

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

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main packet list pane shows a list of captured packets, with the following details visible:

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)

The packet details pane for the selected packet (No. 2241) shows the following structure:

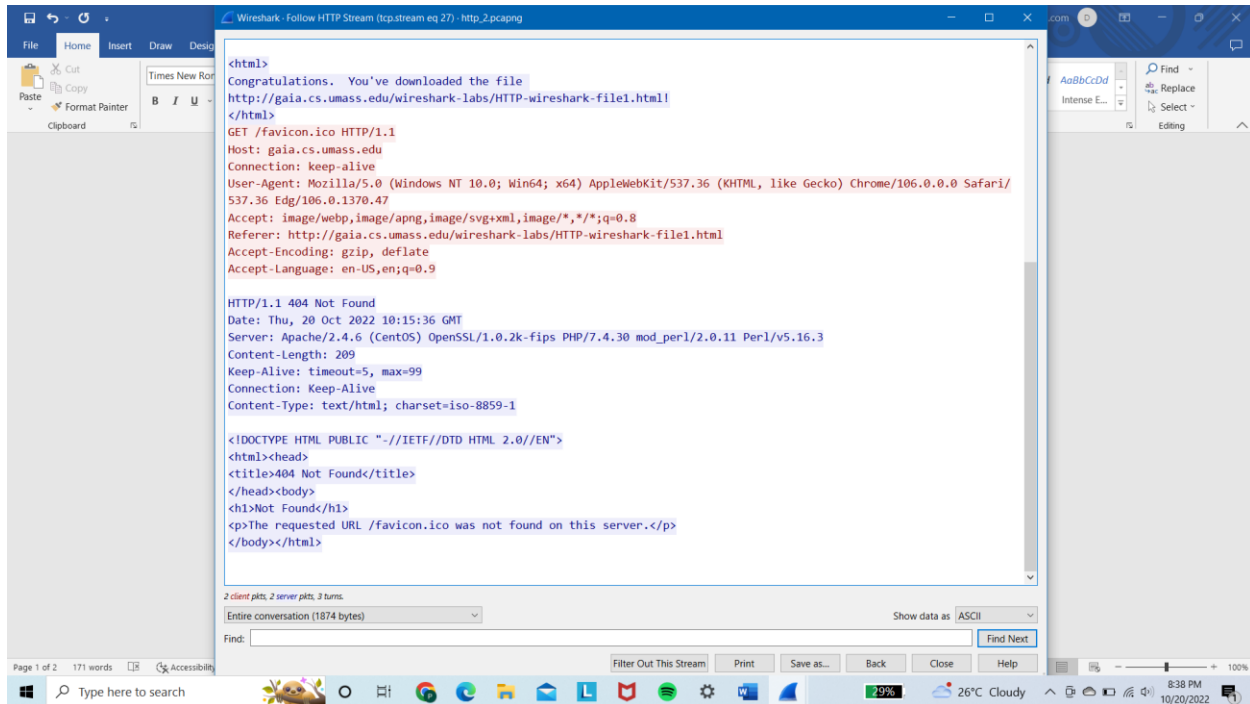
- Frame 2241: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF{...}
- Ethernet II, Src: Se9d:6a:af:47:1a (Se9d:6a:af:47:1a), Dst: CyberTAN_63:33:5b (28:39:26:33:5b:28)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.170.120
- Transmission Control Protocol, Src Port: 80, Dst Port: 56584, Seq: 1, Ack: 480, Len: 486
- Hypertext Transfer Protocol
- Line-based text data: text/html (4 lines)

The packet bytes pane shows the raw data of the packet, including the HTTP request line: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

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

sub2_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
35	2022/293	15:59:04.880380	192.168.170.120	56782	128.119.245.12	80 HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
39	2022/293	15:59:05.389137	128.119.245.12	80	192.168.170.120	56782 HTTP	784	HTTP/1.1 200 OK (text/html)
942	2022/293	15:59:17.847778	192.168.170.120	56781	128.119.245.12	80 HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1256	2022/293	15:59:20.108515	192.168.170.120	56795	128.119.245.12	80 HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1546	2022/293	15:59:20.206201	128.119.245.12	80	192.168.170.120	56781 HTTP	294	HTTP/1.1 304 Not Modified
2114	2022/293	15:59:20.419139	128.119.245.12	80	192.168.170.120	56795 HTTP	784	HTTP/1.1 200 OK (text/html)
3015	2022/293	15:59:22.954408	192.168.170.120	56795	128.119.245.12	80 HTTP	645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
3033	2022/293	15:59:23.243699	128.119.245.12	80	192.168.170.120	56795 HTTP	293	HTTP/1.1 304 Not Modified

