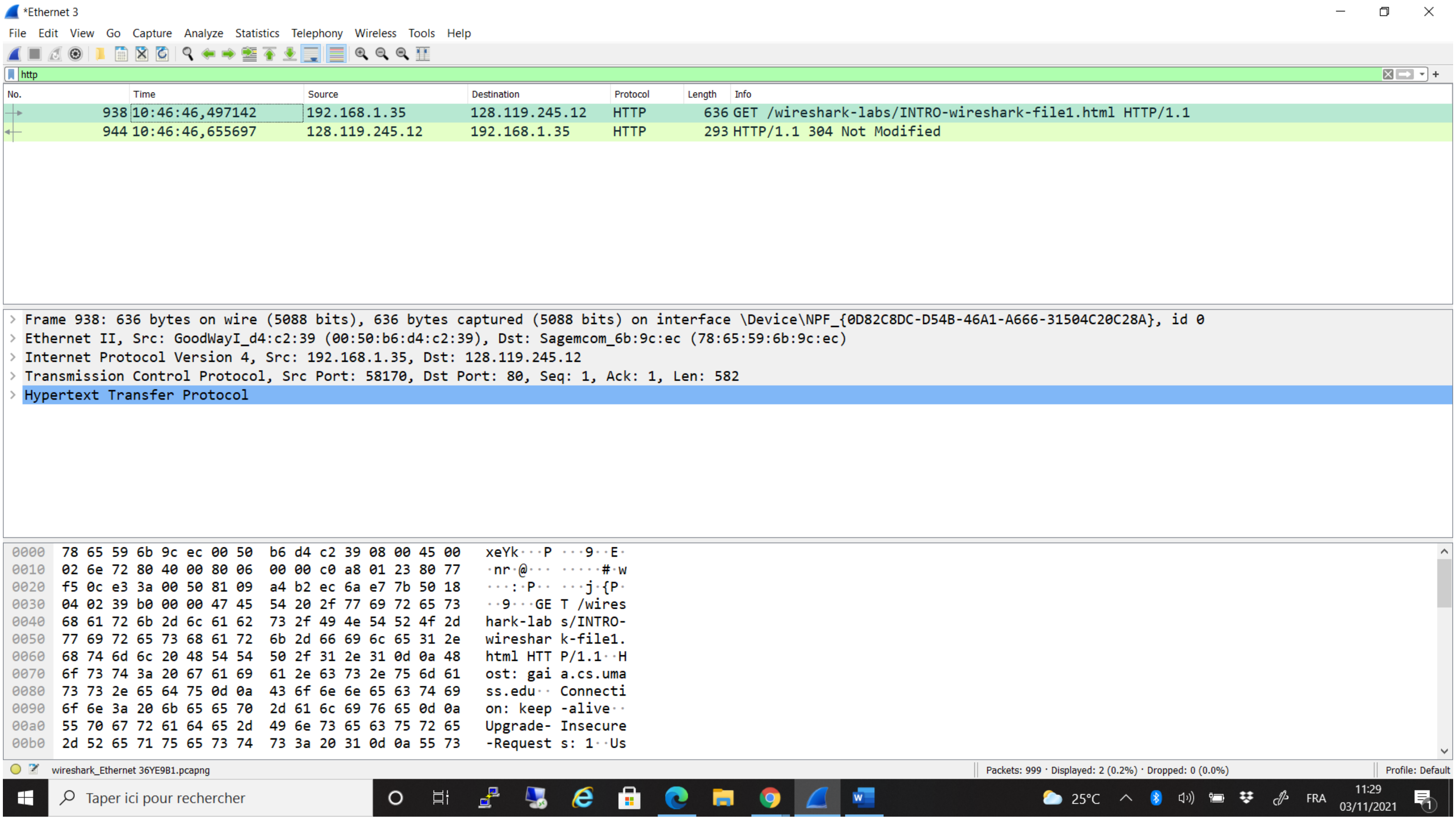
מטלה 1

סטודנט ראשון : אילן מאיר סופיר, ת"ז : 342615648

סטודנט שני : בן כהן , ת"ז : 207029786

First part :

For this part, all we need is in this picture :


*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Taper ici pour rechercher
25°C
FRA
11:29
03/11/2021

http

```
No.     Time             Source          Destination     Protocol  Length Info
    938 10:46:46,497142  192.168.1.35    128.119.245.12  HTTP         636 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    944 10:46:46,655697  128.119.245.12  192.168.1.35    HTTP         293 HTTP/1.1 304 Not Modified
```

```
> Frame 938: 636 bytes on wire (5088 bits), 636 bytes captured (5088 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0
> Ethernet II, Src: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec)
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58170, Dst Port: 80, Seq: 1, Ack: 1, Len: 582
> Hypertext Transfer Protocol
```

```
0000  78 65 59 6b 9c ec 00 50  b6 d4 c2 39 08 00 45 00   xeYk···P ···9··E·
0010  02 6e 72 80 40 00 80 06  00 00 c0 a8 01 23 80 77   ·nr·@··· ·····#·w
0020  f5 0c e3 3a 00 50 81 09  a4 b2 ec 6a e7 7b 50 18   ···:·P·· ···j·{P·
0030  04 02 39 b0 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 HTT P/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  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
```

```
wireshark_Ethernet 36YE9B1.pcapng    Packets: 999 · Displayed: 2 (0.2%) · Dropped: 0 (0.0%)    Profile: Default
```

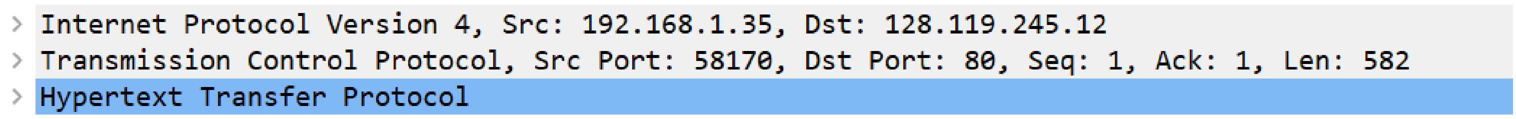
Question 1 : List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

We can see in this picture 3 different protocols :

- **IPV4** : Internet Protocol Version 4.

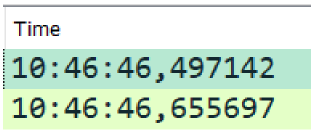
- **TCP** : Transmission Control Protocol.

- **HTTP** : Hypertext Transfer Protocol.



```
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58170, Dst Port: 80, Seq: 1, Ack: 1, Len: 582
> Hypertext Transfer Protocol
```

Question 2 : How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received ? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select *Time Display Format*, then select *Time-of-day*.)



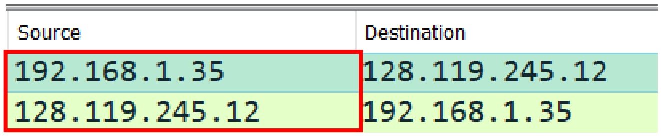
Time
10:46:46,497142
10:46:46,655697

To know the time we need to calculate :

(10h 46min 46.655697s) - (10h 46min 46.497142s) = 0.158555 s

So it takes 0.158555 secondes from when the HTTP GET message was sent until the HTTP OK reply was received.

Question 3 : What is the Internet address of the gaia.cs.umass.edu (also known as www.net.cs.umass.edu) ? What is the Internet address of your computer ?

