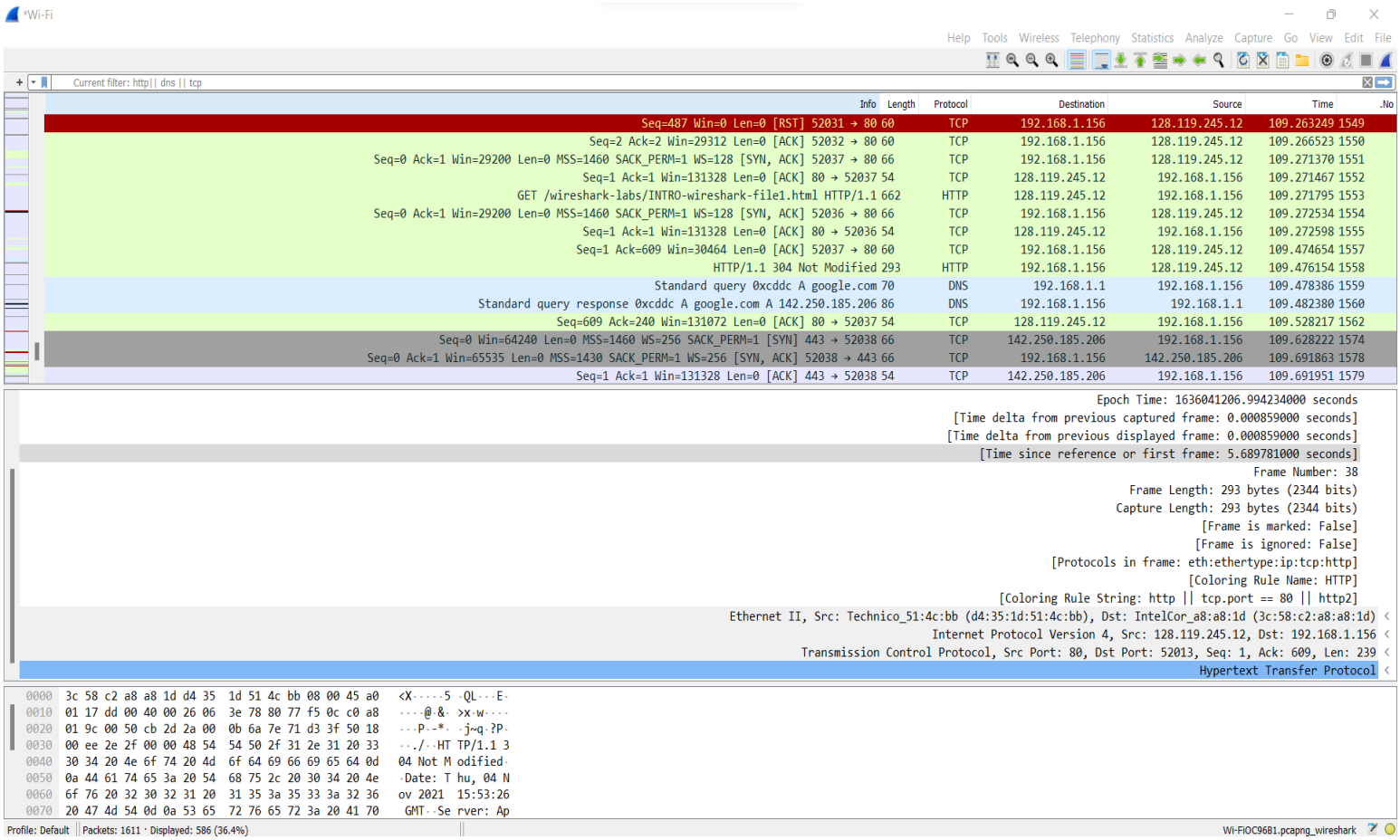
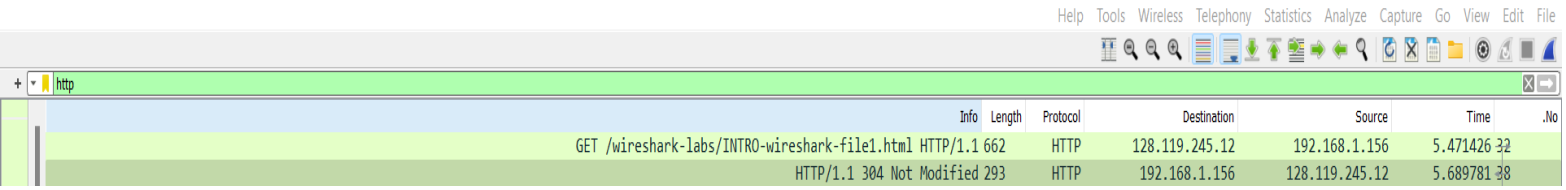
Ex0- WireSharkIntro

Q1- As you can see, at the image below there are 3 different protocols,

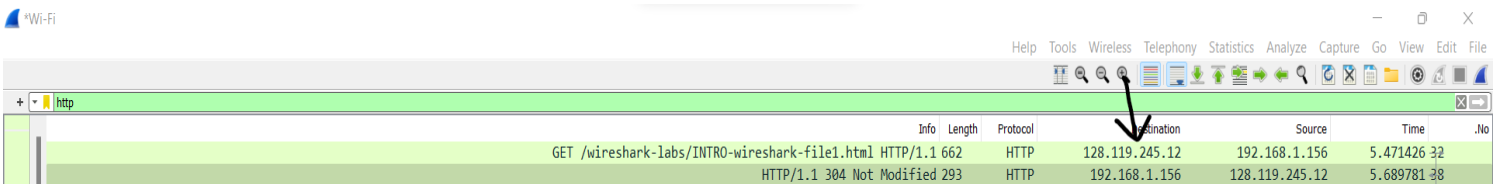
1.TCP.
2.HTTP.
3.DNS.



Q2- As you can see in the image below, the time of the GET request took 5.471426 and the OK respond took 5.689781 , it means that all the request took 0.218355 sec.



<u>Q3-</u> As you can see in the image below, the IP address of gaia.cd.umass.edu is 128.119.245.12.
My IP address id 192.168.1.156.

