TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG
BỘ MÔN AN TOÀN THÔNG TIN

LAB REPORT 2

Subject: Computer Network

Topic: Sniffing HTTP traffic with Wireshark

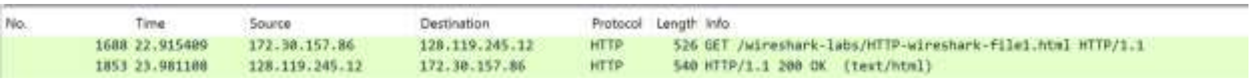
Student information	**Student 1** ID: 22520836 Name: Ngo Thi Hong Ly **Student 2** ID: 22521099 Name: Le Hoang Thien Phu **Student 3** ID: 22521237 Name: Pham Quang Dai Phuc **Student 4** ID: 22521240 Name: Le Minh Sang
Class	**CS4283.O21.CTTT.1**
Work division:	**[Student 1]**: Do the first task and support the other **[Student 2]**: Do the second task and support the other **[Student 1]**: Do the third task and support the other **[Student 2]**: Do the final task and support the other
Video link of implementation *(if required)*	
Opinions (if any) + Difficulties encountered + Suggestions, comments...	

[Report content – Export to .PDF file before submitting]

Task 1

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

   → Both my browser and the server are running HTTP version 1.1

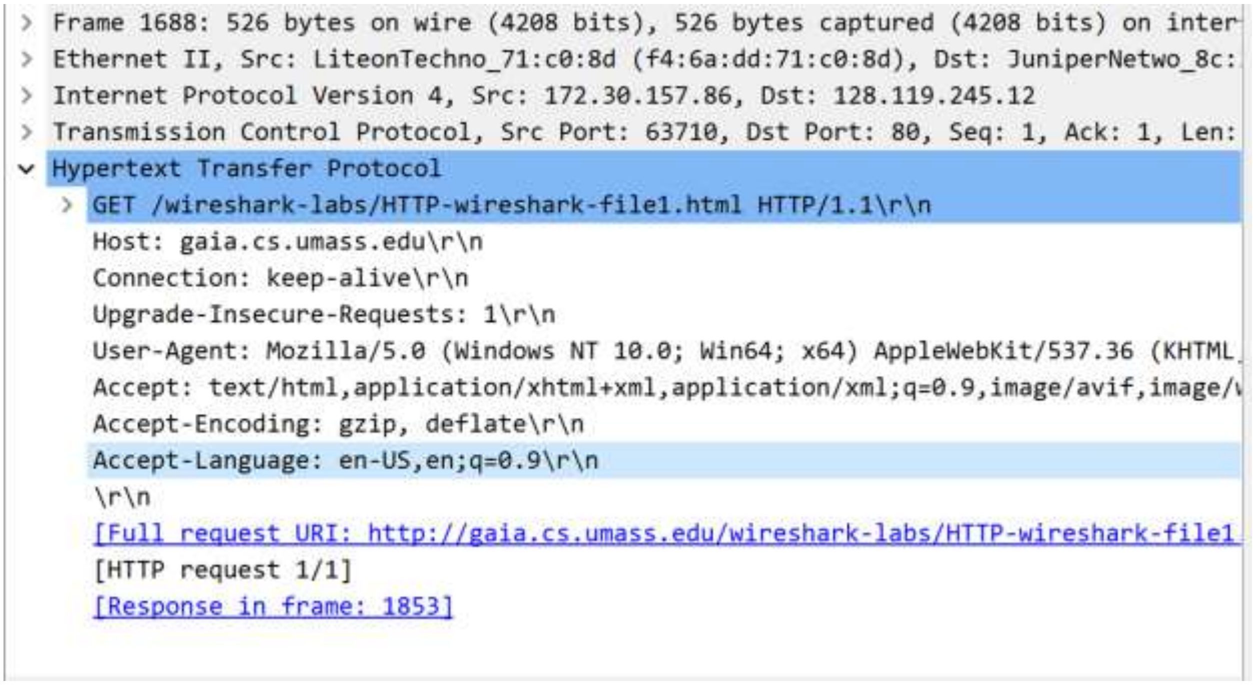


No.	Time	Source	Destination	Protocol	Length	Info
1688	22.915409	172.30.157.86	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1853	23.981100	128.119.245.12	172.30.157.86	HTTP	540	HTTP/1.1 200 OK (text/html)