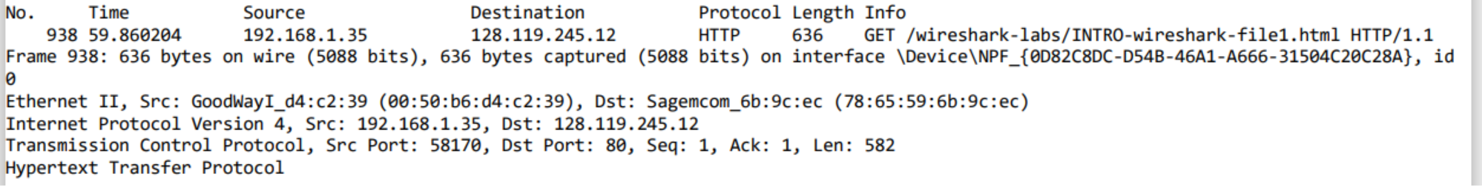


Source	Destination
192.168.1.35	128.119.245.12
128.119.245.12	192.168.1.35

- My computre adress : **192.168.1.35**
- The Internet address of the gaia.cs.umass.edu : **128.119.245.**

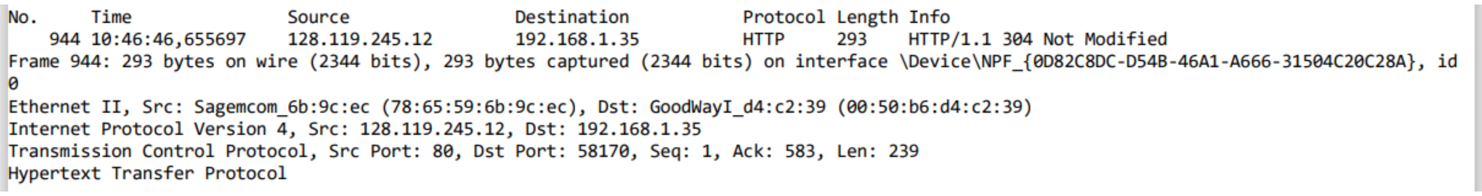
Question 4 : Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “*Selected Packet Only*” and “*Print as displayed*” radial buttons, and then click OK.

The GET message :



```
No.     Time           Source                Destination           Protocol Length Info
    938 59.860204      192.168.1.35          128.119.245.12        HTTP     636    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 938: 636 bytes on wire (5088 bits), 636 bytes captured (5088 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id
0
Ethernet II, Src: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec)
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58170, Dst Port: 80, Seq: 1, Ack: 1, Len: 582
Hypertext Transfer Protocol
```

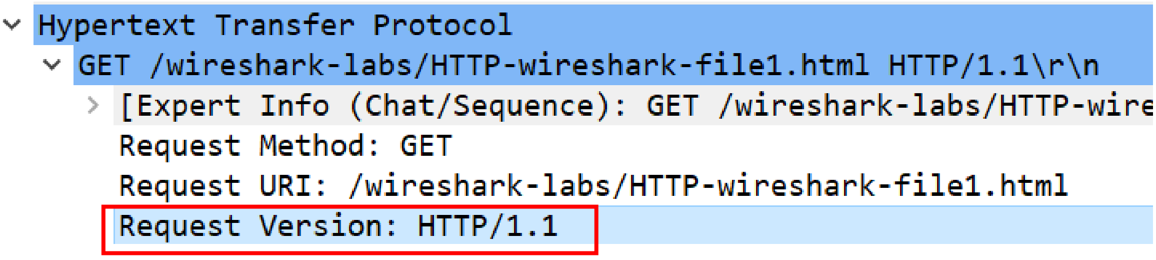
The OK message :



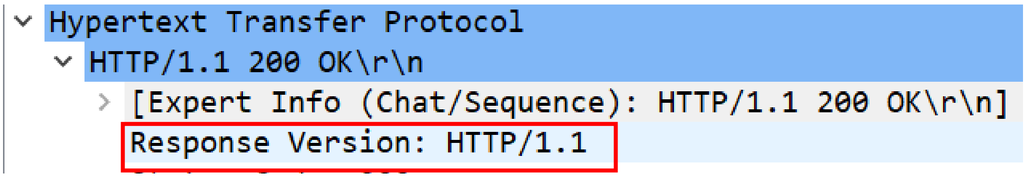
```
No.     Time               Source                Destination           Protocol Length Info
    944 10:46:46,655697    128.119.245.12        192.168.1.35          HTTP     293    HTTP/1.1 304 Not Modified
Frame 944: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id
0
Ethernet II, Src: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.35
Transmission Control Protocol, Src Port: 80, Dst Port: 58170, Seq: 1, Ack: 583, Len: 239
Hypertext Transfer Protocol
```

Second part :

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



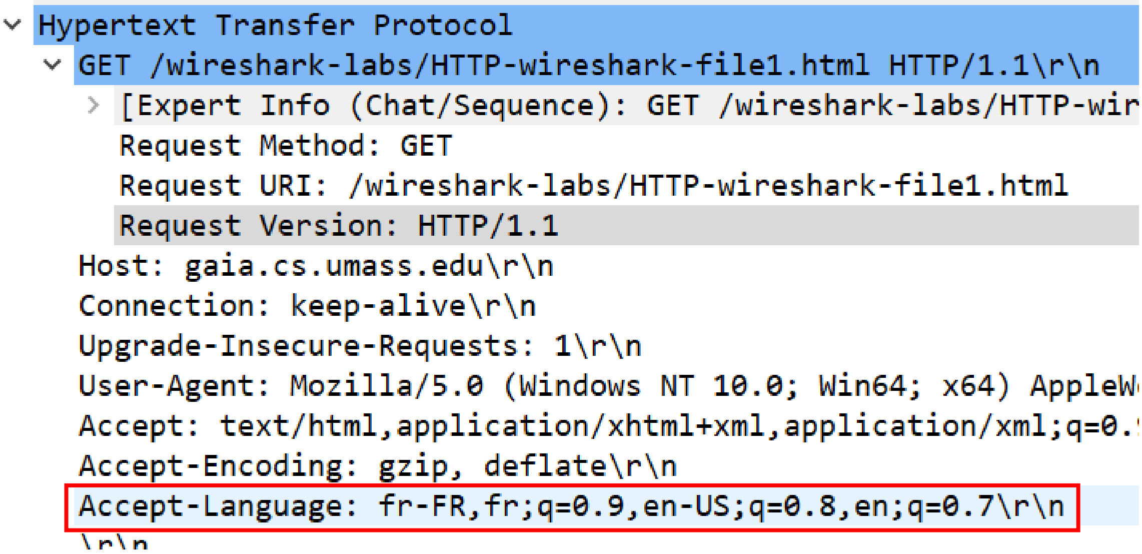
```
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wire
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
```



```
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
```

For both of them it’s HTTP version **1.1.**

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



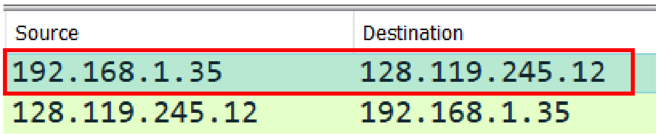
```
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wir
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW
    Accept: text/html,application/xhtml+xml,application/xml;q=0.
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
```

My browser indicate that it can accept to the server the languages :

- English US

- French FR

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



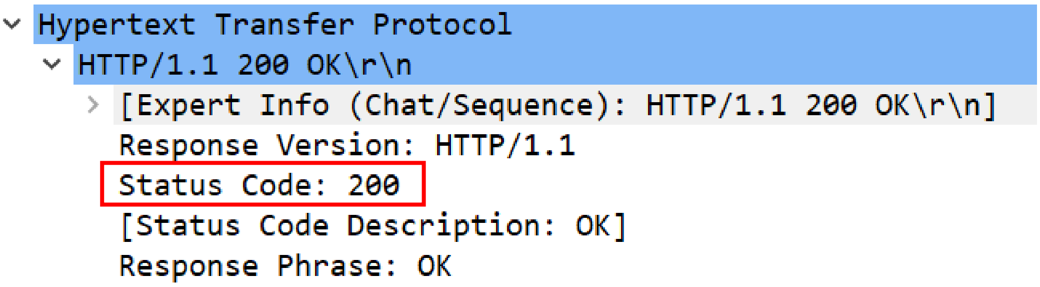
Source	Destination
192.168.1.35	128.119.245.12
128.119.245.12	192.168.1.35