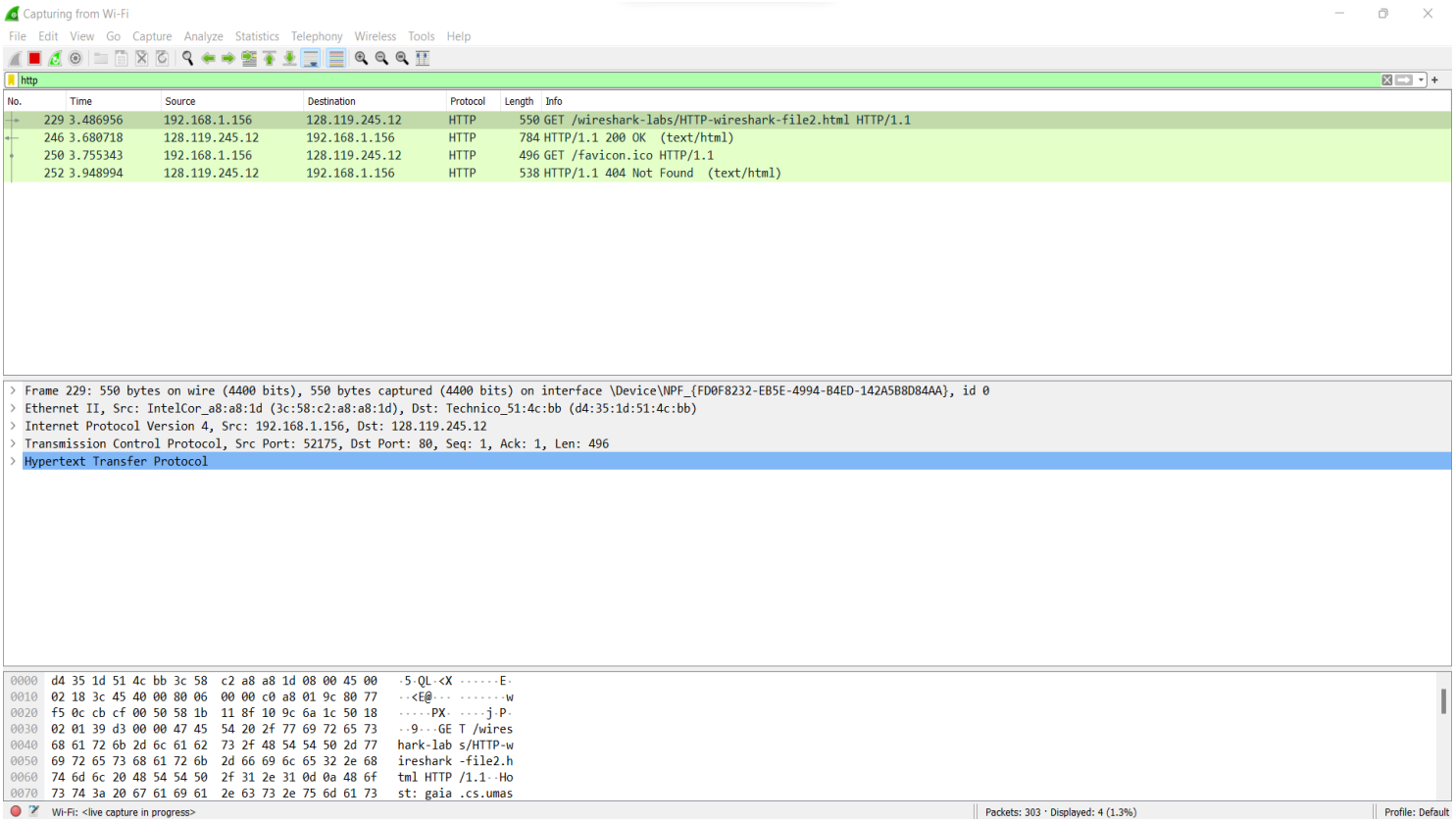


<u>Q4-</u> As you can see in the image below, if we would like to print our OK and GET requests, we can do so.

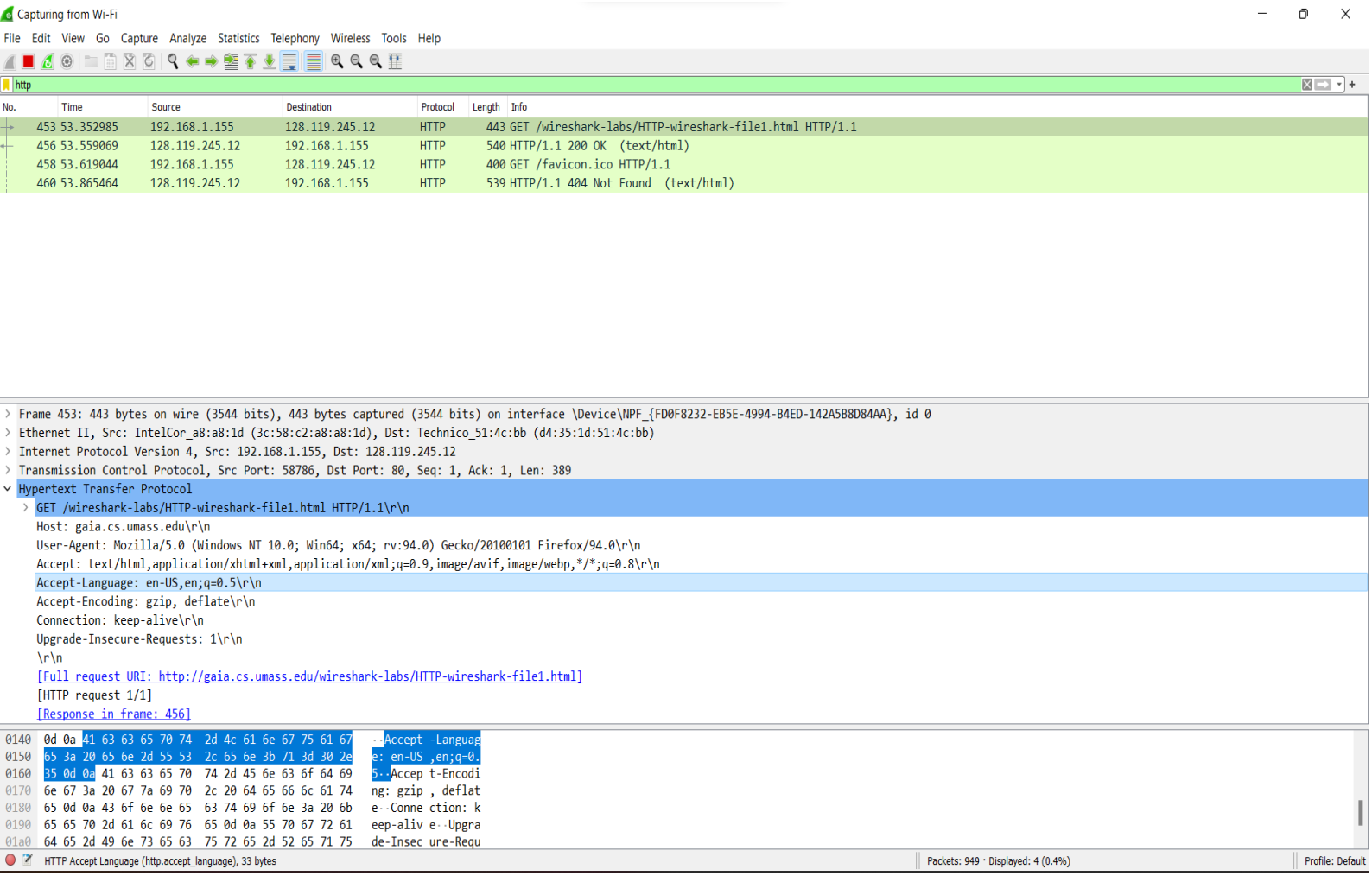
```
    38 5.689781       128.119.245.12        192.168.1.156         HTTP     293    HTTP/1.1 304 Not Modified
Frame 38: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
    Interface id: 0 (\Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  4, 2021 17:53:26.994234000 Jerusalem Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1636041206.994234000 seconds
    [Time delta from previous captured frame: 0.000859000 seconds]
    [Time delta from previous displayed frame: 0.218355000 seconds]
    [Time since reference or first frame: 5.689781000 seconds]
    Frame Number: 38
    Frame Length: 293 bytes (2344 bits)
    Capture Length: 293 bytes (2344 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.156
Transmission Control Protocol, Src Port: 80, Dst Port: 52013, Seq: 1, Ack: 609, Len: 239
Hypertext Transfer Protocol
```