< Frame 942: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF...
> 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: 56781, Dst Port: 80, Seq: 1, Ack: 1, Len: 584
> Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4759.100 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\nIf-None-Match: "173-5eb71059bd74a"\r\nIf-Modified-Since: Thu, 20 Oct 2022 05:59:01 GMT\r\n\r\n0000 5e 9d 6a af 47 1a 28 39 26 63 33 5b 08 00 45 00 ^j.G(9 &c3[...E
0010 02 70 a7 ff 40 00 80 06 6f e3 c0 a8 aa 78 80 77 .p:@...o...x-w
0020 f5 0c dd cd 00 50 a9 0e 4b 6f 04 31 a9 df 50 18P...Ko-1..P-
0030 01 02 c8 2b 00 00 47 45 54 20 2f 77 69 72 65 73GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 ireshark -file2.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1-Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu..C connectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 n: keep-alive..C
00a0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 ache-Con trol: ma
00b0 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 65 x-age=0..Upgrade
00c0 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 -Insecur e-Reques
00d0 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e ts: 1..U ser-Agen
00e0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
00f0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;

sub2_http.pcapng

Packets: 3046 - Displayed: 8 (0.3%)

Profile: Default

9:54 PM 10/20/2022

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?

No.	Time	Source	Source port	Destination	Destn port	Protocol	Length	Info
35	2022/293 15:59:04.880	380 192.168.170.120	56782	128.119.245.12	80	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
39	2022/293 15:59:05.389	137 128.119.245.12	80	192.168.170.120	56782	HTTP	784	HTTP/1.1 200 OK (text/html)
942	2022/293 15:59:17.847	778 192.168.170.120	56781	128.119.245.12	80	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1256	2022/293 15:59:20.108	515 192.168.170.120	56795	128.119.245.12	80	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1546	2022/293 15:59:20.206	201 128.119.245.12	80	192.168.170.120	56781	HTTP	294	HTTP/1.1 304 Not Modified
2114	2022/293 15:59:20.419	139 128.119.245.12	80	192.168.170.120	56795	HTTP	784	HTTP/1.1 200 OK (text/html)
3015	2022/293 15:59:22.954	408 192.168.170.120	56795	128.119.245.12	80	HTTP	645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
3033	2022/293 15:59:23.243	699 128.119.245.12	80	192.168.170.120	56795	HTTP	293	HTTP/1.1 304 Not Modified

> Frame 35: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF...	0000	5e 9d 6a af 47 1a 28 39 26 63 33 5b 08 00 45 00	^j-G(9&c3[...E-
> 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)	0010	02 00 a7 f1 40 00 80 06 70 61 c0 a8 aa 78 80 77	...@... pa...x-w
> Internet Protocol Version 4, Src: 192.168.170.120, Dst: 128.119.245.12	0020	f5 0c dd ce 00 50 63 84 c0 ac 44 aa ed 6e 50 18	...Pc...D...nP-
> Transmission Control Protocol, Src Port: 56782, Dst Port: 80, Seq: 1, Ack: 1, Len: 472	0030	01 02 ff 72 00 00 47 45 54 20 2f 77 69 72 65 73	...-GE T /wires
> Hypertext Transfer Protocol	0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77	hark-lab s/HTTP-w
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n	0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68	irshark -file2.h
Host: gaia.cs.umass.edu\r\n	0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f	tml HTTP /1.1·Ho
Connection: keep-alive\r\n	0070	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73	st: gaia .cs.umas
Upgrade-Insecure-Requests: 1\r\n	0080	73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f	s.edu·C connectio
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	0090	6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55	n: keep-alive·U
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	00a0	70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d	pgrade-I nsecure-
Accept-Encoding: gzip, deflate	00b0	52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65	Requests : 1·Use
Accept-Language: en-US,en;q=0.9\r\n\r\n	00c0	72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61	r-Agent: Mozilla

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?