It’s like the First Part, question 3 :

- My computre adress : **192.168.1.35**

- The Internet address of the gaia.cs.umass.edu : **128.119.245.**

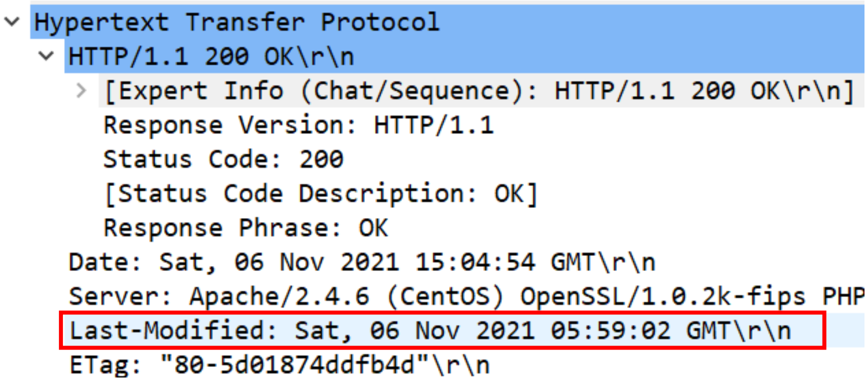
Question 4 : What is the status code returned from the server to your browser ?



```
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
```

The status code returned from the server to my browser is **« 200 ».**

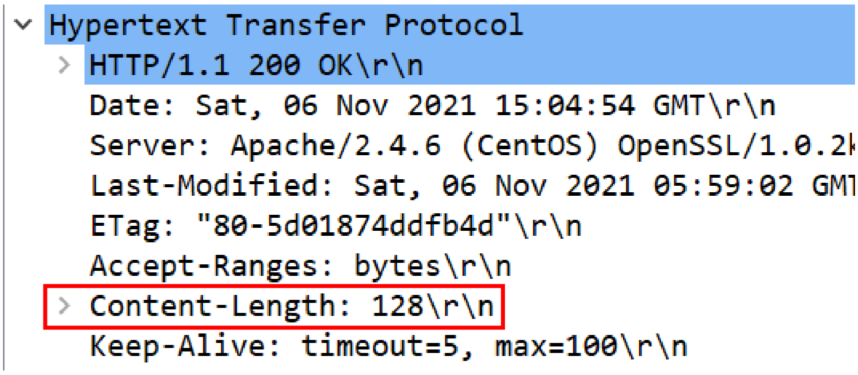
Question 5 : When was the HTML file that you are retrieving last modified at the server ?



```
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
    Date: Sat, 06 Nov 2021 15:04:54 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP
    Last-Modified: Sat, 06 Nov 2021 05:59:02 GMT\r\n
    ETag: "80-5d01874ddfb4d"\r\n
```

it was on **Saturday, the 6th of november 2021 at 05:59:02 GMT.**

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



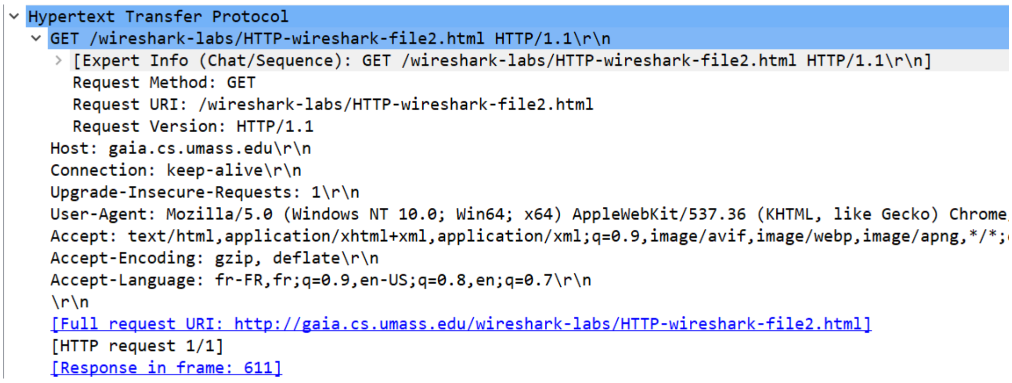
```
⌄ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 06 Nov 2021 15:04:54 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k
    Last-Modified: Sat, 06 Nov 2021 05:59:02 GMT
    ETag: "80-5d01874ddfb4d"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

They are **128 bytes** that are being returned to my browser.

Question 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, i can’t see any headers within the data that are not displayed in the packet-listing window.

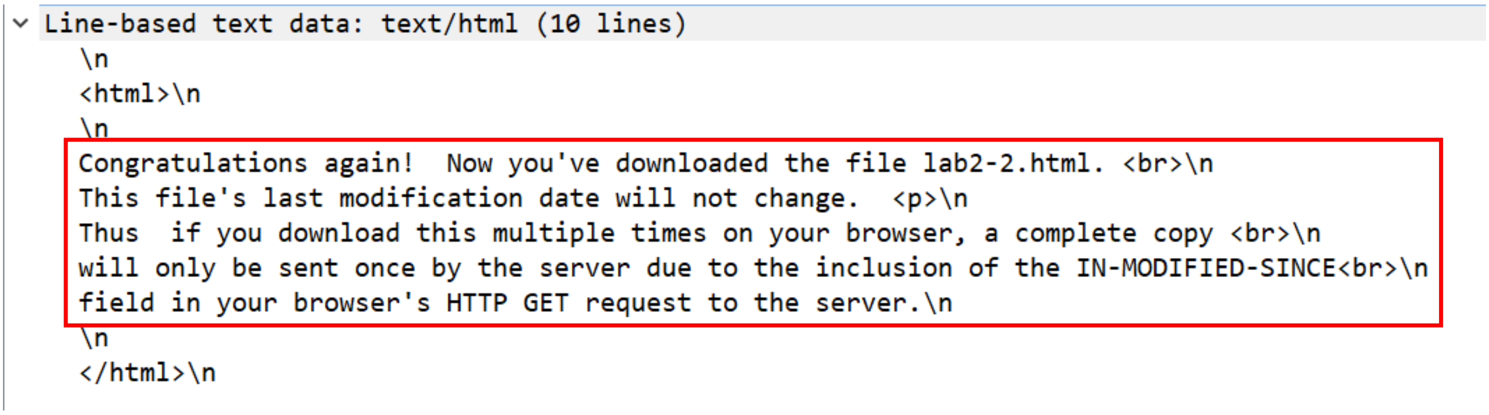
Question 8 : Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET ?



