## CS-315: COMPUTER NETWORKS LAB ASSIGNMENT 3

## PART-1:

 My browser is running http version 1.1 and the server is also running http version 1.1 =>

```
Frame 62: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interf
Ethernet II, Src: IntelCor_1f:79:8a (20:c1:9b:1f:79:8a), Dst: Cisco_0a:9a:e1 (44:
Internet Protocol Version 4, Src: 10.240.16.46, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57120, Dst Port: 80, Seq: 1, Ack: 1, Ler
- Hypertext Transfer Protocol
     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      Fig. [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
     Host: gaia.cs.umass.edu\r\n
     User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) Gecko/20100101 F:
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
     Accept-Language: en-US, en; q=0.5\r\n
     Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
     Upgrade-Insecure-Requests: 1\r\n
Frame 66: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interf Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: IntelCor_1f:79:8a (20: Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.240.16.46

Transmission Control Protocol, Src Port: 80, Dst Port: 57120, Seq: 1, Ack: 390, L
- Hypertext Transfer Protocol
   + HTTP/1.1 200 OK\r\n
      | [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
         [Status Code Description: OK]
        Response Phrase: OK
     Date: Mon, 22 Jan 2024 12:34:39 GMT\r\n
     Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Pe
     Last-Modified: Mon, 22 Jan 2024 06:59:02 GMT\r\n
     ETag: "80-60f835d62e850"\r\n
     Accept-Ranges: bytes\r\n
   Content-Length: 128\r\n
     Keep-Alive: timeout=5, max=100\r\n
```

Accepted-Languages: en-US, en

Accept-Language: en-US, en; q=0.5\r\n

3. My computer IP address: 10.240.16.46

IP address of gaia.cs.umass.edu server: 128.119.245.12

Source	Destination	
10.240.16.46	128.119.245.12	
128.119.245.12	10.240.16.46	

4. Status code: 200

```
HTTP/1.1 200 OK\r\n

| [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
| Response Version: HTTP/1.1
| Status Code: 200
| [Status Code Description: OK]
| Response Phrase: OK
```

5. The HTML file that I was retrieving was last modified on Mon, 22 Jan 2024 06:59:02 GMT.

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips Last-Modified: Mon, 22 Jan 2024 06:59:02 GMT\r\n

ETag: "80-60f835d62e850"\r\n

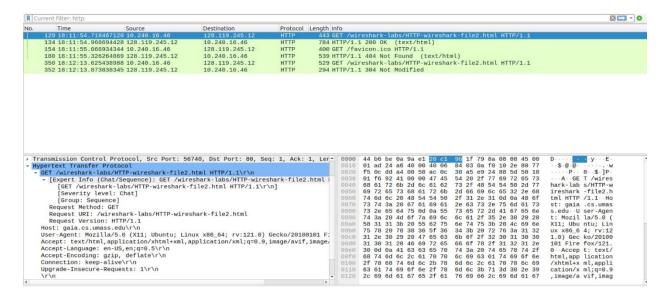
6. Size/Bytes of content = 128 bytes[can be seen below in the screenshot as content length]

```
[Status Code Description: OK]
      Response Phrase: OK
   Date: Mon, 22 Jan 2024 12:34:39 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 P€
   Last-Modified: Mon, 22 Jan 2024 06:59:02 GMT\r\n
   ETag: "80-60f835d62e850"\r\n
   Accept-Ranges: bytes\r\n
  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
    [HTTP response 1/1]
    [Time since request: 0.250192856 seconds]
    [Request in frame: 62]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.htm]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

7. No, all the headers are displayed in the packet listing window since here we can see all the content that we see on the web page of the given URL.

```
Line-based text data: text/html (4 lines)
   \langle html \rangle \backslash n
   Congratulations. You've downloaded the file \n
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
   </html>\n
65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d
                                                     et=UTF-8 ····<htm
6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f
                                                     l> Congr atulatio
                                                     ns. You 've down
6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e
6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20
                                                     loaded t he file
0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e
                                                     http:// gaia.cs.
75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68
                                                     umass.ed u/wiresh
61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69
                                                     ark-labs /HTTP-wi
72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74
                                                    reshark- file1.ht
6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a
                                                     ml! </ht ml>.
```

# PART-2:



- 1. No, there is no 'IF-MODIFIED-SINCE' line in the HTTP GET request as we can see above.
- 2. Yes, the server explicitly returns the contents of the file. As we can see a Line-based text data section which has the same content that we saw on the web page of the given URL.



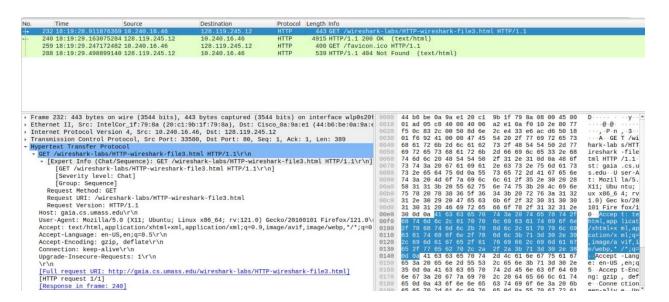
3. Yes, there is an 'IF-MODIFIED-SINCE' line in the HTTP GET. The information that follows the header is the time and date[can be seen below] of the last modification of the file from the previous get request.

