

COMPUTER NETWORK Lab 2a

Student name: Nguyễn Minh Tâm

ID: 1952968

I/ The Basic HTTP GET/response interaction

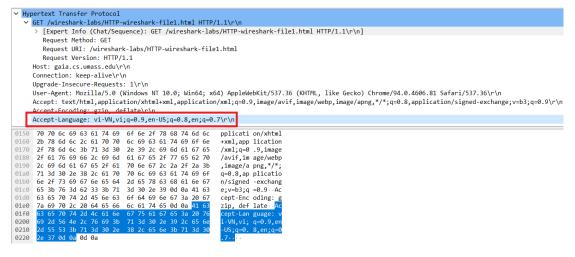
 Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Ans: Both of them are version 1.1

```
Frame 741: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{EF683533-F127-4A1A-A67D-F43EE85AE96D}, id 0 Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
  Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
   Transmission Control Protocol, Src Port: 64956, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
   ✓ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
         Request Method: GET
       Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
     Host: gaia.cs.umass.edu\r
     Connection: keep-alive\r\n
     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
  Frame 792: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0
  Ethernet II, Src: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor_5e:45:34 (dc:fb:48:5e:45:34)
  Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
   Transmission Control Protocol, Src Port: 80, Dst Port: 64956, Seq: 1, Ack: 497, Len: 486
  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: Sat, 16 Oct 2021 01:57:56 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
0030 00 ed af b6 00 00 48 54 54 50 2f 31 2e 31 20 32
```

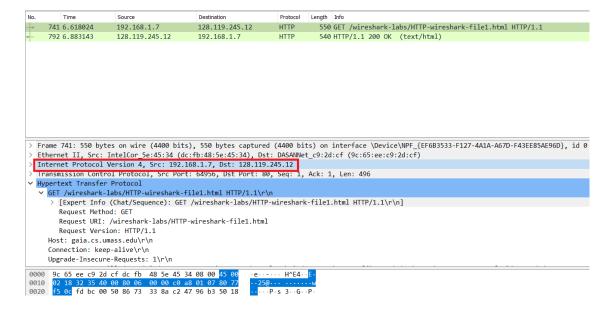
What languages (if any) does your browser indicate that it can accept to the server?Ans: vi-VN and en-US



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

My computer: 192.168.1.7

gaia.cs.umass.edu: 128.119.245.12



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

Ans: 200

5. When was the HTML file that you are retrieving last modified at the server? Ans: Fri, 15 Oct 2021 05:59:01 GMT

```
> Ethernet II, Src: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf), Dst: IntelCor_5e:45:34 (dc:fb:48:5e:45:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 64956, Seq: 1, Ack: 497, Len: 486

→ 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: Sat, 16 Oct 2021 01:57:56 GMT\r\n
                                                           PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
     Last-Modified: Fri, 15 Oct 2021 05:59:01 GMT\r\n
      2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69
                                                               .16.3⋅⋅<mark>L ast-Modi</mark>
      66 69 65 64 3a 20 46 72 69 2c 20 31 35 20 4f 63
74 20 32 30 32 31 20 30 35 3a 35 39 3a 30 31 20
00d0
                                                              fied: Fr i, 15 Oc
                                                              GMT...ETa g: "80-5
      47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 35
00f0
```

How many bytes of content are being returned to your browser?Ans: 128 bytes



```
∨ 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: Sat, 16 Oct 2021 01:57:56 GMT\r\n
     Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\
     Last-Modified: Fri, 15 Oct 2021 05:59:01 GMT\r\n
     ETag: "80-5ce5de452c15f"\r\n
     Accent_Ranges: hytes\r\n
    Content-Length: 128\r\n
0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e
                                                         tes -- Con tent-Len
0130 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41
                                                         gth: 128 ··Keep-A
```

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.

Ans: I do not see any headers within the data that are not displayed in the packet-listing window

II/ The HTTP CONDITIONAL GET/response interaction

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?

Ans: I do not see any "IF-MODIFIED-SINCE" line in the HTTP GET

- Frame 893: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{EF683533-F127-4A1A-A67D-F43EE85AE96D}, id 0 Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
 Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 61853, Dst Port: 80, Seq: 1, Ack: 1, Len: 496 Hypertext Transfer Protocol

 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n \rightarrow [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n] Request URI: /wireshark-labs/HTTP-wireshark-file2.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 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n Accept-Encoding: gzip, deflate\r\n Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html] [HTTP request 1/1]
 - [Response in frame: 932]



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

Ans: Yes, the server explicitly returned the contents of the file by "Line-based text data" section