```
⌄ 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]
      Request Method: GET
      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
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 611]
```

No I can’t see an “IF-MODIFIED-SINCE” line in the HTTP GET.

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

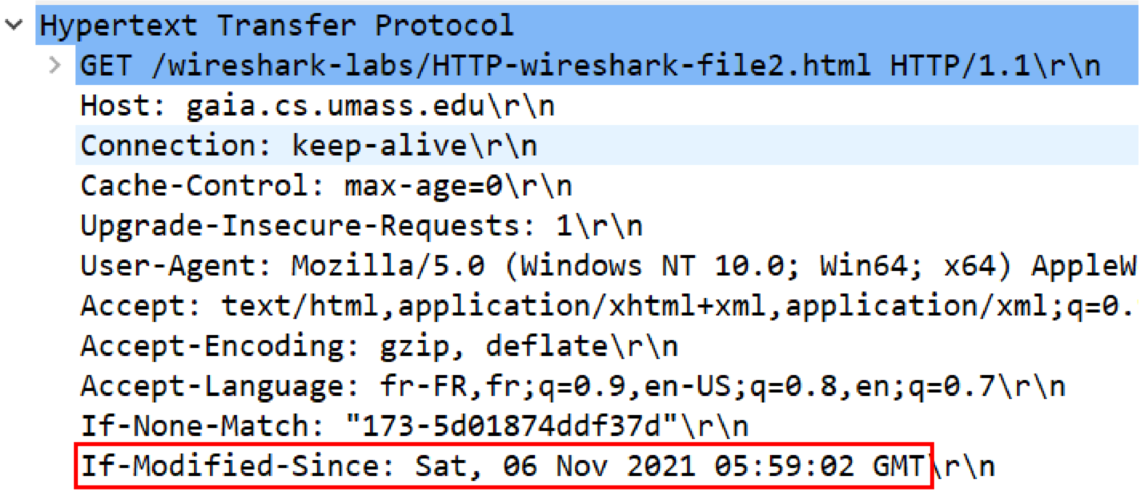


```
∨ Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

Yes I can clearly see the message : « Congralutations again ! […] to the server ».

It's the response to the first GET.

Question 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 ?



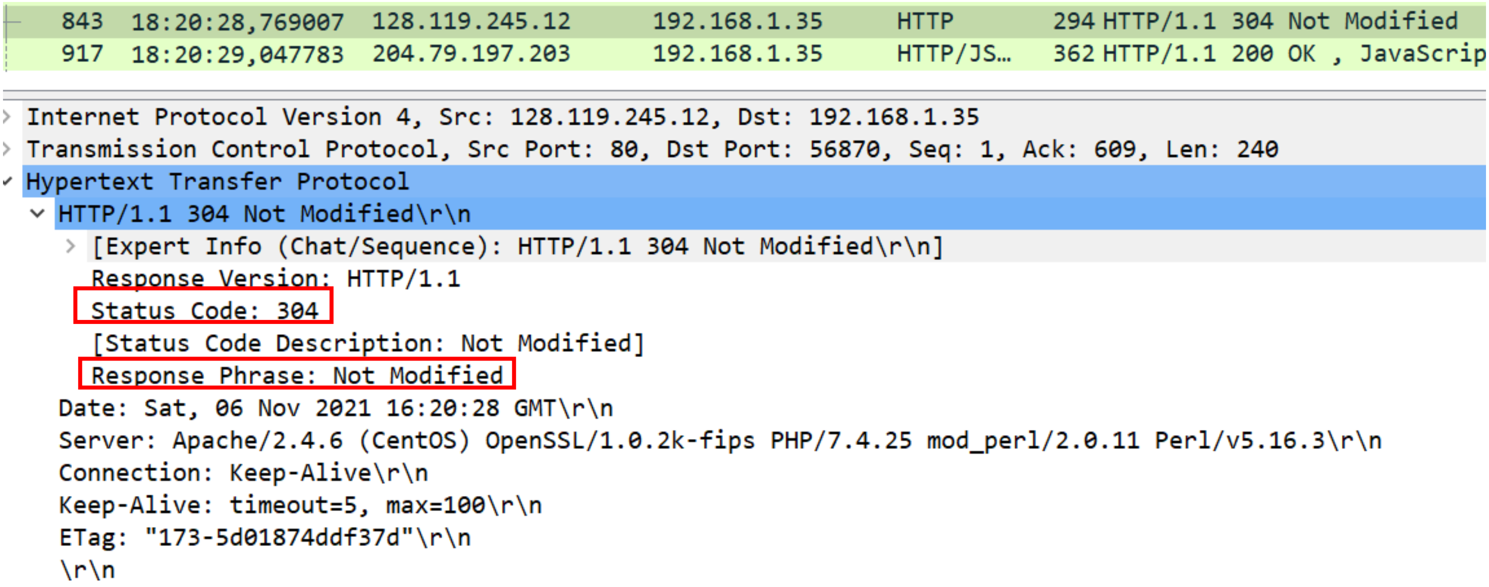
```
∨ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW
    Accept: text/html,application/xhtml+xml,application/xml;q=0.
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    If-None-Match: "173-5d01874ddf37d"\r\n
    If-Modified-Since: Sat, 06 Nov 2021 05:59:02 GMT\r\n
```

Yes I can see an "IF-MODIFIED-SINCE : " in the http GET. And we can see that is write :

Sat, 06 Nov 2021 05:59:02 GMT.

Sat = Saturday.

Question 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.



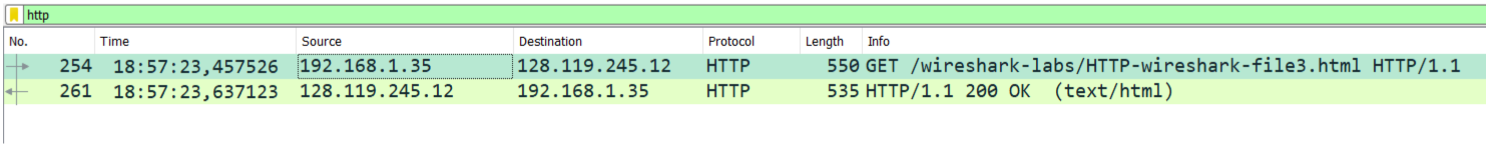
```
843  18:20:28,769007  128.119.245.12    192.168.1.35    HTTP        294 HTTP/1.1 304 Not Modified
917  18:20:29,047783  204.79.197.203    192.168.1.35    HTTP/JS…    362 HTTP/1.1 200 OK , JavaScrip

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.35
> Transmission Control Protocol, Src Port: 80, Dst Port: 56870, Seq: 1, Ack: 609, Len: 240
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Sat, 06 Nov 2021 16:20:28 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-5d01874ddf37d"\r\n
    \r\n
```

The status code returned is **304** and the phrase returned is **Not Modified** from the server in response to this second HTTP GET.

Because the request don't have to be renew the cash well know this adress so it can be signified that nothing was modified since my last request.