Figure 1: Version of browser and server

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

   → Accept language: en-US,en;q=0.9\r\n



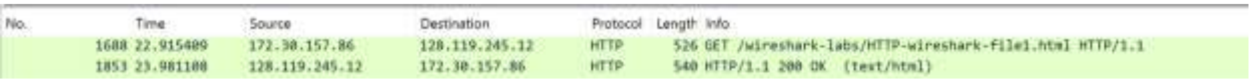
```
> Frame 1688: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on inter
> Ethernet II, Src: LiteonTechno_71:c0:8d (f4:6a:dd:71:c0:8d), Dst: JuniperNetwo_8c:
> Internet Protocol Version 4, Src: 172.30.157.86, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63710, Dst Port: 80, Seq: 1, Ack: 1, Len:
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1
    [HTTP request 1/1]
    [Response in frame: 1853]
```

Figure 2: Accept language

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

   → IP address of my computer: 172.30.157.86

   → IP address of the sever: 128.119.245.12

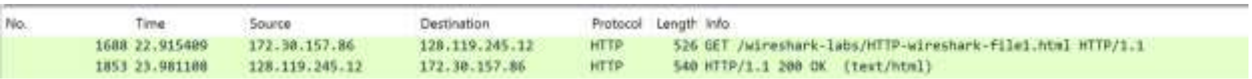


No.	Time	Source	Destination	Protocol	Length	Info
1688	22.915409	172.30.157.86	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1853	23.981100	128.119.245.12	172.30.157.86	HTTP	540	HTTP/1.1 200 OK (text/html)

Figure 3: IP address

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

→ The status code: 200

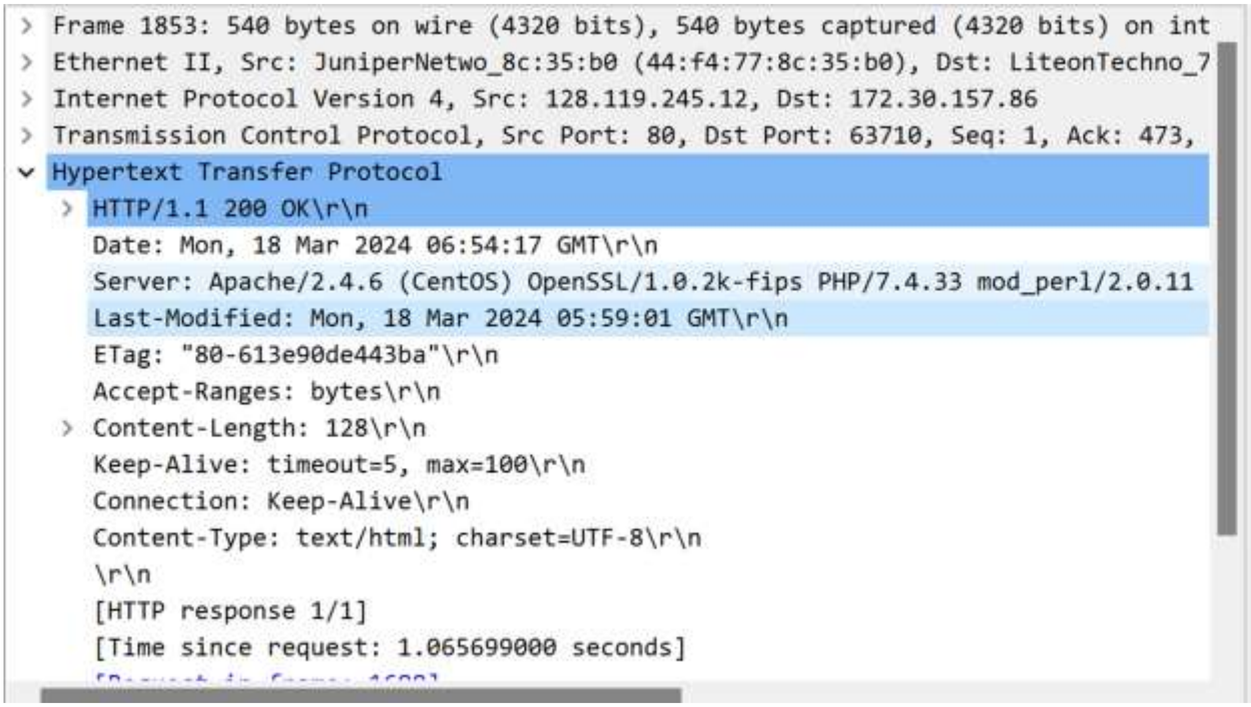


```
No.        Time          Source            Destination       Protocol  Length  Info
      1688 22.915409     172.30.157.86     128.119.245.12    HTTP         526  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
      1853 23.981108     128.119.245.12    172.30.157.86     HTTP         540  HTTP/1.1 200 OK  (text/html)
```

