the status code and phrase in the response?

Ans:Status code – 200 and Phrase – OK

How many data-containing TCP segments were needed to carry the singleHTTP response and the text of the Bill of Rights?



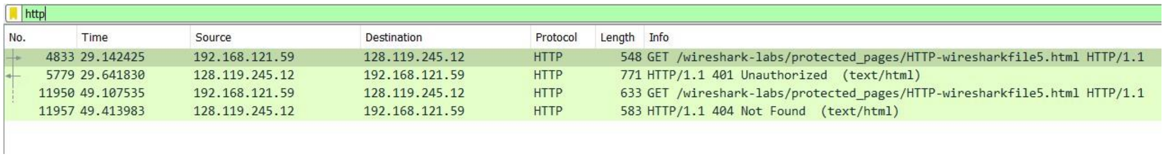
No.	Time	Source	Destination	Protocol	Length	Info
914	9.439677	192.168.121.59	128.119.245.12	TCP	66	52678 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1094	10.287381	128.119.245.12	192.168.121.59	TCP	66	80 → 52678 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=128
1096	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)
1260	13.371801	192.168.121.59	128.119.245.12	TCP	54	52678 → 80 [ACK] Seq=480 Ack=4862 Win=66560 Len=0
1273	13.469913	192.168.121.59	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
1410	14.914302	192.168.121.59	128.119.245.12	TCP	479	[TCP Retransmission] 52678 → 80 [PSH, ACK] Seq=480 Ack=4862 Win=66560 Len=425
1497	15.269769	128.119.245.12	192.168.121.59	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1505	15.316895	192.168.121.59	128.119.245.12	TCP	54	52678 → 80 [ACK] Seq=905 Ack=5346 Win=66048 Len=0
1746	16.462629	128.119.245.12	192.168.121.59	TCP	66	[TCP Dup ACK 1497#1] 80 → 52678 [ACK] Seq=5346 Ack=905 Win=31360 Len=0 SLE=480 SRE=905

Ans:There are 3 TCP segments are there between the HTTP request and responsewhich are having the length greater than zero. So, these are the TCP segments which are carrying the HTTP response.

4)Questions:

What is the server's response (status code and phrase) in response to the

Initial HTTP GET message from your browser?

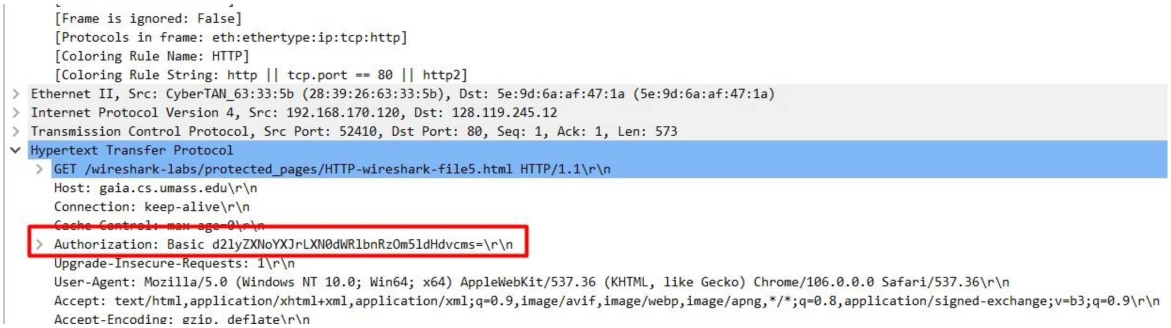


http

No.	Time	Source	Destination	Protocol	Length	Info
4833	29.142425	192.168.121.59	128.119.245.12	HTTP	548	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
5779	29.641830	128.119.245.12	192.168.121.59	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
11950	49.107535	192.168.121.59	128.119.245.12	HTTP	633	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
11957	49.413983	128.119.245.12	192.168.121.59	HTTP	583	HTTP/1.1 404 Not Found (text/html)

Ans:We are getting 401 Unauthorized segment as the server's response to theinitial HTTP GET message from my browser.

When your browser sends the HTTP GET message for the second time, whatnew field is included in the HTTP GET message?



```
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: CyberTAN_63:33:5b (28:39:26:63:33:5b), Dst: 5e:9d:6a:af:47:1a (5e:9d:6a:af:47:1a)
Internet Protocol Version 4, Src: 192.168.170.120, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52410, Dst Port: 80, Seq: 1, Ack: 1, Len: 573
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\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 (KHTML, like Gecko) Chrome/106.0.0.0 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
```

Ans:We can get the authorization type and the encoded Username and Password for the HTTP.