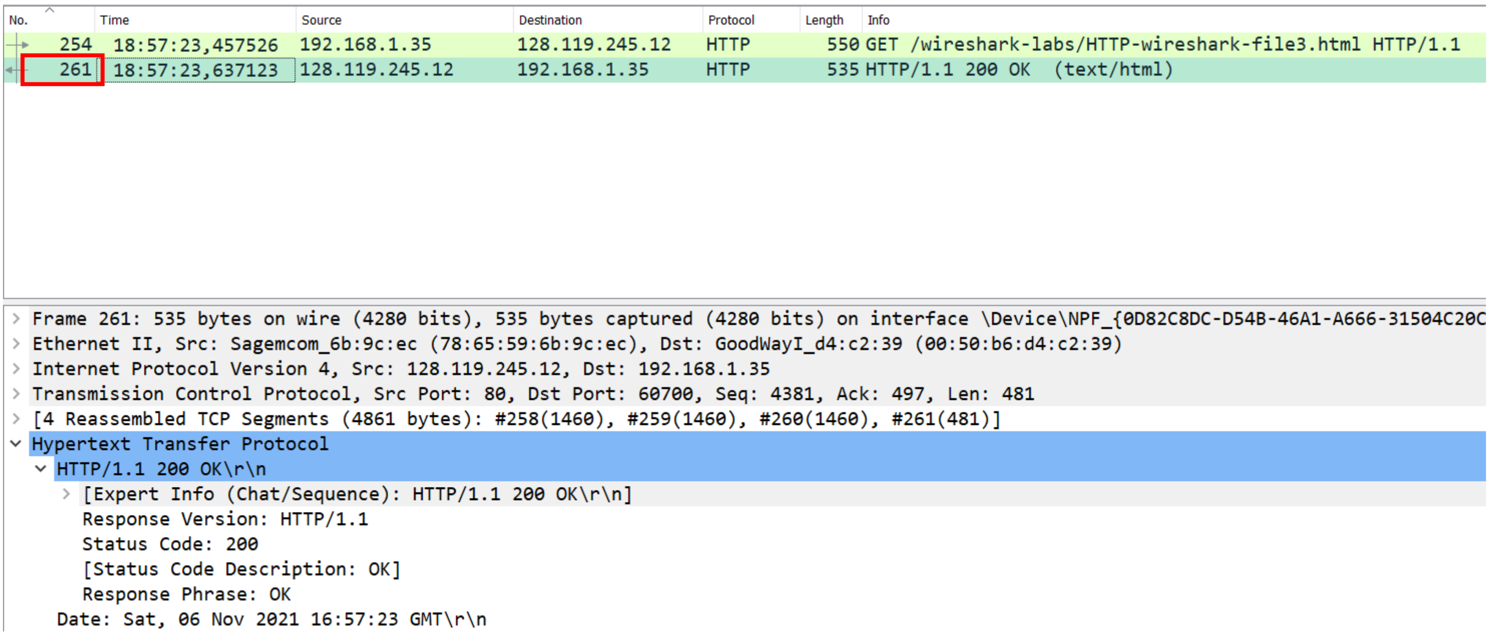
Question 12 : How many HTTP GET request messages did your browser send ? Which packet number in the trace contains the GET message for the Bill or Rights ?



```
http
No.    Time              Source           Destination      Protocol   Length  Info
254    18:57:23,457526   192.168.1.35     128.119.245.12   HTTP       550     GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
261    18:57:23,637123   128.119.245.12   192.168.1.35     HTTP       535     HTTP/1.1 200 OK  (text/html)
```

My browser send only **one** http GET request message.

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

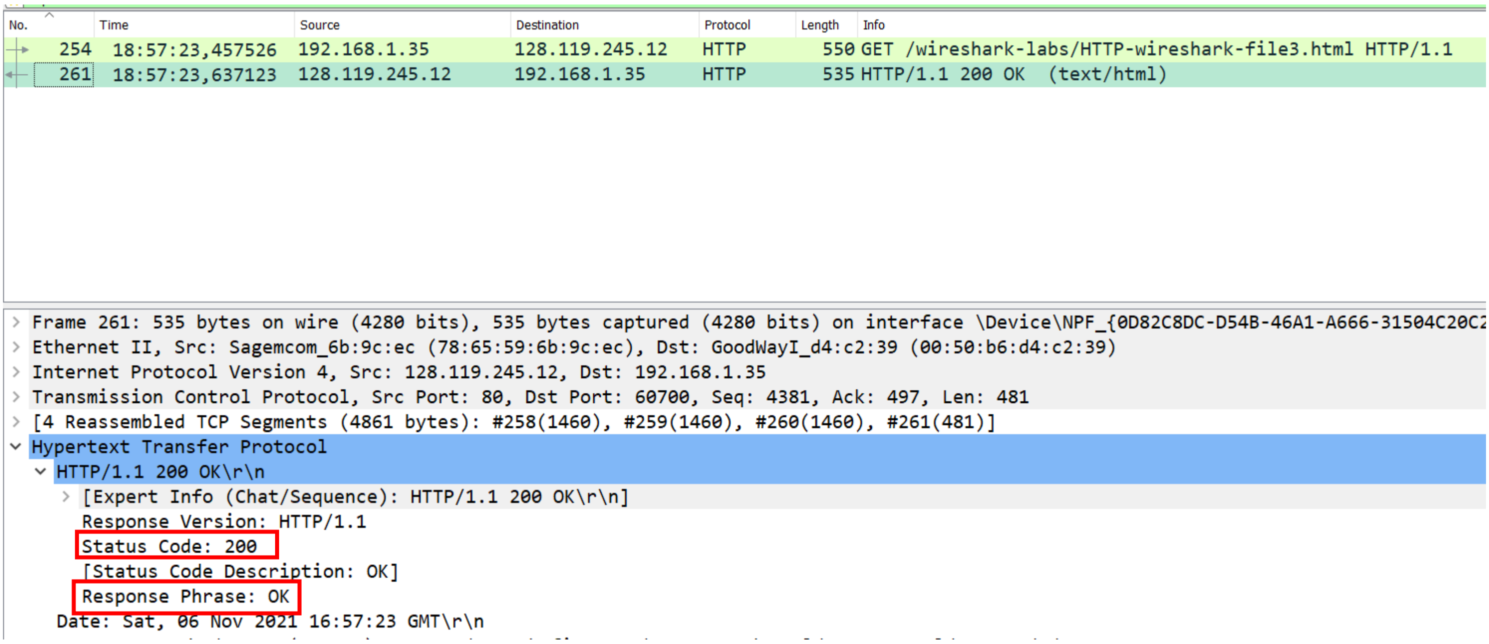


```
No.   Time              Source          Destination     Protocol  Length Info
 254  18:57:23,457526   192.168.1.35    128.119.245.12  HTTP      550 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 261  18:57:23,637123   128.119.245.12  192.168.1.35    HTTP      535 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 261: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C
> Ethernet II, Src: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.35
> Transmission Control Protocol, Src Port: 80, Dst Port: 60700, Seq: 4381, Ack: 497, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #258(1460), #259(1460), #260(1460), #261(481)]
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
    Date: Sat, 06 Nov 2021 16:57:23 GMT\r\n
```

It’s the packet **number 261** that contains the the status code and phrase associated with the response to the HTTP GET request.

Question 14 : What is the status code and phrase in the response ?

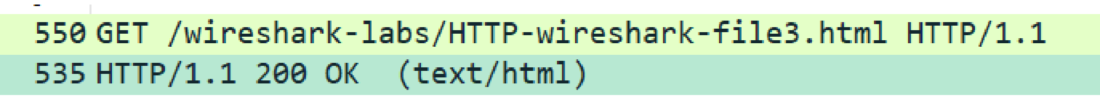


```
No.   Time              Source          Destination     Protocol  Length Info
 254  18:57:23,457526   192.168.1.35    128.119.245.12  HTTP      550 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 261  18:57:23,637123   128.119.245.12  192.168.1.35    HTTP      535 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 261: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C2
> Ethernet II, Src: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.35
> Transmission Control Protocol, Src Port: 80, Dst Port: 60700, Seq: 4381, Ack: 497, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #258(1460), #259(1460), #260(1460), #261(481)]
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
    Date: Sat, 06 Nov 2021 16:57:23 GMT\r\n
```

The Status code is : **200** and the phrase in the response is : **OK**.

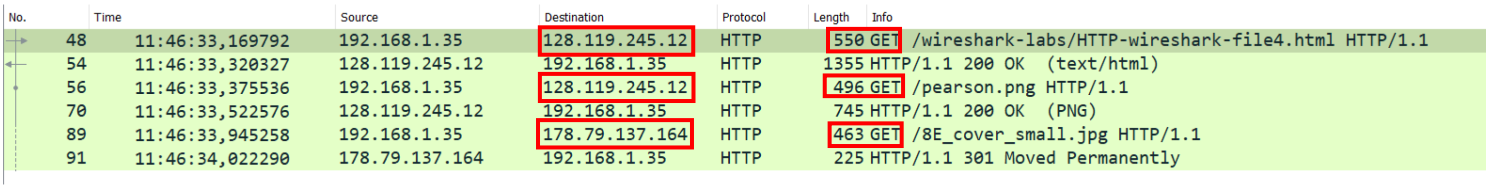
Question 15 : How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights ?



```
550 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
535 HTTP/1.1 200 OK  (text/html)
```

Two TCP segments (one GET and one OK) were needed to carry the single HTTP response and the text of the Bill of Rights.