```
Hypertext Transfer Protocol
   GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
   [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
   [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
   [Severity level: Chat]
   [Group: Sequence]
   Request Method: GET
   Request URI: /wireshark-labs/HTTP-wireshark-file2.html
   Request Version: HTTP/1.1
   Host: gaia.cs.umass.edu\r\n
   User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.6
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=Accept-Language: en-US,en;q=0.5\r\n
   Accept-Encoding: gzip, deflate\r\n
   Connection: keep-alive\r\n
   Upgrade-Insecure-Requests: 1\r\n
   If-Modified-Since: Mon, 22 Jan 2024 06:59:02 GMT\r\n
   If-None-Match: "173-60f835d62e080"\r\n
```

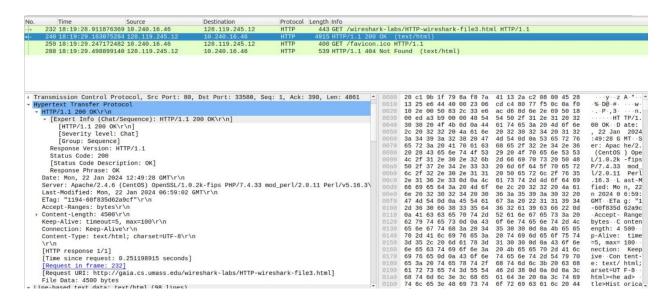
4. The status code and phrase returned from the server is 'HTTP/1.1 304 Not Modified'. No, the server didn't return the contents of the file as the browser loaded it from its cache.

# <u>PART-3:</u>

1. My browser sent one HTTP GET request message(ignoring the request for favicon). Packet number 232 in the trace contains the GET message for the Bill or Rights.



2. Packet number 240 in the trace contains the status code and phrase associated with the response to the HTTP GET request.



3. Status Code: 200; Phrase in the Response: OK [Can be seen above from the screenshot]

```
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]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK
```

4. The data was sent in 4 TCP segments to the browser, then reassembled.

```
Transmission Control Protocol, Src Port: 80, Dst Port: 63037, Seq: 3751, Ack: 473, Len: 1111 [4 Reassembled TCP Segments (4861 bytes): #232(1250), #233(1250), #234(1250), #235(1111)]
```

#### PART-4:

No.	Time	Source	Destination	Protocol	Length Info
+	240 18:41:16.0	86242871 10.240.16.46	128.119.245.12	HTTP	443 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
4-	244 18:41:16.4	26723125 128.119.245.12	10.240.16.46	HTTP	1355 HTTP/1.1 200 OK (text/html)
	259 18:41:16.5	95981801 10.240.16.46	128.119.245.12	HTTP	400 GET /pearson.png HTTP/1.1
	263 18:41:16.7	96884105 10.240.16.46	128.119.245.12	HTTP	400 GET /favicon.ico HTTP/1.1
	280 18:41:16.8	40127093 128.119.245.12	10.240.16.46	HTTP	3666 HTTP/1.1 200 OK (PNG)
	283 18:41:17.0	82193957 128.119.245.12	10.240.16.46	HTTP	539 HTTP/1.1 404 Not Found (text/html)
	308 18:41:19.8	94054962 10.240.16.46	178.79.137.164	HTTP	379 GET /8E cover_small.jpg HTTP/1.1
	323 18:41:20.0	86078361 178.79.137.164	10.240.16.46	HTTP	237 HTTP/1.1 301 Moved Permanently

- 1. My browser sent 3 HTTP GET request messages(ignoring the one for favicon). The internet addresses to which the GET requests were sent:
  - 1) 128.119.245.12 (1st GET Page Address)
  - 2) 128.119.245.12 (2<sup>nd</sup> GET pearson.png)
  - 3) 178.79.137.164 (3rd GET 8E\_cover\_small.jpg)

2. The browser downloaded the images serially because we can see from the screenshot above that the request for the second image was sent only after a response for the first image was received after sending the request for the first image, i.e., the second image was only requested after the first image came back. Also, the images were transmitted over two TCP connections, so we can say that they were downloaded serially.

## PART-5:

1. Status code: 401; Phrase: Unauthorized

```
→ Hypertext Transfer Protocol

→ HTTP/1.1 401 Unauthorized\r\n

→ [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]

Response Version: HTTP/1.1

Status Code: 401

[Status Code Description: Unauthorized]

Response Phrase: Unauthorized
```

As we can see in the screenshot below, a new field (Authorization) is included in the HTTP GET message=> Authorization: Basic