Part 2-

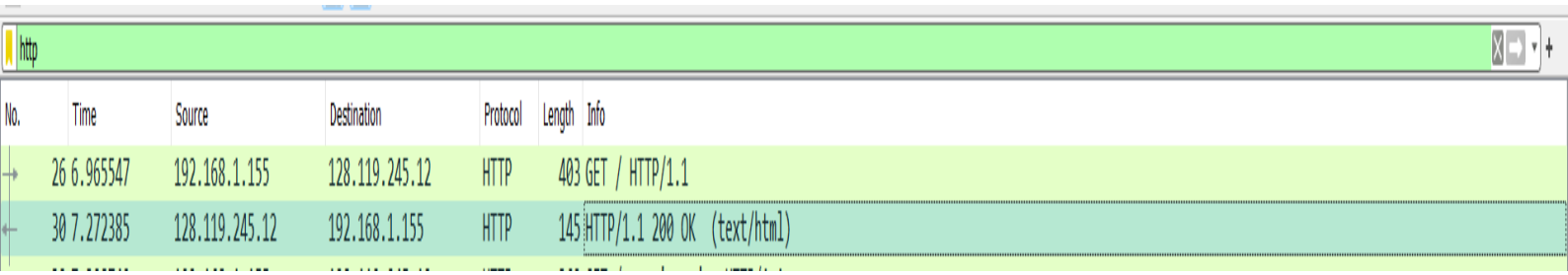
Q1- As you can see in the image below, my browser use HTTP 1.1.



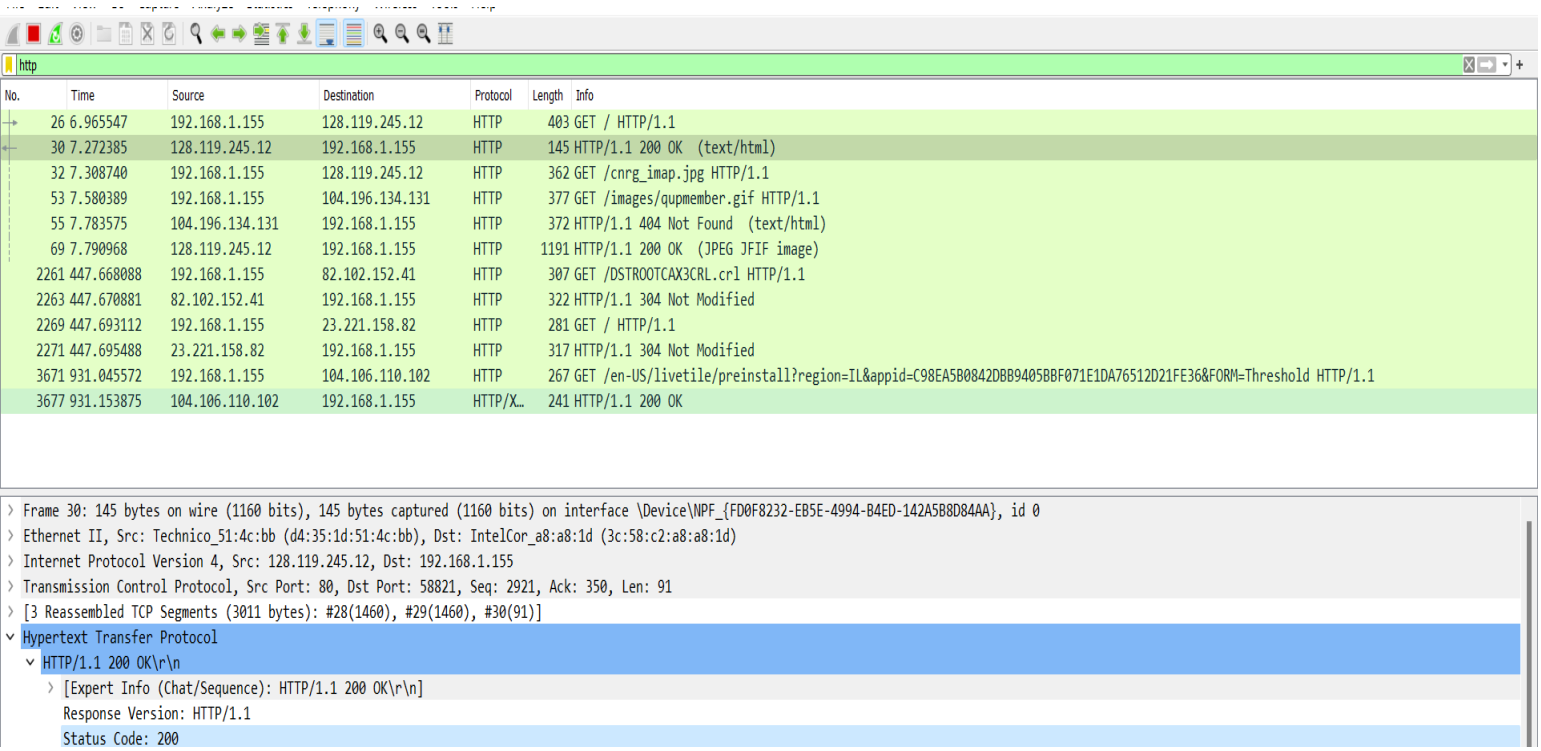
<u>Q2-</u> As you can see in the image below, I have marked the language which our WireShark work with, and as we can see, its English.