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



No.	Time	Source	Destination	Protocol	Length	Info
48	11:46:33,169792	192.168.1.35	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
54	11:46:33,320327	128.119.245.12	192.168.1.35	HTTP	1355	HTTP/1.1 200 OK (text/html)
56	11:46:33,375536	192.168.1.35	128.119.245.12	HTTP	496	GET /pearson.png HTTP/1.1
70	11:46:33,522576	128.119.245.12	192.168.1.35	HTTP	745	HTTP/1.1 200 OK (PNG)
89	11:46:33,945258	192.168.1.35	178.79.137.164	HTTP	463	GET /8E_cover_small.jpg HTTP/1.1
91	11:46:34,022290	178.79.137.164	192.168.1.35	HTTP	225	HTTP/1.1 301 Moved Permanently

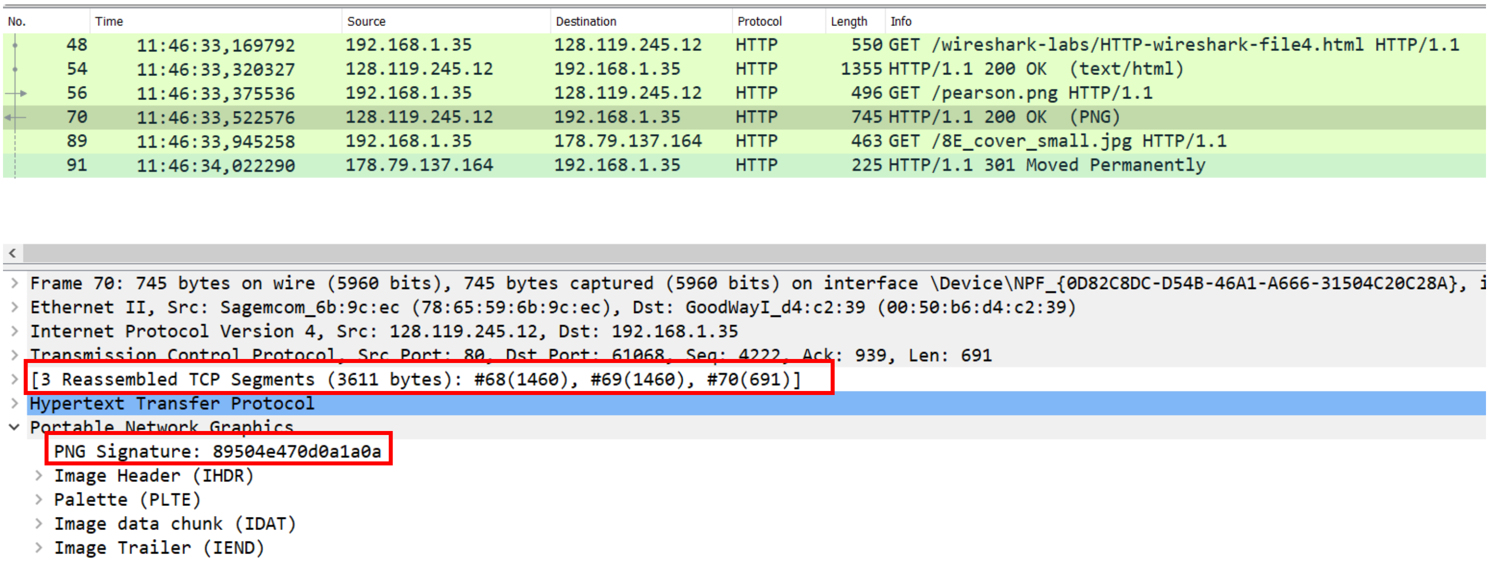
My browser send **Tree** http GET request messages :

- Two to the adress : **128.119.245.12**

- One to the adress : **178.79.137.164**

Question 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.

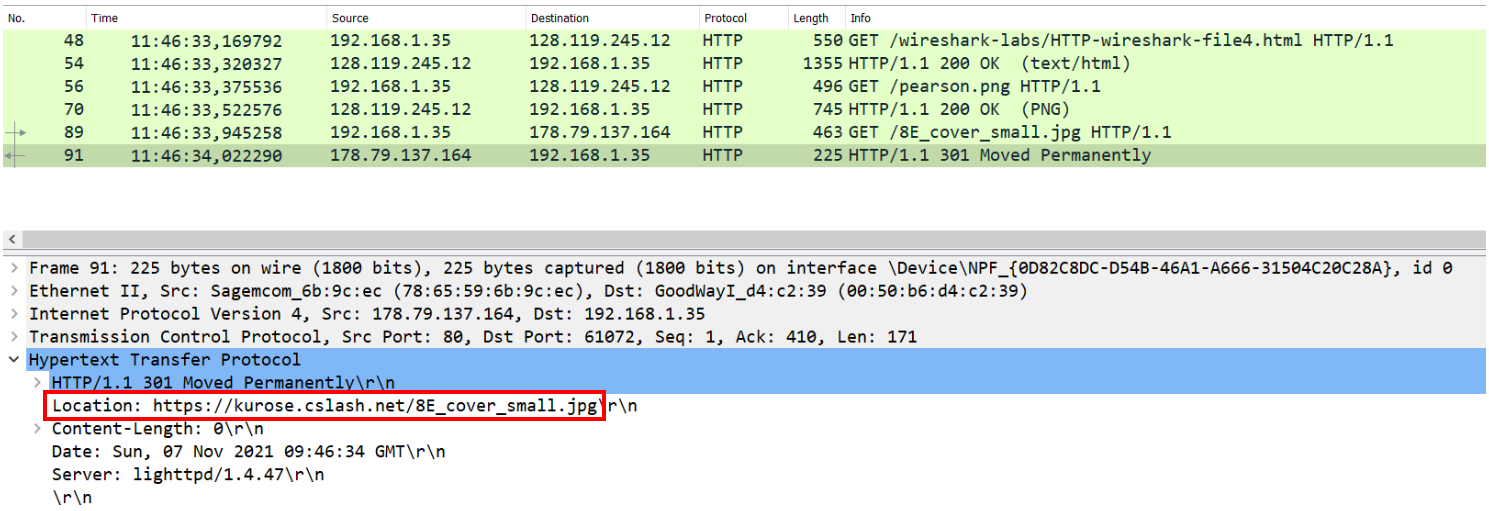
Picture num 1 :



```
No.   Time              Source            Destination       Protocol  Length Info
  48  11:46:33,169792   192.168.1.35      128.119.245.12    HTTP       550 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  54  11:46:33,320327   128.119.245.12    192.168.1.35      HTTP      1355 HTTP/1.1 200 OK  (text/html)
  56  11:46:33,375536   192.168.1.35      128.119.245.12    HTTP       496 GET /pearson.png HTTP/1.1
  70  11:46:33,522576   128.119.245.12    192.168.1.35      HTTP       745 HTTP/1.1 200 OK  (PNG)
  89  11:46:33,945258   192.168.1.35      178.79.137.164    HTTP       463 GET /8E_cover_small.jpg HTTP/1.1
  91  11:46:34,022290   178.79.137.164    192.168.1.35      HTTP       225 HTTP/1.1 301 Moved Permanently
```