Figure 4: Status code

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

→ Mon, 18 March 2024 05:59:01 GMT

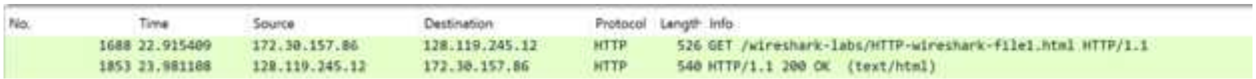


```
> Frame 1853: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on int
> Ethernet II, Src: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:b0), Dst: LiteonTechno_7
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.30.157.86
> Transmission Control Protocol, Src Port: 80, Dst Port: 63710, Seq: 1, Ack: 473,
v Hypertext Transfer Protocol
   > HTTP/1.1 200 OK\r\n
     Date: Mon, 18 Mar 2024 06:54:17 GMT\r\n
     Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11
     Last-Modified: Mon, 18 Mar 2024 05:59:01 GMT\r\n
     ETag: "80-613e90de443ba"\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: 1.065699000 seconds]
     [Request in frame: 1688]
```

Figure 5: Date of the HTML was retrieved

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

→ 540 bytes of content are being returned to my browser

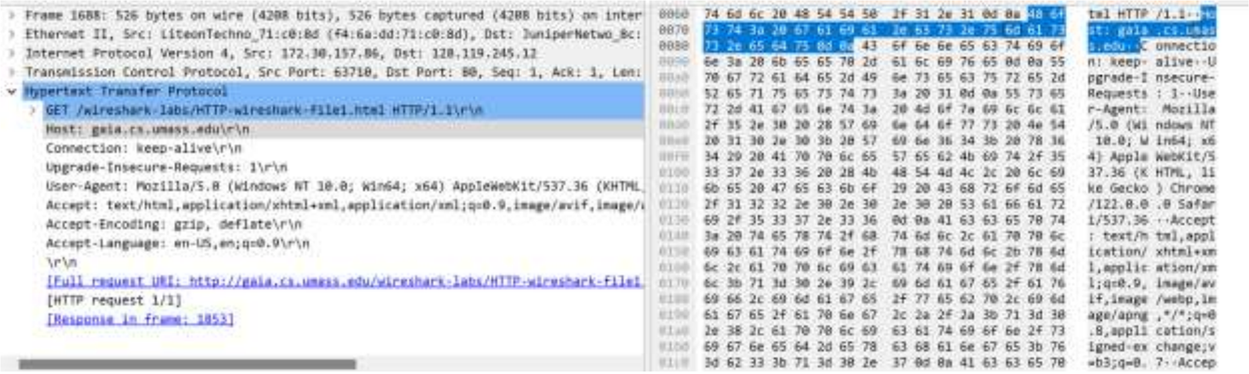


```
No.        Time          Source            Destination       Protocol  Length  Info
      1688 22.915409     172.30.157.86     128.119.245.12    HTTP         526  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
      1853 23.981108     128.119.245.12    172.30.157.86     HTTP         540  HTTP/1.1 200 OK  (text/html)
```