The image shows a Wireshark packet capture of an HTTP GET request and its response. The packet list on the left shows the request (Frame 35) and the response (Frame 39). The packet details pane for the response (Frame 39) is expanded, showing the following information:

- Host: gaia.cs.umass.edu
- Connection: keep-alive
- 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
- HTTP/1.1 200 OK
- Date: Thu, 20 Oct 2022 10:29:05 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: Thu, 20 Oct 2022 05:59:01 GMT
- ETag: "173-5eb71059bd74a"
- Accept-Ranges: bytes
- Content-Length: 371
- Keep-Alive: timeout=5, max=100
- Connection: Keep-Alive
- Content-Type: text/html; charset=UTF-8

The packet bytes pane shows the raw HTTP response, including the status line and the beginning of the HTML body:

```
HTTP/1.1 200 OK
Date: Thu, 20 Oct 2022 10:29:05 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: Thu, 20 Oct 2022 05:59:01 GMT
ETag: "173-5eb71059bd74a"
Accept-Ranges: bytes
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
  <body>
    <p>Congratulations again! Now you've downloaded the file lab2-2.html. <br>
    This file's last modification date will not change. <p>
    This 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.
  </body>
</html>
```

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?

No.	Time	Source	Source port	Destination	Destn port	Protocol	Length	Info
35	2022/293	15:59:04.880380	192.168.170.120	56782	128.119.245.12	80 HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
39	2022/293	15:59:05.389137	128.119.245.12	80	192.168.170.120	56782 HTTP	784	HTTP/1.1 200 OK (text/html)
942	2022/293	15:59:17.847778	192.168.170.120	56781	128.119.245.12	80 HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1256	2022/293	15:59:20.108515	192.168.170.120	56795	128.119.245.12	80 HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1546	2022/293	15:59:20.206201	128.119.245.12	80	192.168.170.120	56781 HTTP	294	HTTP/1.1 304 Not Modified
2114	2022/293	15:59:20.419139	128.119.245.12	80	192.168.170.120	56795 HTTP	784	HTTP/1.1 200 OK (text/html)
3015	2022/293	15:59:22.954408	192.168.170.120	56795	128.119.245.12	80 HTTP	645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
3033	2022/293	15:59:23.243699	128.119.245.12	80	192.168.170.120	56795 HTTP	293	HTTP/1.1 304 Not Modified