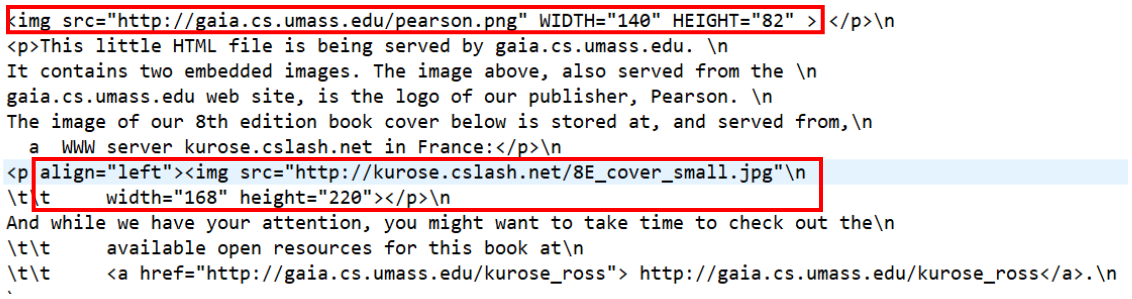
```
> Frame 70: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, i
> Ethernet II, Src: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.35
> Transmission Control Protocol, Src Port: 80, Dst Port: 61068, Seq: 4222, Ack: 939, Len: 691
> [3 Reassembled TCP Segments (3611 bytes): #68(1460), #69(1460), #70(691)]
> Hypertext Transfer Protocol
v Portable Network Graphics
    PNG Signature: 89504e470d0a1a0a
  > Image Header (IHDR)
  > Palette (PLTE)
  > Image data chunk (IDAT)
  > Image Trailer (IEND)
```

Picture num 2 :



```
No.   Time              Source            Destination       Protocol  Length Info
  48  11:46:33,169792   192.168.1.35      128.119.245.12    HTTP       550 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  54  11:46:33,320327   128.119.245.12    192.168.1.35      HTTP      1355 HTTP/1.1 200 OK  (text/html)
  56  11:46:33,375536   192.168.1.35      128.119.245.12    HTTP       496 GET /pearson.png HTTP/1.1
  70  11:46:33,522576   128.119.245.12    192.168.1.35      HTTP       745 HTTP/1.1 200 OK  (PNG)
  89  11:46:33,945258   192.168.1.35      178.79.137.164    HTTP       463 GET /8E_cover_small.jpg HTTP/1.1
  91  11:46:34,022290   178.79.137.164    192.168.1.35      HTTP       225 HTTP/1.1 301 Moved Permanently
```

```
> Frame 91: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0
> Ethernet II, Src: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39)
> Internet Protocol Version 4, Src: 178.79.137.164, Dst: 192.168.1.35
> Transmission Control Protocol, Src Port: 80, Dst Port: 61072, Seq: 1, Ack: 410, Len: 171
v Hypertext Transfer Protocol
  > HTTP/1.1 301 Moved Permanently\r\n
    Location: https://kurose.cslash.net/8E_cover_small.jpg\r\n
  > Content-Length: 0\r\n
    Date: Sun, 07 Nov 2021 09:46:34 GMT\r\n
    Server: lighttpd/1.4.47\r\n
    \r\n
```

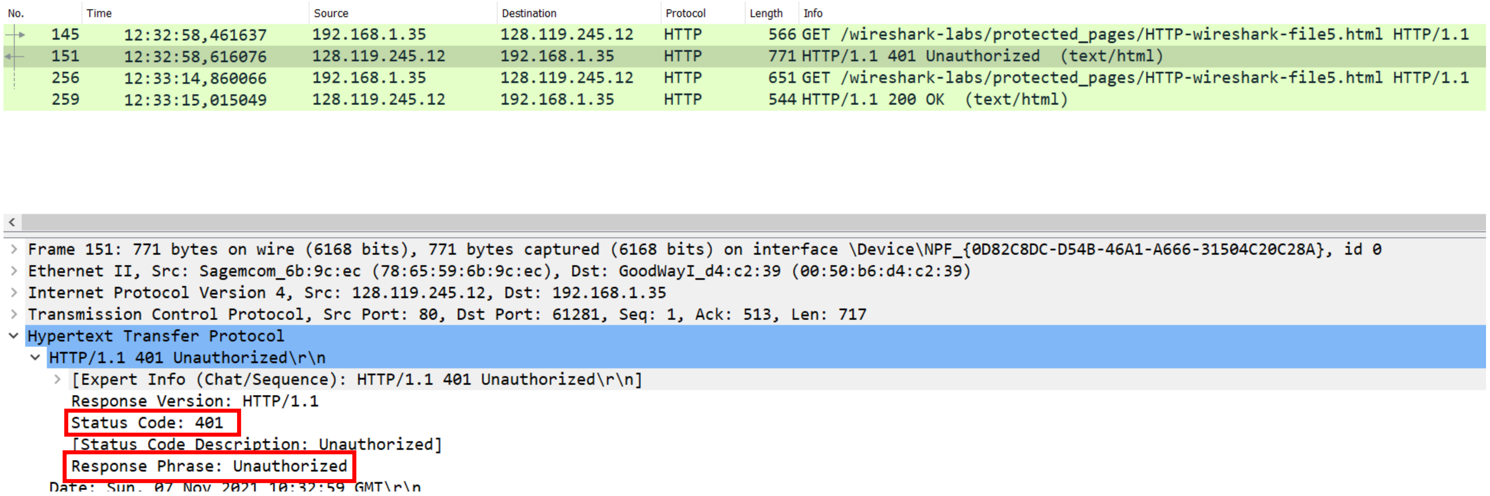


```
<img src="http://gaia.cs.umass.edu/pearson.png" WIDTH="140" HEIGHT="82" > </p>\n
<p>This little HTML file is being served by gaia.cs.umass.edu. \n
It contains two embedded images. The image above, also served from the \n
gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. \n
The image of our 8th edition book cover below is stored at, and served from,\n
  a  WWW server kurose.cslash.net in France:</p>\n
<p align="left"><img src="http://kurose.cslash.net/8E_cover_small.jpg"\n
\t\t     width="168" height="220"></p>\n
And while we have your attention, you might want to take time to check out the\n
\t\t     available open resources for this book at\n
\t\t     <a href="http://gaia.cs.umass.edu/kurose_ross"> http://gaia.cs.umass.edu/kurose_ross</a>.\n
```

We can see that my browser downloaded the first image serially from their site : http://gaia.cs.umass.edu/pearson.png .

And the Second was dowloaded from another site : http://kurose.cslash.net/8E_small.jpg

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



```
No.   Time               Source           Destination      Protocol  Length  Info
145   12:32:58,461637    192.168.1.35     128.119.245.12   HTTP      566 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
151   12:32:58,616076    128.119.245.12   192.168.1.35     HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
256   12:33:14,860066    192.168.1.35     128.119.245.12   HTTP      651 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
259   12:33:15,015049    128.119.245.12   192.168.1.35     HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 151: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0
> Ethernet II, Src: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec), Dst: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.35
> Transmission Control Protocol, Src Port: 80, Dst Port: 61281, Seq: 1, Ack: 513, Len: 717
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
    Date: Sun, 07 Nov 2021 10:32:59 GMT\r\n
```