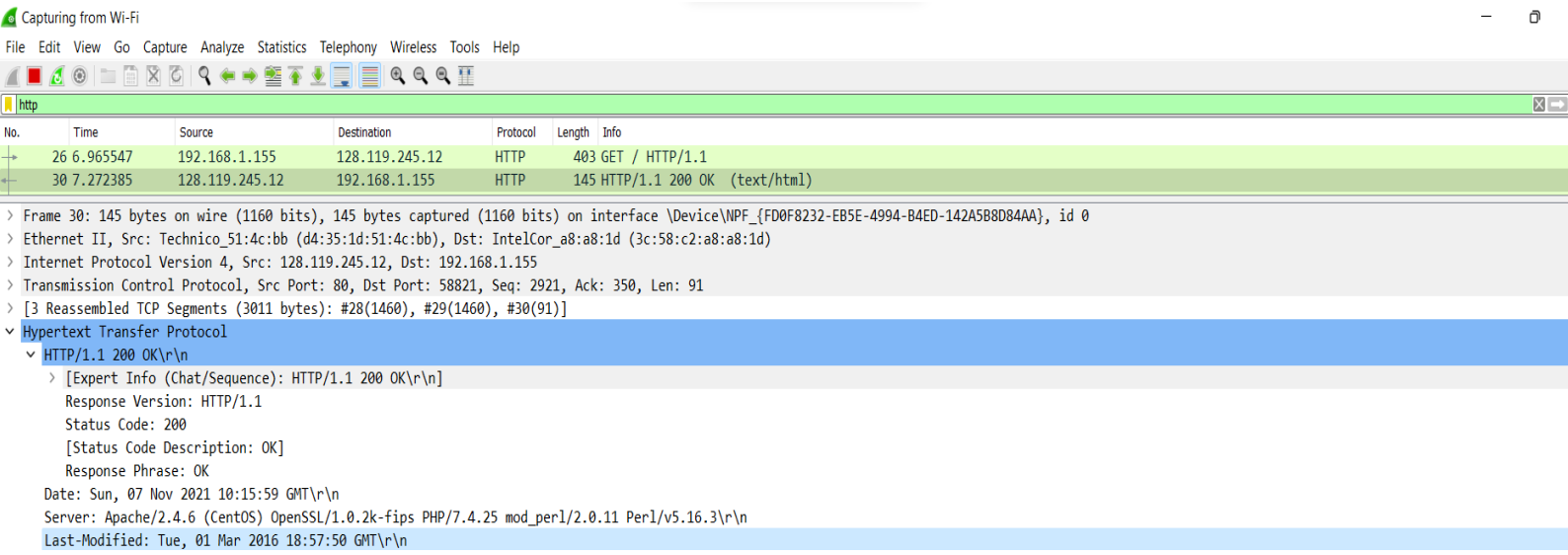
<u>Q3-</u> As you can see in the image below, the source IP (which is my computer IP) is 192.168.1.155.
And gaia.cs.umass.edu's IP is 128.119.245.12.



Q4- **As you can see in the image below, the status code is 200 (which I marked below).**



Q5- **As you can see in the image below, every html file has a date which show when it was last modified, in our case, the html file was last modified in Tuesday, 01 March 2016 18:57:50.**



Q6- **As you can see in the image below, the number of bite, which returned from my browser, are 2651.**

http

No.	Time	Source	Destination	Protocol	Length	Info
26	6.965547	192.168.1.155	128.119.245.12	HTTP	403	GET / HTTP/1.1
30	7.272385	128.119.245.12	192.168.1.155	HTTP	145	HTTP/1.1 200 OK (text/html)

```
> Frame 30: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 58821, Seq: 2921, Ack: 350, Len: 91
> [3 Reassembled TCP Segments (3011 bytes): #28(1460), #29(1460), #30(91)]
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: Sun, 07 Nov 2021 10:15:59 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
    Last-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\n
    ETag: "a5b-52d015789ee9e"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 2651\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: 0.306838000 seconds]
    [Request in frame: 26]
    [Request URI: http://gaia.cs.umass.edu/]
    File Data: 2651 bytes
```

Q7- **As you can see in the image below there are exactly the same number of content file and file data, so the answer is: No, there is no data which not display.**

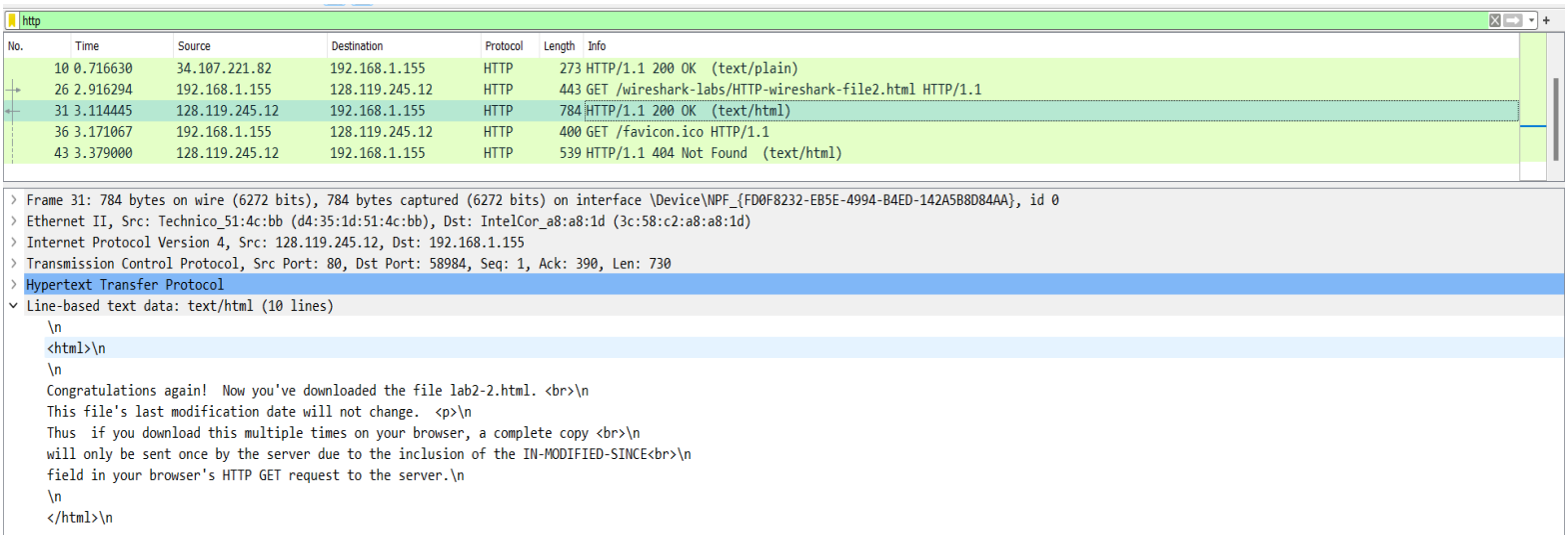
http

No.	Time	Source	Destination	Protocol	Length	Info
26	6.965547	192.168.1.155	128.119.245.12	HTTP	403	GET / HTTP/1.1
30	7.272385	128.119.245.12	192.168.1.155	HTTP	145	HTTP/1.1 200 OK (text/html)

