



LAB 2



Name : Eslam Mostafa Mohamed

ID : 20p4797

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

-1.1

- 1.1

```
> Transmission Control Protocol, Src Port: 55816, Dst Port: 80, Seq: 1, Ack: 1, Len: 600
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n
    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\r\n
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
```

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

-English - Arabic

```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,ar;q=0.8\r\n
If-None-Match: "51-60870091f059a"\r\n
```

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

- For my computer 192.168.0.100
- For the server 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
115	33.666470	192.168.0.100	128.119.245.12	HTTP	654	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
126	33.834701	128.119.245.12	192.168.0.100	HTTP	293	HTTP/1.1 304 Not Modified
2982	116.922463	192.168.0.100	102.132.97.55	HTTP	59	POST /chat HTTP/1.1
19303	461.504955	192.168.0.100	102.132.97.55	HTTP	59	POST /chat HTTP/1.1

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

- 200

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
```

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

```
Date: Tue, 24 Oct 2023 18:42:05 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 24 Oct 2023 05:59:02 GMT\r\n
ETag: "51-60870091f059a"\r\n
```

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

```
Accept-Ranges: bytes\r\n
> Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
```

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.

- All found

0000	98 da c4 c7 e4 0c 9c 29	76 f2 4d d3 08 00 45 00) v-M...E-
0010	02 80 1f 35 40 00 80 06	00 00 c0 a8 00 64 80 77	...5@... ..d-w
0020	f5 0c e0 8f 00 50 3b 1f	2d e7 7b b4 28 d0 50 18P;- --{-(.P-
0030	02 00 39 03 00 00 47 45	54 20 2f 77 69 72 65 73	..9...GE T /wires
0040	68 61 72 6b 2d 6c 61 62	73 2f 49 4e 54 52 4f 2d	hark-lab s/INTRO-
0050	77 69 72 65 73 68 61 72	6b 2d 66 69 6c 65 31 2e	wireshar k-file1.
0060	68 74 6d 6c 20 48 54 54	50 2f 31 2e 31 0d 0a 48	html HTTP/1.1..H
0070	6f 73 74 3a 20 67 61 69	61 2e 63 73 2e 75 6d 61	ost: gai a.cs.uma
0080	73 73 2e 65 64 75 0d 0a	43 6f 6e 6e 65 63 74 69	ss.edu..Connecti
0090	6f 6e 3a 20 6b 65 65 70	2d 61 6c 69 76 65 0d 0a	on: keep -alive..
00a0	43 61 63 68 65 2d 43 6f	6e 74 72 6f 6c 3a 20 6d	Cache-Co ntrol: m
00b0	61 78 2d 61 67 65 3d 30	0d 0a 55 70 67 72 61 64	ax-age=0 ..Upgrad
00c0	65 2d 49 6e 73 65 63 75	72 65 2d 52 65 71 75 65	e-Insecu re-Reque
00d0	73 74 73 3a 20 31 0d 0a	55 73 65 72 2d 41 67 65	sts: 1.. User-Age
00e0	6e 74 3a 20 4d 6f 7a 69	6c 6c 61 2f 35 2e 30 20	nt: Mozi lla/5.0
00f0	28 57 69 6e 64 6f 77 73	20 4e 54 20 31 30 2e 30	(Windows NT 10.0
0100	3b 20 57 69 6e 36 34 3b	20 78 36 34 29 20 41 70	; Win64; x64) Ap
0110	70 6c 65 57 65 62 4b 69	74 2f 35 33 37 2e 33 36	pleWebKi t/537.36

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

```
[Severity level: Critical]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Tue, 24 Oct 2023 18:42:05 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 24 Oct 2023 05:59:02 GMT\r\n
ETag: "51-60870091f059a"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 81\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
[HTTP response 1/1]
```

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

- Yes from content length and there was message saying ok (html/file)

```
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Tue, 24 Oct 2023 18:42:05 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 24 Oct 2023 05:59:02 GMT\r\n
ETag: "51-60870091f059a"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 81\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
[HTTP response 1/1]
```

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? If so, what information follows the "IF-MODIFIED-SINCE:" header?

```
Accept-Language: en-US,en;q=0.9,ar;q=0.8\r\n
If-None-Match: "51-60870091f059a"\r\n
If-Modified-Since: Tue, 24 Oct 2023 05:59:02 GMT\r\n
\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 contents of the file? Explain

- the server explicitly didn't return the contents of the file

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 304 Not Modified\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      [HTTP/1.1 304 Not Modified\r\n]
```

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?

- One
- 29

No.	Time	Source	Destination	Protocol	Length	Info
29	8.968485	192.168.0.100	128.119.245.12	HTTP	542	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
47	9.146719	128.119.245.12	192.168.0.100	HTTP	775	HTTP/1.1 200 OK (text/html)

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

- 49

No.	Time	Source	Destination	Protocol	Length	Info
29	8.968485	192.168.0.100	128.119.245.12	HTTP	542	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
47	9.146719	128.119.245.12	192.168.0.100	HTTP	775	HTTP/1.1 200 OK (text/html)

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

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
```

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

- 4

```
▼ [4 Reassembled TCP Segments (4861 bytes): #44(1380), #45(1380), #46(1380), #47(721)]
  [Frame: 44, payload: 0-1379 (1380 bytes)]
  [Frame: 45, payload: 1380-2759 (1380 bytes)]
  [Frame: 46, payload: 2760-4139 (1380 bytes)]
  [Frame: 47, payload: 4140-4860 (721 bytes)]
  [Segment count: 4]
```

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

- 3 messages
- 192.168.0.100

Time	Source	Destination	Protocol	Length	Info
273.23.062890	192.168.0.100	128.119.245.12	HTTP	542	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
275.23.228763	128.119.245.12	192.168.0.100	HTTP	1355	HTTP/1.1 200 OK (text/html)
277.23.282482	192.168.0.100	128.119.245.12	HTTP	488	GET /pearson.png HTTP/1.1

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

- Serially

275.23.228763	128.119.245.12	192.168.0.100	HTTP	1355	HTTP/1.1 200 OK (text/html)
277.23.282482	192.168.0.100	128.119.245.12	HTTP	488	GET /pearson.png HTTP/1.1
281.23.365604	192.168.0.100	178.79.137.164	HTTP	455	GET /8E_cover_small.jpg HTTP/1.1
285.23.450251	128.119.245.12	192.168.0.100	HTTP	905	HTTP/1.1 200 OK (PNG)
287.23.450774	178.79.137.164	192.168.0.100	HTTP	225	HTTP/1.1 301 Moved Permanently

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

- 401 unauthorized

```
558 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
771 HTTP/1.1 401 Unauthorized (text/html)
```

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

252.60.637686	192.168.0.100	128.119.245.12	HTTP	643	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
257.60.805212	128.119.245.12	192.168.0.100	HTTP	544	HTTP/1.1 200 OK (text/html)

```
▼ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\r\n
  Credentials: wireshark-students:network
  Upgrade-Insecure-Requests: 1\r\n
```