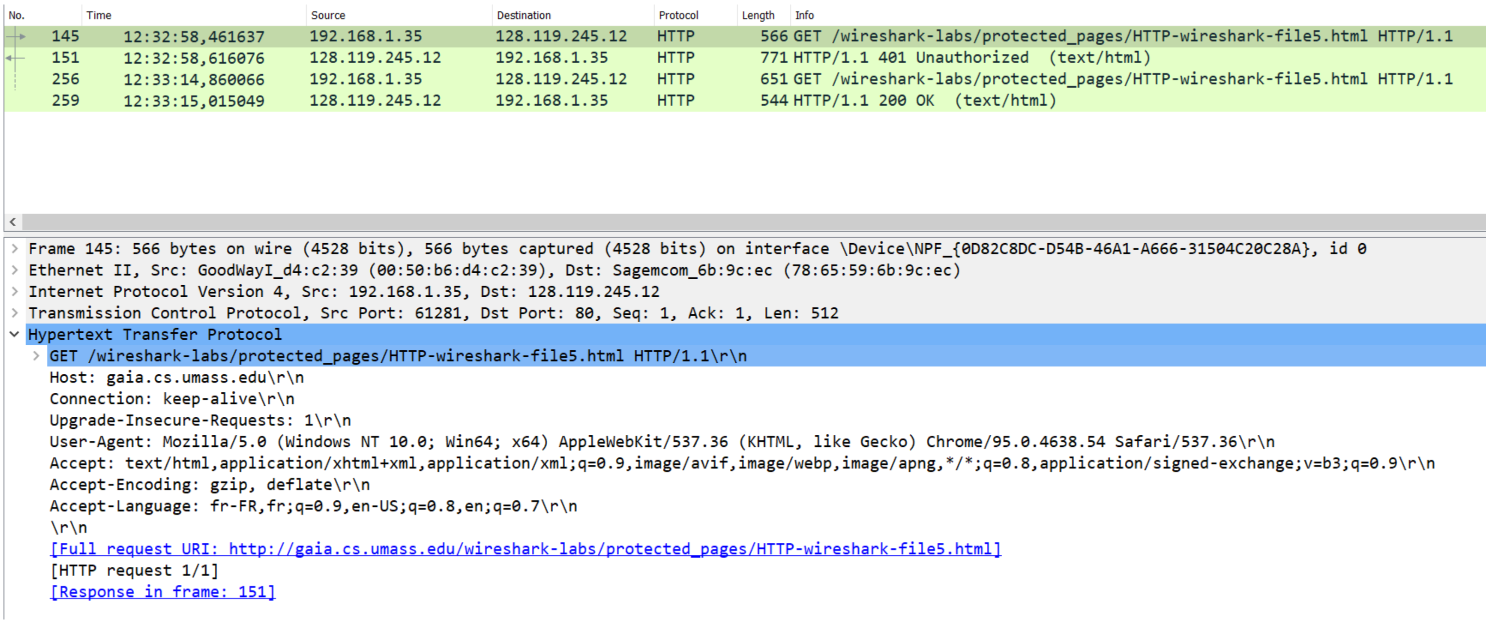
The server’s response to the initial http GET message from my browser is :

- Status code : **401**

- Phrase : **Unauthorized**

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

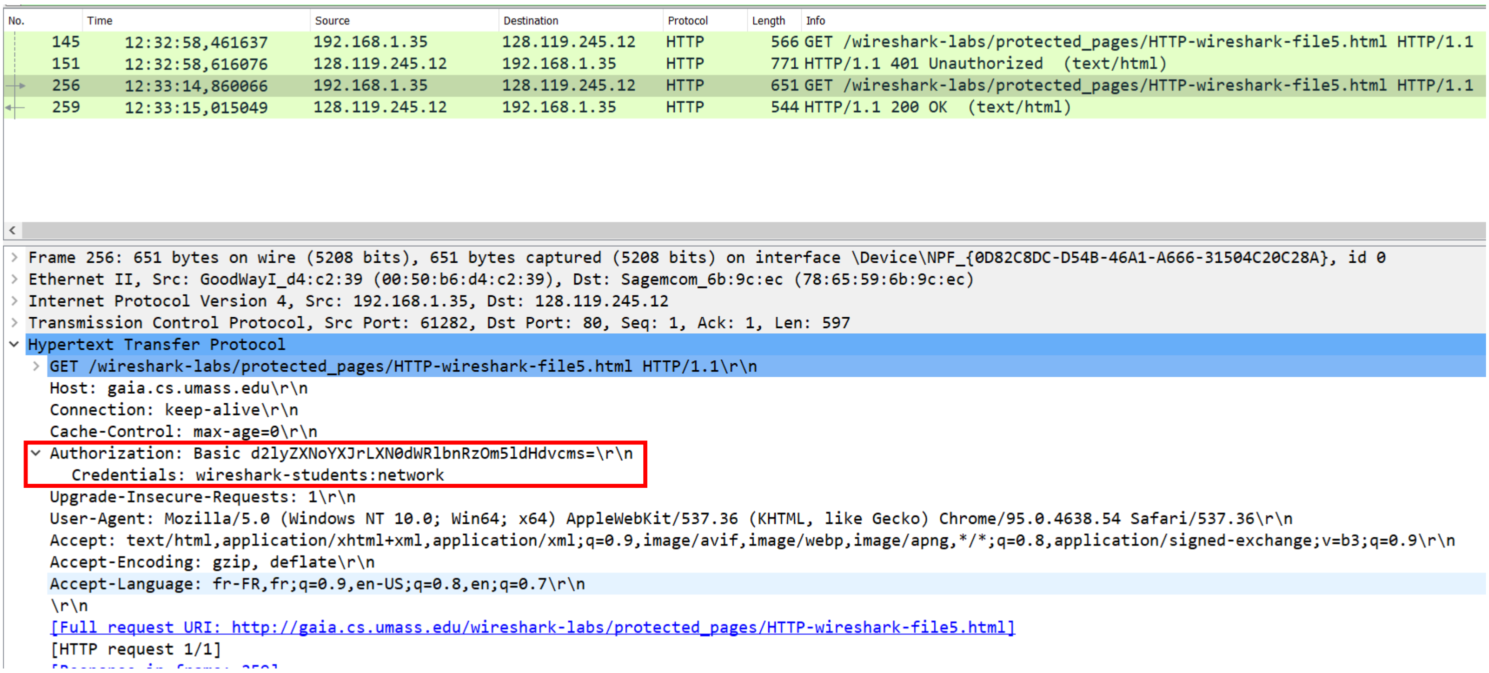
This is the picture of the first http GET :



```
No.   Time               Source           Destination      Protocol  Length  Info
145   12:32:58,461637    192.168.1.35     128.119.245.12   HTTP      566 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
151   12:32:58,616076    128.119.245.12   192.168.1.35     HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
256   12:33:14,860066    192.168.1.35     128.119.245.12   HTTP      651 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
259   12:33:15,015049    128.119.245.12   192.168.1.35     HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 145: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0
> Ethernet II, Src: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec)
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61281, Dst Port: 80, Seq: 1, Ack: 1, Len: 512
v 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 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=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 151]
```

And this is the picture of the second HTTP GET :



```
No.     Time              Source          Destination     Protocol  Length Info
  145   12:32:58,461637   192.168.1.35    128.119.245.12  HTTP      566 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  151   12:32:58,616076   128.119.245.12  192.168.1.35    HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
  256   12:33:14,860066   192.168.1.35    128.119.245.12  HTTP      651 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  259   12:33:15,015049   128.119.245.12  192.168.1.35    HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 256: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface \Device\NPF_{0D82C8DC-D54B-46A1-A666-31504C20C28A}, id 0
> Ethernet II, Src: GoodWayI_d4:c2:39 (00:50:b6:d4:c2:39), Dst: Sagemcom_6b:9c:ec (78:65:59:6b:9c:ec)
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61282, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
v 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
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      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 Gecko) Chrome/95.0.4638.54 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=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
```

We can see that a new field is included in the HTTP GET message :

- **Authorization.**