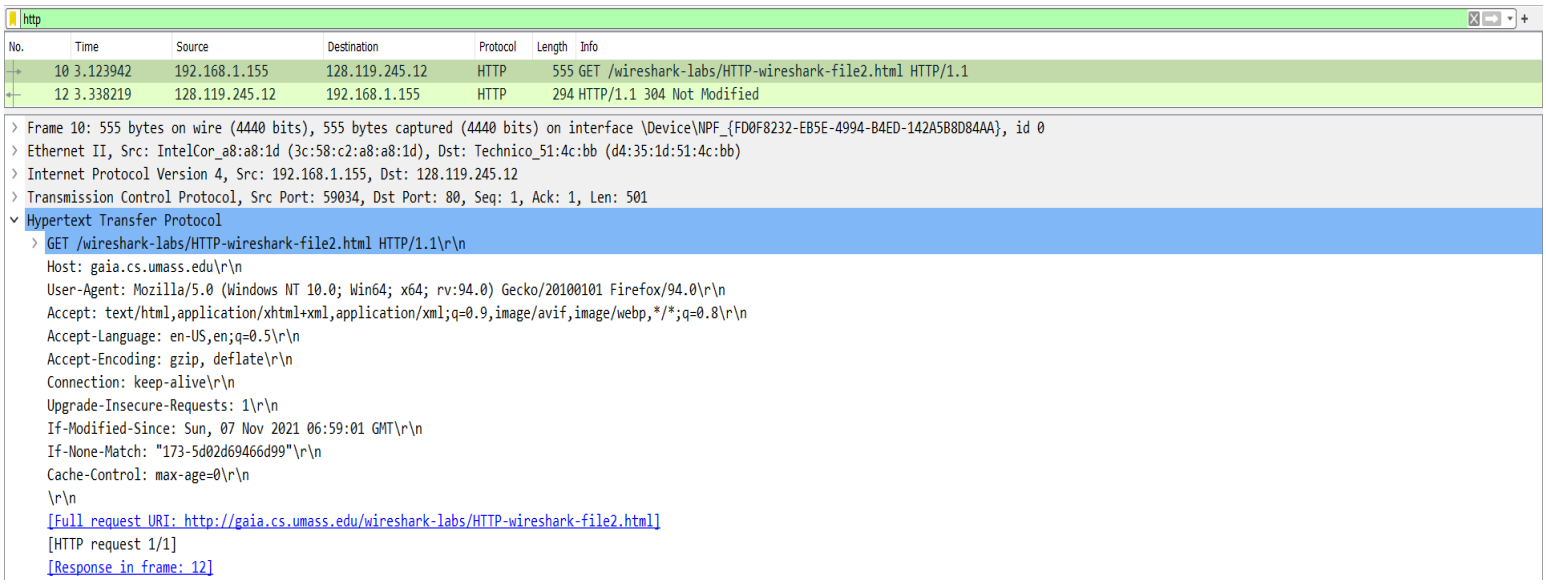
```
> Frame 30: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 58821, Seq: 2921, Ack: 350, Len: 91
> [3 Reassembled TCP Segments (3011 bytes): #28(1460), #29(1460), #30(91)]
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: Sun, 07 Nov 2021 10:15:59 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
    Last-Modified: Tue, 01 Mar 2016 18:57:50 GMT\r\n
    ETag: "a5b-52d015789ee9e"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 2651\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: 0.306838000 seconds]
    [Request in frame: 26]
    [Request URI: http://gaia.cs.umass.edu/]
    File Data: 2651 bytes
```

<u>Q8-</u> No, we cannot see the Last Modified information in GET requests.

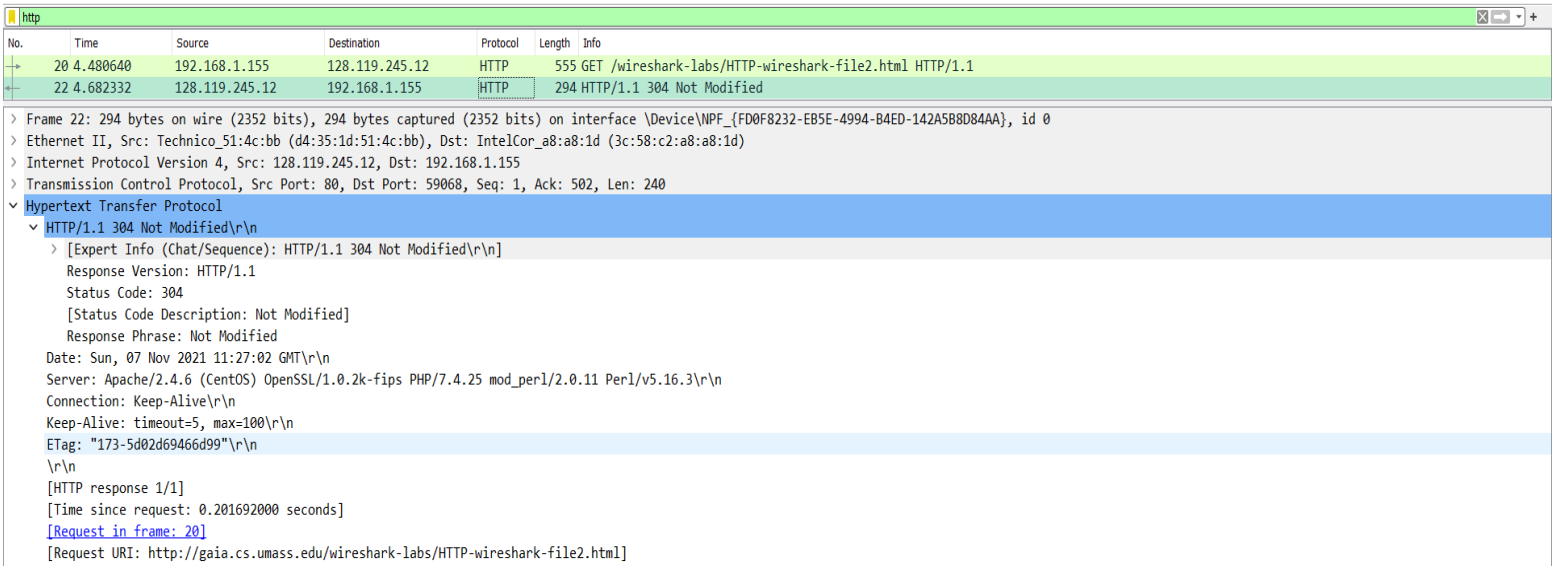
<u>Q9-</u> As you can see in the image below, the html content in our inspecting is exactly like the browser content.