Figure 6: Length

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.



```
> Frame 1688: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on inter
> Ethernet II, Src: LiteonTechno_71:c0:8d (f4:6a:dd:71:c0:8d), Dst: JuniperNetwo_8c:
> Internet Protocol Version 4, Src: 172.30.157.86, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63710, Dst Port: 80, Seq: 1, Ack: 1, Len:
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1
    [HTTP request 1/1]
    [Response in frame: 1853]
```

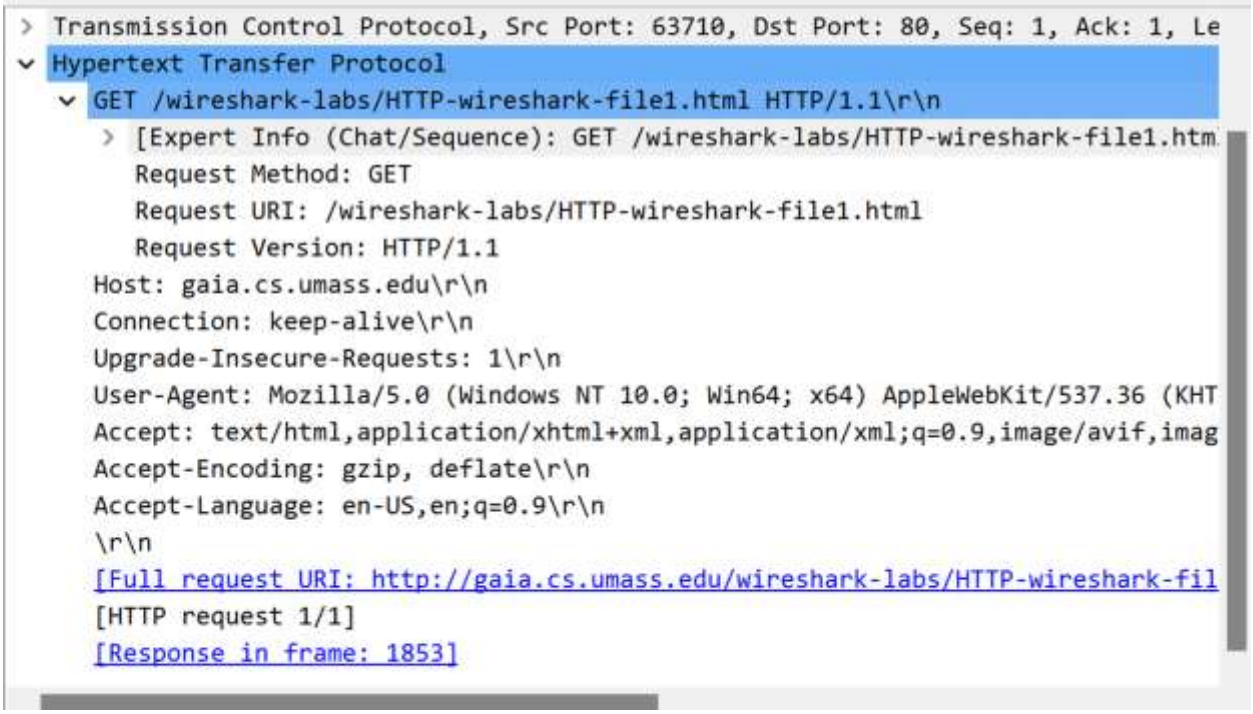
```
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 32 32 2e 30 2e 30  2e 30 20 53 61 66 61 72   /122.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  0d 0a 41 63 63 65 70 74   i/537.36 ··Accept
0140  3a 20 74 65 78 74 2f 68  74 6d 6c 2c 61 70 70 6c   : text/h tml,appl
0150  69 63 61 74 69 6f 6e 2f  78 68 74 6d 6c 2b 78 6d   ication/ xhtml+xm
0160  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 6d   l,applic ation/xm
0170  6c 3b 71 3d 30 2e 39 2c  69 6d 61 67 65 2f 61 76   l;q=0.9, image/av
0180  69 66 2c 69 6d 61 67 65  2f 77 65 62 70 2c 69 6d   if,image /webp,im
0190  61 67 65 2f 61 70 6e 67  2c 2a 2f 2a 3b 71 3d 30   age/apng ,*/*;q=0
01a0  2e 38 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 73   .8,appli cation/s
01b0  69 67 6e 65 64 2d 65 78  63 68 61 6e 67 65 3b 76   igned-ex change;v
01c0  3d 62 33 3b 71 3d 30 2e  37 0d 0a 41 63 63 65 70   =b3;q=0. 7··Accep
```