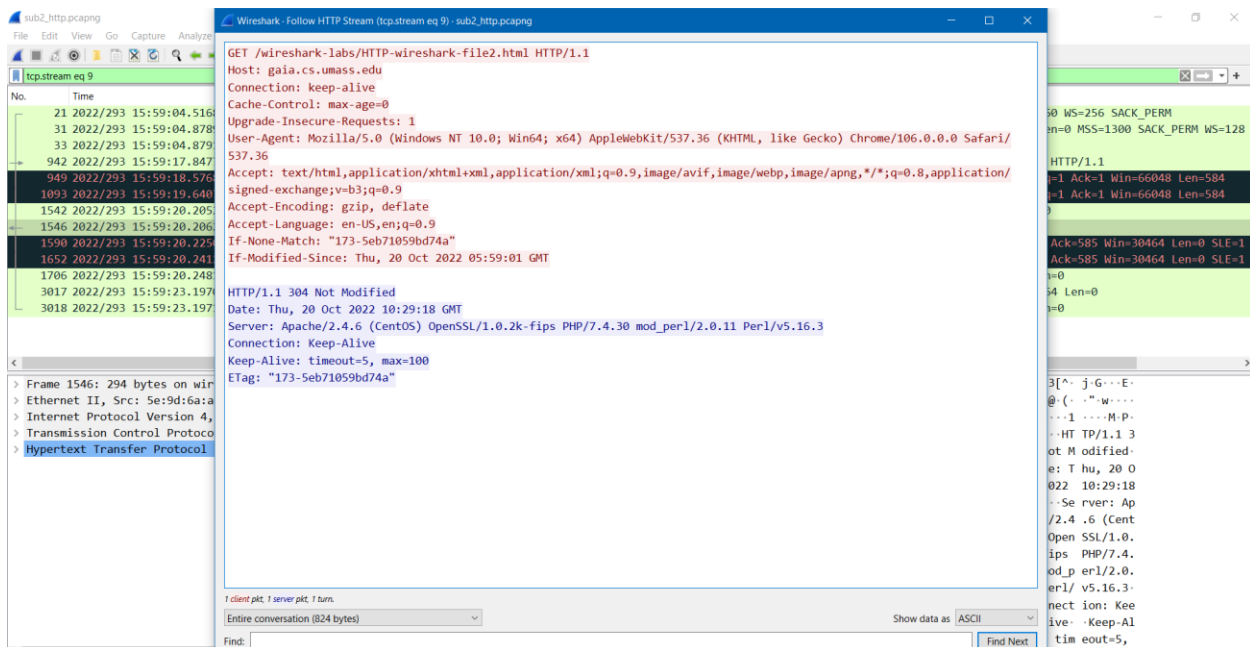
> Transmission Control Protocol, Src Port: 56781, Dst Port: 80, Seq: 1, Ack: 1, Len: 584	0000	5e 9d 6a af 47 1a 28 39	26 63 33 5b 08 00 45 00	^jG(9 &c3[...E:
> Hypertext Transfer Protocol	0010	02 70 a7 ff 40 00 80 06	6f e3 c0 a8 aa 78 80 77	·p·@... o...x·w
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n	0020	f5 0c dd cd 00 50 a9 0e	4b 6f 04 31 a9 df 50 18P· Ko-1·P·
Host: gaia.cs.umass.edu\r\n	0030	01 02 c8 2b 00 00 47 45	54 20 2f 77 69 72 65 73GE T /wires
Connection: keep-alive\r\n	0040	68 61 72 6b 2d 6c 61 62	73 2f 48 54 54 50 2d 77	hark-lab s/HTTP-w
Cache-Control: max-age=0\r\n	0050	69 72 65 73 68 61 72 6b	2d 66 69 6c 65 32 2e 68	reshark -file2.h
Upgrade-Insecure-Requests: 1\r\n	0060	74 6d 6c 20 48 54 54 50	2f 31 2e 31 0d 0a 48 6f	tml HTTP /1.1·Ho
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	0070	73 74 3a 20 67 61 69 61	2e 63 73 2e 75 6d 61 73	st: gaia .cs.umas
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i	0080	73 2e 65 64 75 0d 0a 43	6f 6e 6e 65 63 74 69 6f	s.edu·C onnectio
Accept-Encoding: gzip, deflate\r\n	0090	6e 3a 20 6b 65 65 70 2d	61 6c 69 76 65 0d 0a 43	n: keep- alive·C
Accept-Language: en-US,en;q=0.9\r\n	00a0	61 63 68 65 2d 43 6f 6e	74 72 6f 6c 3a 20 6d 61	ache-Con trol: ma
If-None-Match: "173-5eb71059bd74a"\r\n	00b0	78 2d 61 67 65 3d 30 0d	0a 55 70 67 72 61 64 65	x-age=0· Upgrade
If-Modified-Since: Thu, 20 Oct 2022 05:59:01 GMT\r\n	00c0	2d 49 6e 73 65 63 75 72	65 2d 52 65 71 75 65 73	-Insecur e-Reques

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'.