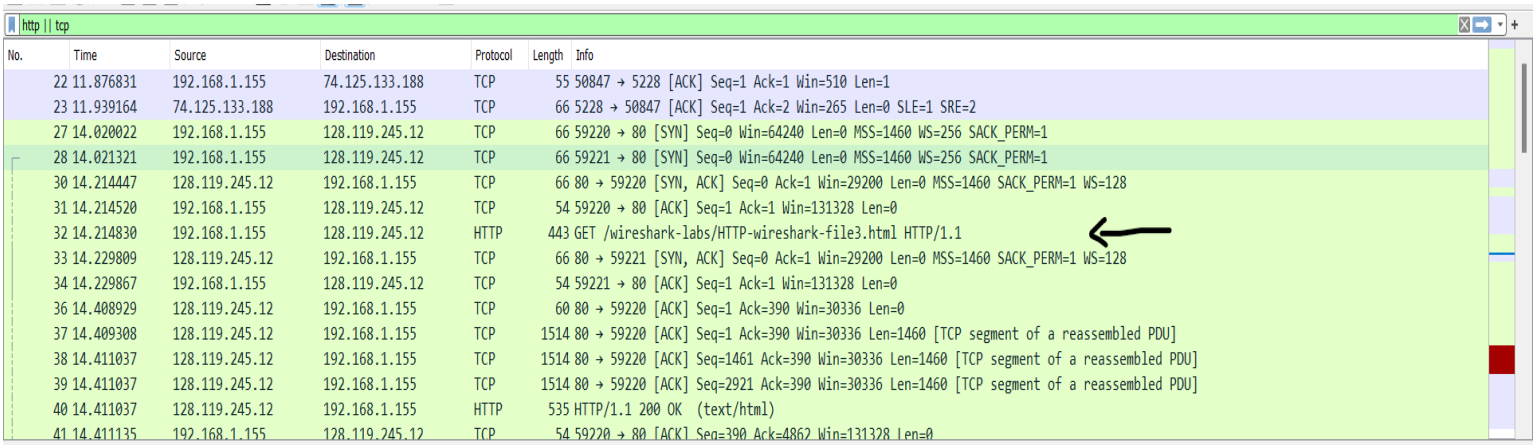
<u>Q10-</u> Yes, As we can see in the second get request, now we can see the "IF-Modified-Since", and the date is Sunday, 07 November, 2021 06:59:01.



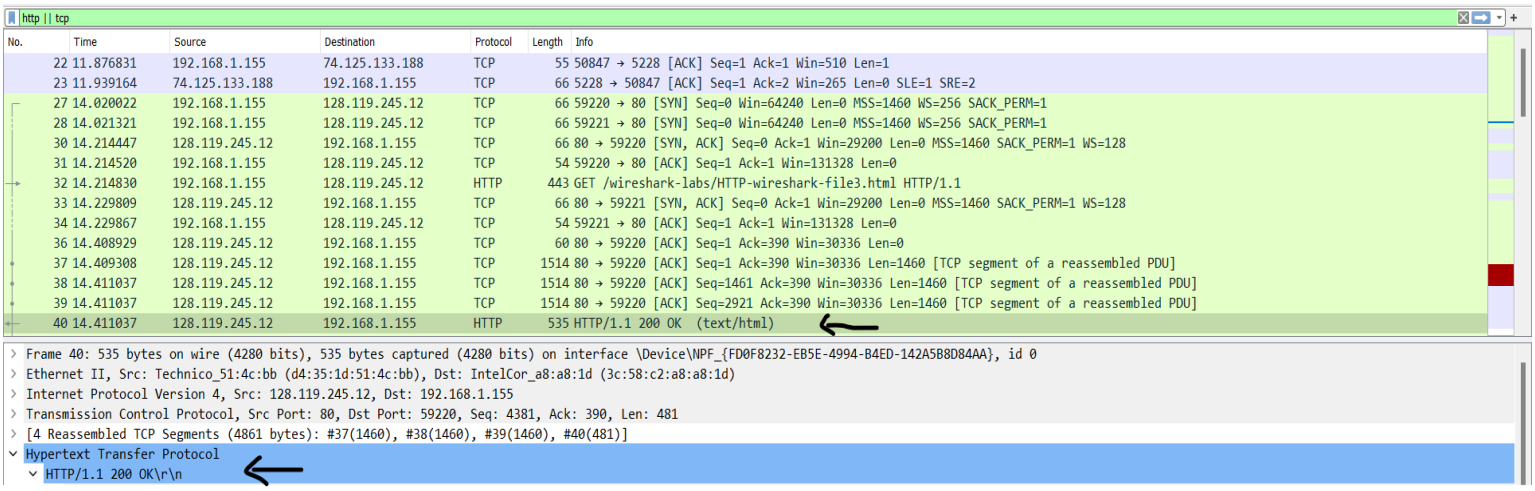
<u>Q11-</u> The HTTP status code which return is 304, and the phrase contents which returned in "Not Modified".
Right now we see that the contents which return is not the file content, the reason for that is that the status code is "Not Modified", all of the details we got from the website at the first time we visit in is already saved in my computer. In addition, we see that this packet is much smaller than the first time we visit this website.



<u>Q12-</u> There is only one GET request for Bill or Rights and the number of packet is 32.