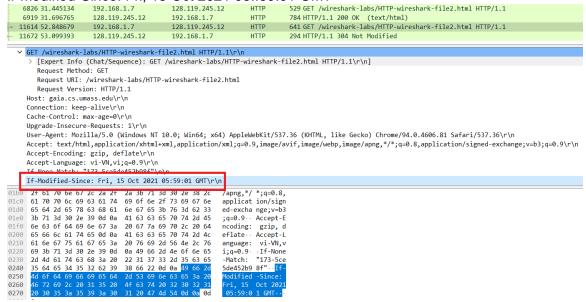
N	lo.	Time	Source	Destination	Protocol	Length Info
-	÷ 89	3 6.228532	192.168.1.7	128.119.245.12	HTTP	550 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
-	- 93	2 6.497040	128.119.245.12	192.168.1.7	HTTP	784 HTTP/1.1 200 OK (text/html)

```
Line-based text data: text/html (10 lines)
                        <html>\n
                       Congratulations again! Now you've downloaded the file lab2-2.html. <br/> <br/> \n
                        This file's last modification date will not change. \n
                       Thus \, if you download this multiple times on your browser, a complete copy \begin{tabular}{ll} copy & 
                        will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br/>br>\n
                        field in your browser's HTTP GET request to the server.\n
                            73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 0a 3d
01b0
01c0
                                                                                                                                                   26 64 67 77 66 66 67 61
66 69 6c 65 20 6c 61 62
2e 20 3c 62 72 3e 0a 54
27 73 20 6c 61 73 74 20
74 69 6f 6e 20 64 61 74
6f 74 20 63 68 61 6e 67
                                   4 65 64 20 74 68 65 20
2 2d 32 2e 68 74 6d 6c
8 69 73 20 66 69 6c 65
01e0
01f0
0200
0210
0220
0230
0240
```

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?

Ans: Yes, I see an "IF-MODIFIED-SINCE:" line the HTTP GET.

If-Modified-Since: Fri, 15 Oct 2021 05::59:01 GMT



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.

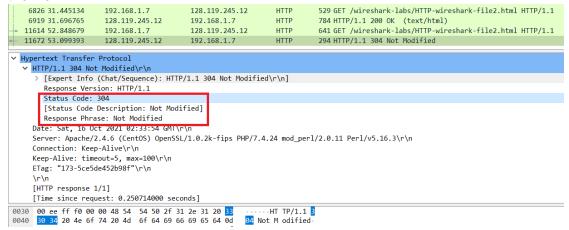


Ans:

HTTP status code is 304.

Response phrase: Not Modified.

The server did not explicitly return the contents of the file because there is no change in the file.





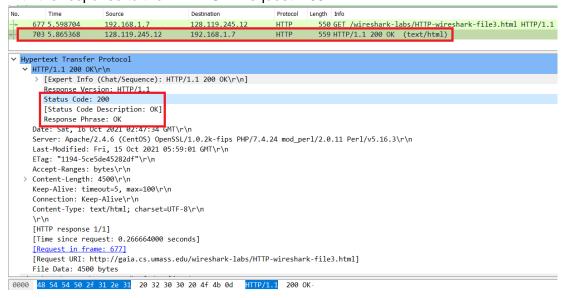
III/ Retrieving Long Documents

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? Ans: Only 1 HTTP GET request message was sent. The packet number in the trace contains the GET message for the Bill or Rights is 677



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

Ans: The packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request: 703



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

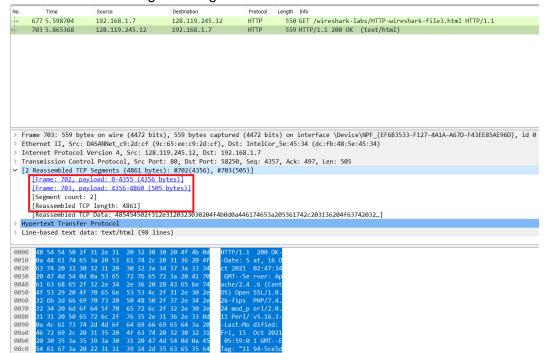
Ans: Using the figure above.

Status Code: 200 and Response 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?

Ans: 2 data-containing TCP segments were needed





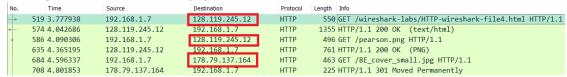
IV/ HTML Documents with Embedded Objects

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

Ans: There were 3 HTTP GET request messages sent.

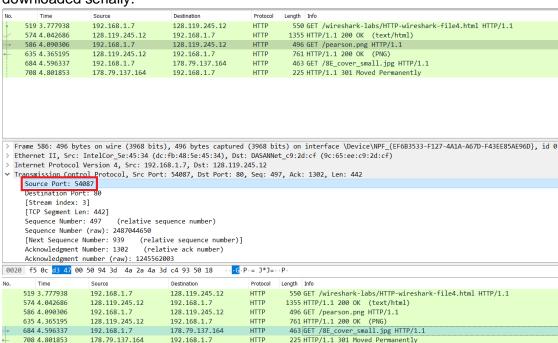
The intial page "HTTP-wideshark-file4.html" and the figure "pearson.png" were sent to the IP address: 128.119.245.12.