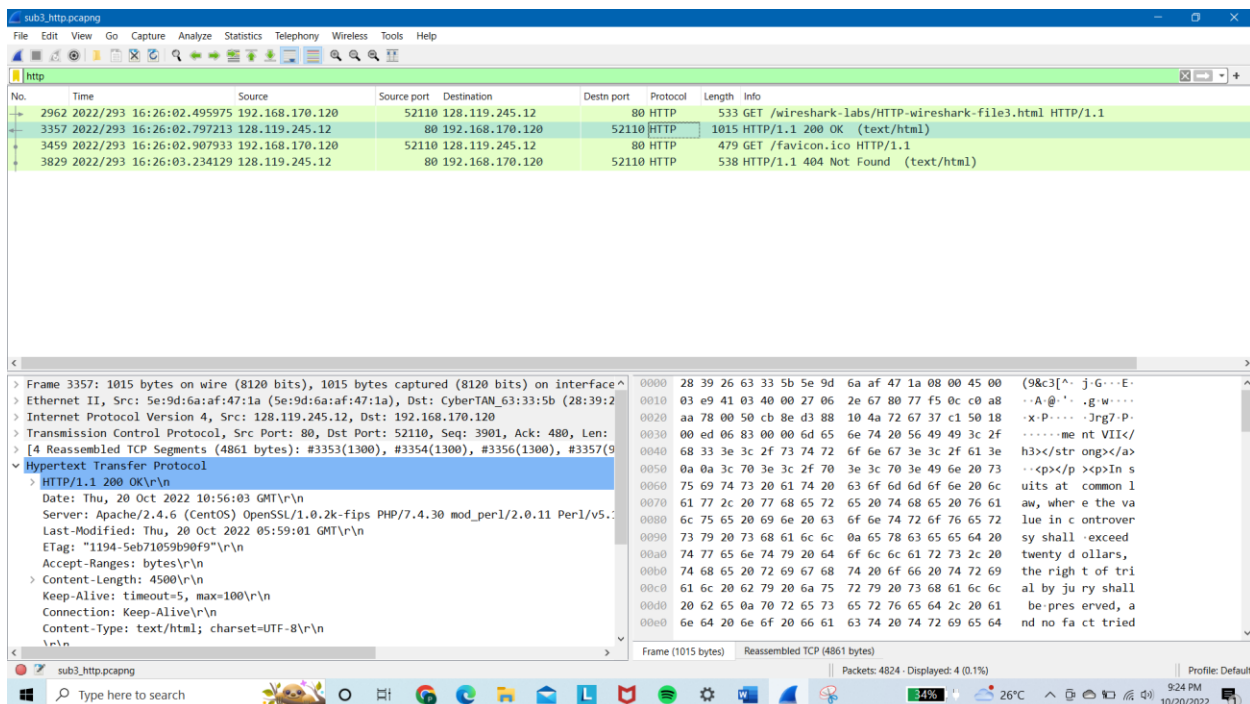
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the file's contents? Explain.

Status code: 304

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



3. file3.html



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

The image shows a Wireshark packet capture window titled 'password.pcapng'. The packet list on the left shows four packets. Packet 33 is a GET request to /wireshark-labs/protected_pages/HTTP-wireshark-file5.html. Packet 37 is the corresponding 401 Unauthorized response. The packet details pane for packet 37 shows the response structure: HTTP/1.1 401 Unauthorized (text/html). The packet bytes pane shows the raw data of the response, including the status line and headers.

No.	Time	Source	Source port	Destination	Destn port	Protocol	Length	Info
33	2022/293 16:49:22.452525	192.168.170.120	52409	128.119.245.12	80	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
37	2022/293 16:49:22.763598	128.119.245.12	80	192.168.170.120	52409	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
128	2022/293 16:49:41.856890	192.168.170.120	52410	128.119.245.12	80	HTTP	627	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
135	2022/293 16:49:42.216322	128.119.245.12	80	192.168.170.120	52410	HTTP	544	HTTP/1.1 200 OK (text/html)

Questions:

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

The image shows a Wireshark packet capture window titled 'http'. The packet list on the left shows two packets. Packet 33 is a GET request to /wireshark-labs/protected_pages/HTTP-wireshark-file5.html. Packet 37 is the corresponding 401 Unauthorized response. The packet details pane for packet 37 shows the response structure: HTTP/1.1 401 Unauthorized (text/html).

No.	Time	Source	Source port	Destination	Destn port	Protocol	Length	Info
33	2022/293 16:49:22.452525	192.168.170.120	52409	128.119.245.12	80	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
37	2022/293 16:49:22.763598	128.119.245.12	80	192.168.170.120	52409	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

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?

128	2022/293	16:49:41.856890	192.168.170.120	52410	128.119.245.12	80	HTTP	627	GET	/wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1
135	2022/293	16:49:42.216322	128.119.245.12	80	192.168.170.120	52410	HTTP	544	HTTP/1.1	200 OK (text/html)	

```
> Frame 128: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface vD\
> Ethernet II, Src: CyberTAN_63:33:5b (28:39:26:63:33:5b), Dst: Se:9d:6a:af:47:1a (Se:9d:6
> Internet Protocol Version 4, Src: 192.168.170.120, Dst: 189.128.245.12
> 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=
      Credentials: wireshark-students:network
      Upgrade-Insecure-Requests: 1/r/n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
```

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.