Figure 7: Headers of the data

TASK 2

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?

   → There is no an "IF-MODIFIED-SINCE" line in the HTTP GET

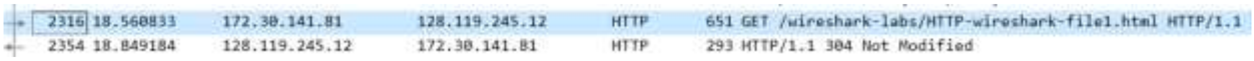


```
> Transmission Control Protocol, Src Port: 63710, Dst Port: 80, Seq: 1, Ack: 1, Le
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.htm
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-fil
    [HTTP request 1/1]
    [Response in frame: 1853]
```

Figure 8: "IF-MODIFIED-SINCE" line

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

   → The response code: 304 Not Modified

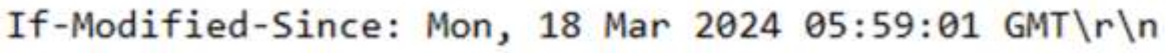


```
2316 18.560833   172.30.141.81    128.119.245.12   HTTP   651 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2354 18.849184   128.119.245.12   172.30.141.81    HTTP   293 HTTP/1.1 304 Not Modified
```

Figure 9: The response code

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?

    → Yes, we can. The information follows the "IF-MODIFIED_SINCE:" header is:

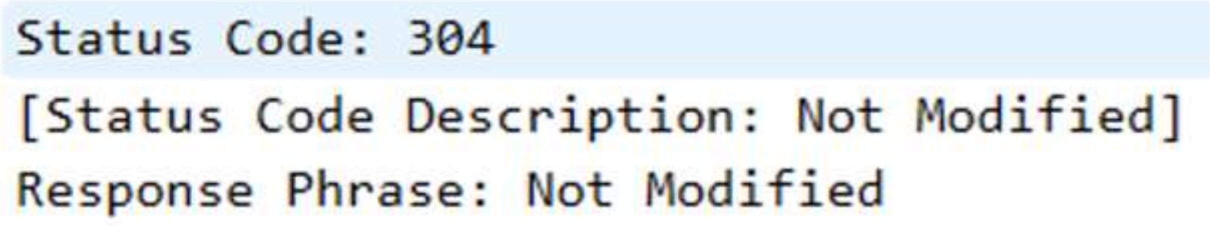


```
If-Modified-Since: Mon, 18 Mar 2024 05:59:01 GMT\r\n
```

Figure 10: Header

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.