The figure "8E cover small.jpg" was sent to the IP address: 178.79.137.164.



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

Ans: By checking the TCP port, I can see that the 2 images were received over 2 different TCP port connections which are 54087 and 64414. Therefore, they were downloaded serially.



```
Frame 684: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface \Device\NPF_[EF683533-F127-4A1A-A67D-F43EE85AE96D], id 0
 Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)
  Internet Protocol Version 4, Src: 192.168.1.7, Dst: 178.79.137.164
Transmission Control Protocol, Src Port: 64414, Dst Port: 80, Seq: 1, Ack: 1, Len: 409
   Source Port: 64414
    Destination Port:
    [Stream index: 8]
     [TCP Segment Len: 409]
     Sequence Number: 1
                          (relative sequence number)
    Sequence Number (raw): 3705028877
    [Next Sequence Number: 410
                                 (relative sequence number)]
    Acknowledgment Number: 1
                               (relative ack number)
    Acknowledgment number (raw): 2675106424
0020 89 a4 fb 9e 00 50 dc d6 41 0d 9f 72 e2 78 50 18
                                                        ......P... A..r.xP.
```



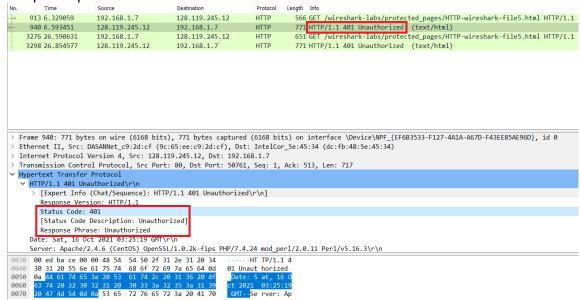
V/ HTTP Authentication

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

Ans: We get a response: 'HTTP/1.1 401 Unauthorized'.

Status code: 401.

Response phrase: Unauthorized.



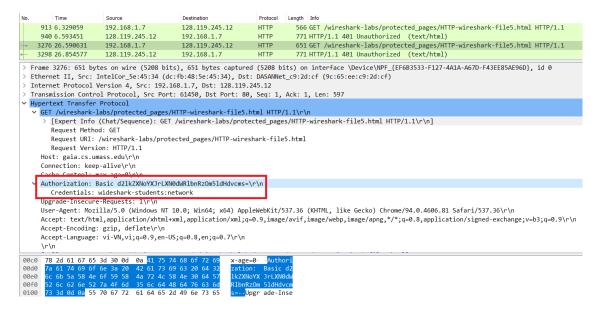
19. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? Ans:

The screenshot of the first HTTP GET message:

No.		Time	Source	Destination	Protocol	Length	Info					
	913	6.329059	192.168.1.7	128.119.245.12	HTTP	566	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1					
-	940	6.593451	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)					
	3276	26.590631	192.168.1.7	128.119.245.12	HTTP	651	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1					
	3298	26.854577	128.119.245.12	192.168.1.7	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)					
>	Frame	913: 566 bytes	on wire (4528 bits),	566 bytes captured (4528 bit	s) on	interface \Device\NPF_{EF6B3533-F127-4A1A-A67D-F43EE85AE96D}, id 0					
>	Ethernet II, Src: IntelCor_5e:45:34 (dc:fb:48:5e:45:34), Dst: DASANNet_c9:2d:cf (9c:65:ee:c9:2d:cf)											
>	Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12											
>	> Transmission Control Protocol, Src Port: 50761, Dst Port: 80, Seq: 1, Ack: 1, Len: 512 Hypertext Transfer Protocol											
~												
<pre>✓ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]</pre>												
											Request Method: GET	
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html												
	Request Version: HTTP/1.1 Host: gaia.cs.umass.edu\r\n Connection: keep-alive\r\n											
	Upg	rade-Insecure-	Requests: 1\r\n									
	(KHTML, like Gecko) Chrome/94.0.4606.81 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 Accept-Encoding: gzip, deflate\r\n											
Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n												
\r\n												
	[Fu	s/HTTP-wireshark-file5.html]										
	[HT	ITTP request 1/1]										
	[Re	sponse in fram	e: 940]									

The screenshot of the second HTTP GET message:





Comparing these two HTTP GET messages, it is easy to find that the second HTTP GET message contains the 'Authorization' field.

The username (wideshark-students) and password (network) that I entered are encoded in the string of characters (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=) following the "Authorization: Basic" header in the client's HTTP GET message.