Q13- **As you can see in the image below, it contain the message "OK", the number of packet is 40.**

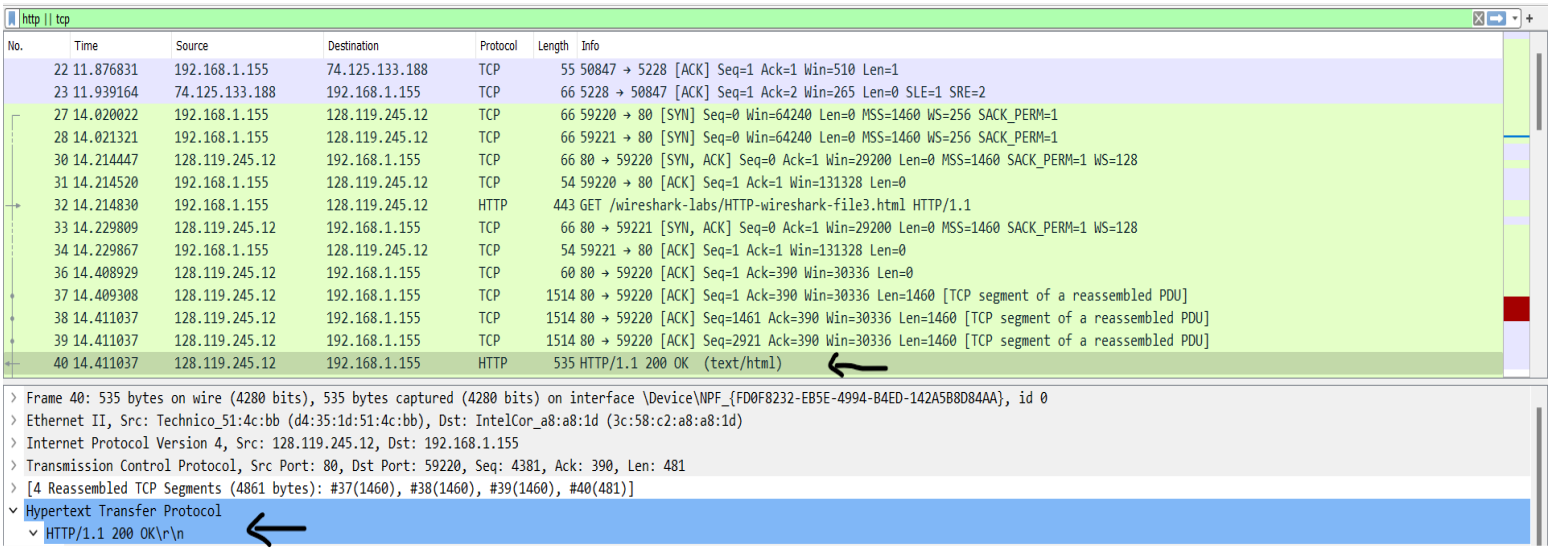


http || tcp

No.	Time	Source	Destination	Protocol	Length	Info
22	11.876831	192.168.1.155	74.125.133.188	TCP	55	50847 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
23	11.939164	74.125.133.188	192.168.1.155	TCP	66	5228 → 50847 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
27	14.020022	192.168.1.155	128.119.245.12	TCP	66	59220 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28	14.021321	192.168.1.155	128.119.245.12	TCP	66	59221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	14.214447	128.119.245.12	192.168.1.155	TCP	66	80 → 59220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
31	14.214520	192.168.1.155	128.119.245.12	TCP	54	59220 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
32	14.214830	192.168.1.155	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
33	14.229809	128.119.245.12	192.168.1.155	TCP	66	80 → 59221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
34	14.229867	192.168.1.155	128.119.245.12	TCP	54	59221 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
36	14.408929	128.119.245.12	192.168.1.155	TCP	60	80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=0
37	14.409308	128.119.245.12	192.168.1.155	TCP	1514	80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
38	14.411037	128.119.245.12	192.168.1.155	TCP	1514	80 → 59220 [ACK] Seq=1461 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
39	14.411037	128.119.245.12	192.168.1.155	TCP	1514	80 → 59220 [ACK] Seq=2921 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
40	14.411037	128.119.245.12	192.168.1.155	HTTP	535	HTTP/1.1 200 OK (text/html)

```
> Frame 40: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 59220, Seq: 4381, Ack: 390, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #37(1460), #38(1460), #39(1460), #40(481)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
```

Q14- **As we can see in the image below the status code is 200, and the response phrase is "OK".**



http || tcp

No.	Time	Source	Destination	Protocol	Length	Info
22	11.876831	192.168.1.155	74.125.133.188	TCP	55	50847 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
23	11.939164	74.125.133.188	192.168.1.155	TCP	66	5228 → 50847 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
27	14.020022	192.168.1.155	128.119.245.12	TCP	66	59220 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28	14.021321	192.168.1.155	128.119.245.12	TCP	66	59221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
30	14.214447	128.119.245.12	192.168.1.155	TCP	66	80 → 59220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
31	14.214520	192.168.1.155	128.119.245.12	TCP	54	59220 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
32	14.214830	192.168.1.155	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
33	14.229809	128.119.245.12	192.168.1.155	TCP	66	80 → 59221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
34	14.229867	192.168.1.155	128.119.245.12	TCP	54	59221 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
36	14.408929	128.119.245.12	192.168.1.155	TCP	60	80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=0
37	14.409308	128.119.245.12	192.168.1.155	TCP	1514	80 → 59220 [ACK] Seq=1 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
38	14.411037	128.119.245.12	192.168.1.155	TCP	1514	80 → 59220 [ACK] Seq=1461 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
39	14.411037	128.119.245.12	192.168.1.155	TCP	1514	80 → 59220 [ACK] Seq=2921 Ack=390 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
40	14.411037	128.119.245.12	192.168.1.155	HTTP	535	HTTP/1.1 200 OK (text/html)

```
> Frame 40: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 59220, Seq: 4381, Ack: 390, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #37(1460), #38(1460), #39(1460), #40(481)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
```

Q15- **As we can see in the image below , there are 4 TCP response, the size of 3 of them is 1460 bytes and the last one is 471 bytes.**

0

http

No.	Time	Source	Destination	Protocol	Length	Info
32	14.214830	192.168.1.155	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
40	14.411037	128.119.245.12	192.168.1.155	HTTP	535	HTTP/1.1 200 OK (text/html)
50	14.477161	192.168.1.155	128.119.245.12	HTTP	400	GET /favicon.ico HTTP/1.1
56	14.686122	128.119.245.12	192.168.1.155	HTTP	539	HTTP/1.1 404 Not Found (text/html)