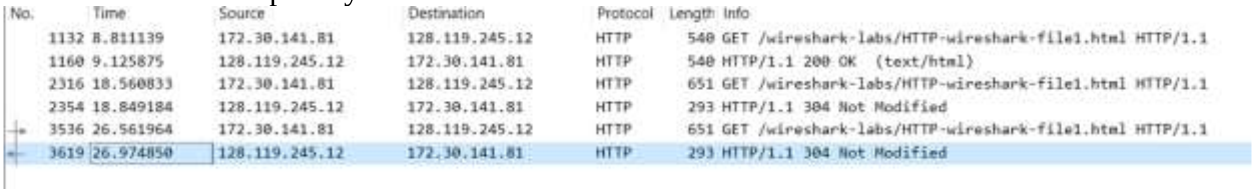
    → The status code: 304 (similar to the first reload page). The phrase is returned from the server in response to this second HTTP GET: Not Modified.



```
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
```

Figure 11: Status code of the second HTTP GET

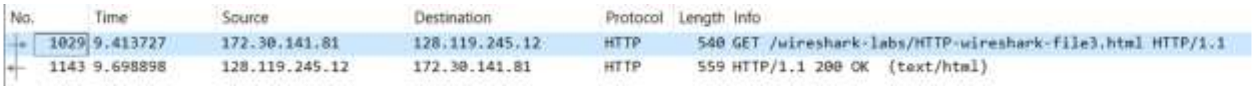
The server **didn't** explicitly return the contents of the file:



```
No.   Time        Source           Destination      Protocol  Length Info
 1132 8.811139    172.30.141.81    128.119.245.12   HTTP      540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 1160 9.125875    128.119.245.12   172.30.141.81    HTTP      540 HTTP/1.1 200 OK  (text/html)
 2316 18.560833   172.30.141.81    128.119.245.12   HTTP      651 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 2354 18.849184   128.119.245.12   172.30.141.81    HTTP      293 HTTP/1.1 304 Not Modified
 3536 26.561964   172.30.141.81    128.119.245.12   HTTP      651 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 3619 26.974850   128.119.245.12   172.30.141.81    HTTP      293 HTTP/1.1 304 Not Modified
```

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 is only one HTTP GET request messages which is sent by my browser. The packet number in the trace contains the GET message for the Bill or Rights is 1029.

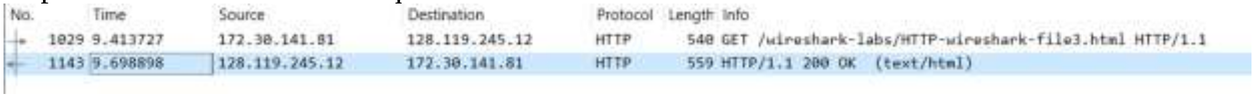


No.	Time	Source	Destination	Protocol	Length	Info
1029	9.413727	172.30.141.81	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1143	9.698898	128.119.245.12	172.30.141.81	HTTP	559	HTTP/1.1 200 OK (text/html)

Figure 12: HTTP GET request

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

→ The packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request is 1143.

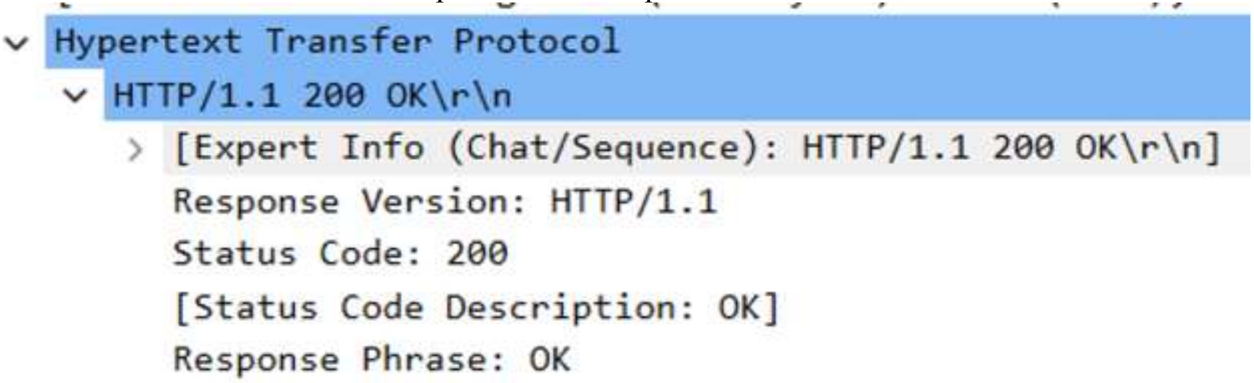


No.	Time	Source	Destination	Protocol	Length	Info
1029	9.413727	172.30.141.81	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1143	9.698898	128.119.245.12	172.30.141.81	HTTP	559	HTTP/1.1 200 OK (text/html)

Figure 13: Packet contains the status code and phrase associated with the response to the HTTP GET request

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

→ The status code is 200 and the phrase in the response is OK.

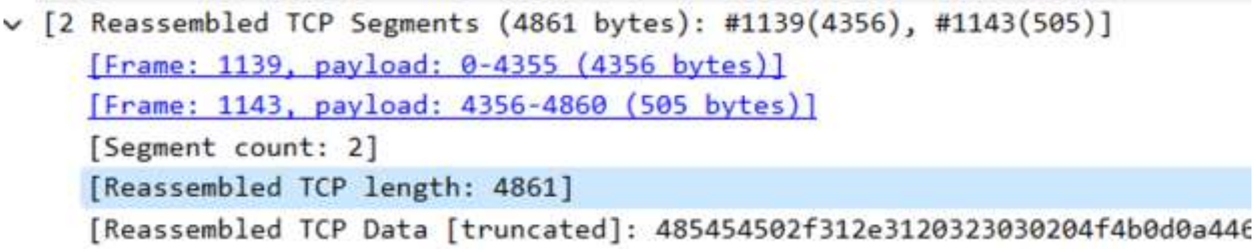


```
v Hypertext Transfer Protocol
    v HTTP/1.1 200 OK\r\n
        > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
          Response Version: HTTP/1.1
          Status Code: 200
          [Status Code Description: OK]
          Response Phrase: OK
```

Figure 14: Status code and the phrase in the response

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

→ There are 2 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.



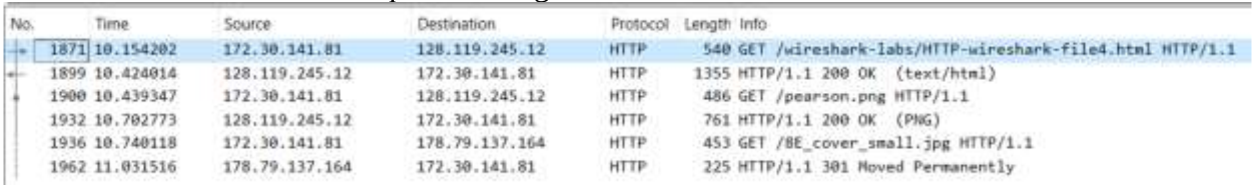
```
v [2 Reassembled TCP Segments (4861 bytes): #1139(4356), #1143(505)]
    [Frame: 1139, payload: 0-4355 (4356 bytes)]
    [Frame: 1143, payload: 4356-4860 (505 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data [truncated]: 485454502f312e3120323030204f4b0d0a446
```