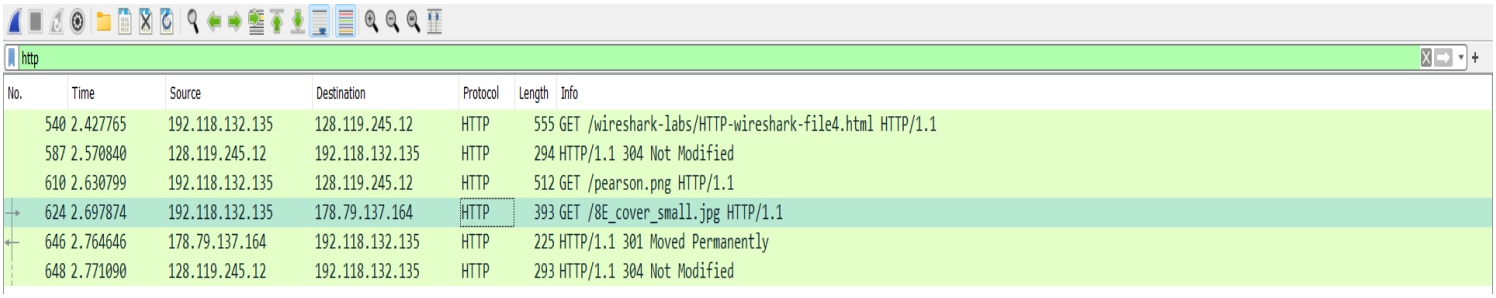
```
> Frame 40: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: Technico_51:4c:bb (d4:35:1d:51:4c:bb), Dst: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
> Transmission Control Protocol, Src Port: 80, Dst Port: 59220, Seq: 4381, Ack: 390, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #37(1460), #38(1460), #39(1460), #40(481)]
    [Frame: 37, payload: 0-1459 (1460 bytes)]
    [Frame: 38, payload: 1460-2919 (1460 bytes)]
    [Frame: 39, payload: 2920-4379 (1460 bytes)]
    [Frame: 40, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203037204e6f762032…]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

<u>Q16-</u> As you can see in the image below, the are 3 GET requests messages.
Two of them sent to IP 128.119.245.12 (gaia's website),
the other one sent to IP 178.79.137.164 (the cover book's website).

http

No.	Time	Source	Destination	Protocol	Length	Info
540	2.427765	192.118.132.135	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
587	2.570840	128.119.245.12	192.118.132.135	HTTP	294	HTTP/1.1 304 Not Modified
610	2.630799	192.118.132.135	128.119.245.12	HTTP	512	GET /pearson.png HTTP/1.1
624	2.697874	192.118.132.135	178.79.137.164	HTTP	393	GET /8E_cover_small.jpg HTTP/1.1
646	2.764646	178.79.137.164	192.118.132.135	HTTP	225	HTTP/1.1 301 Moved Permanently
648	2.771090	128.119.245.12	192.118.132.135	HTTP	293	HTTP/1.1 304 Not Modified

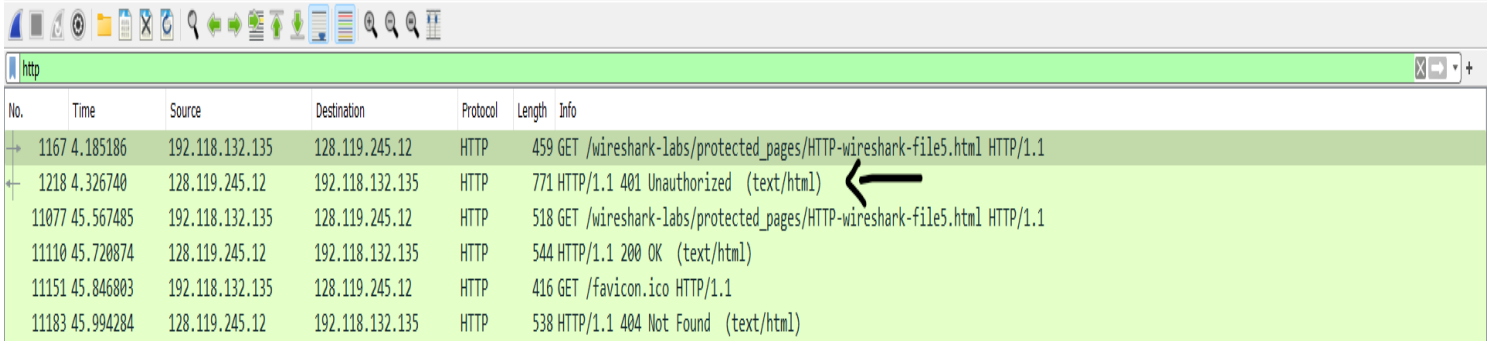
<u>Q17-</u> As we can see in the image below, every GET requests for each of the images is standing independently and serially, and as we can see, every GET request is closed and have different TCP connections.



http

No.	Time	Source	Destination	Protocol	Length	Info
540	2.427765	192.118.132.135	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
587	2.570840	128.119.245.12	192.118.132.135	HTTP	294	HTTP/1.1 304 Not Modified
610	2.630799	192.118.132.135	128.119.245.12	HTTP	512	GET /pearson.png HTTP/1.1
624	2.697874	192.118.132.135	178.79.137.164	HTTP	393	GET /8E_cover_small.jpg HTTP/1.1
646	2.764646	178.79.137.164	192.118.132.135	HTTP	225	HTTP/1.1 301 Moved Permanently
648	2.771090	128.119.245.12	192.118.132.135	HTTP	293	HTTP/1.1 304 Not Modified

<u>Q18-</u> As we can see in the image below, the status code is 401. And the phrase is "Unauthorized".



http

No.	Time	Source	Destination	Protocol	Length	Info
1167	4.185186	192.118.132.135	128.119.245.12	HTTP	459	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1218	4.326740	128.119.245.12	192.118.132.135	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
11077	45.567485	192.118.132.135	128.119.245.12	HTTP	518	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
11110	45.720874	128.119.245.12	192.118.132.135	HTTP	544	HTTP/1.1 200 OK (text/html)
11151	45.846803	192.118.132.135	128.119.245.12	HTTP	416	GET /favicon.ico HTTP/1.1
11183	45.994284	128.119.245.12	192.118.132.135	HTTP	538	HTTP/1.1 404 Not Found (text/html)

<u>Q19-</u> As you can see in the image below, the new field which added is the "Authorization" field

11077	45.567485	192.118.132.135	128.119.245.12	HTTP	518 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
11110	45.720874	128.119.245.12	192.118.132.135	HTTP	544 HTTP/1.1 200 OK (text/html)
11151	45.846803	192.118.132.135	128.119.245.12	HTTP	416 GET /favicon.ico HTTP/1.1
11183	45.994284	128.119.245.12	192.118.132.135	HTTP	538 HTTP/1.1 404 Not Found (text/html)

```
> Frame 11077: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on interface \Device\NPF_{FD0F8232-EB5E-4994-B4ED-142A5B8D84AA}, id 0
> Ethernet II, Src: IntelCor_a8:a8:1d (3c:58:c2:a8:a8:1d), Dst: PaloAlto_35:ea:30 (84:d4:12:35:ea:30)
> Internet Protocol Version 4, Src: 192.118.132.135, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59806, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
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
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    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
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/2]
    [Response in frame: 11110]
    [Next request in frame: 11151]
```