Figure 15: TCP length

Task 3

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

→ There are 3 HTTP GET request messages. Internet address was 172.30.141.81



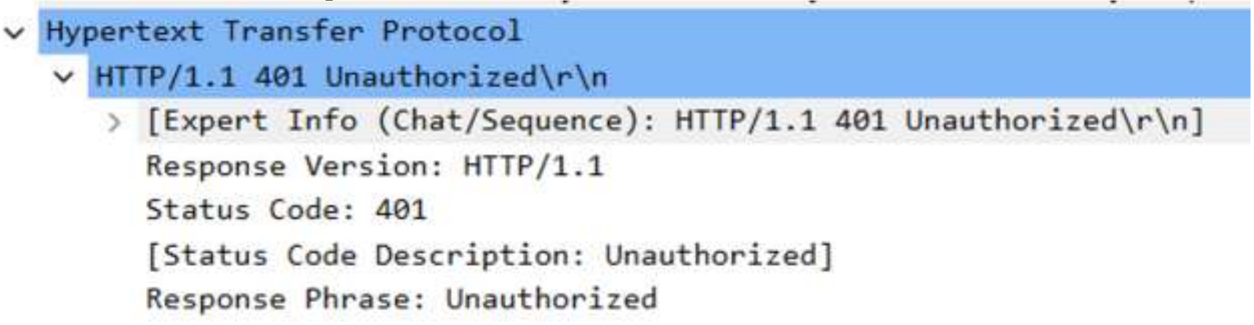
```
No.   Time       Source           Destination      Protocol  Length Info
1871  10.154202  172.30.141.81    128.119.245.12   HTTP       540 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1899  10.424014  128.119.245.12   172.30.141.81    HTTP      1355 HTTP/1.1 200 OK  (text/html)
1900  10.439347  172.30.141.81    128.119.245.12   HTTP       486 GET /pearson.png HTTP/1.1
1932  10.702773  128.119.245.12   172.30.141.81    HTTP       761 HTTP/1.1 200 OK  (PNG)
1936  10.740118  172.30.141.81    178.79.137.164   HTTP       453 GET /8E_cover_small.jpg HTTP/1.1
1962  11.031516  178.79.137.164   172.30.141.81    HTTP       225 HTTP/1.1 301 Moved Permanently
```

Figure 16

Task 4

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

→ Status Code: 401. Response Phrase: Unauthorized

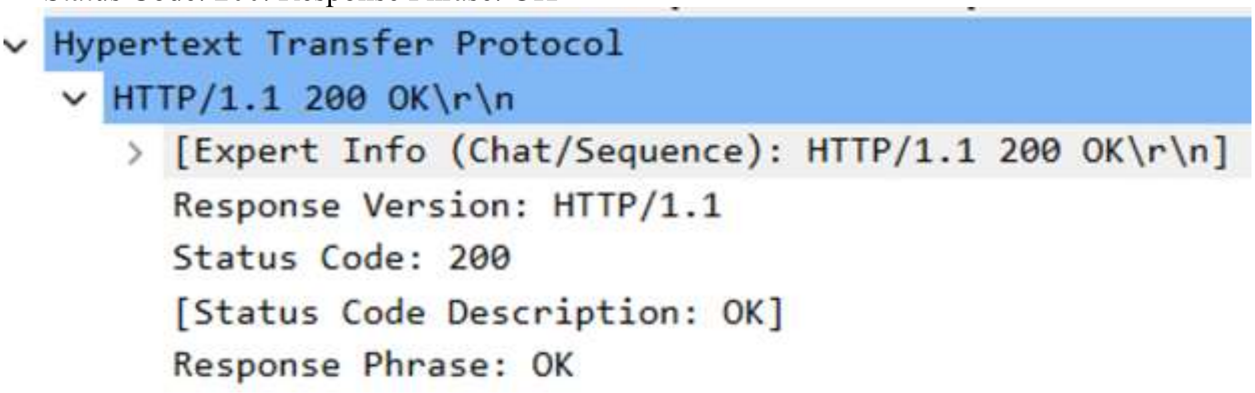


```
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
```

Figure 17: Server's response

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

→ Status Code: 200. Response Phrase: OK



```
v Hypertext Transfer Protocol
  v 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
```

Figure 18