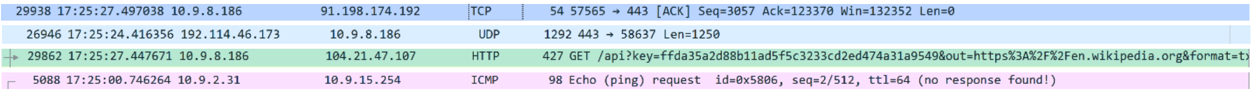
Assignment-1

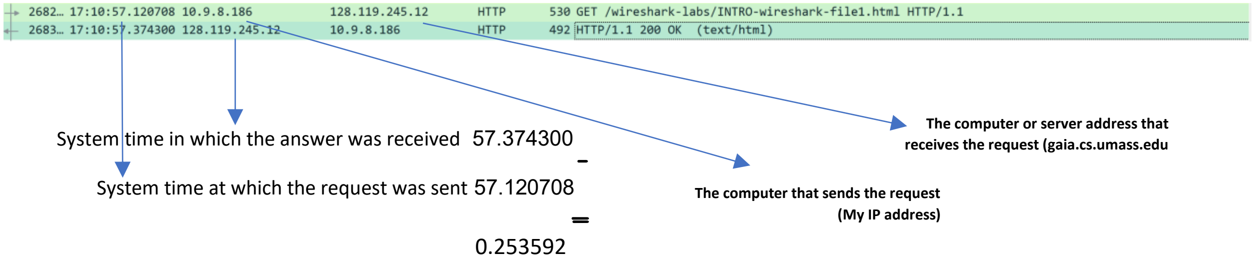
1. We will present three different protocols that appeared when recording the packets passing through the Internet and were recorded using the Wireshark
    - TCP
    - UDP
    - HTTP
    - ICMP



```
29938 17:25:27.497038 10.9.8.186        91.198.174.192    TCP     54 57565 → 443 [ACK] Seq=3057 Ack=123370 Win=132352 Len=0
 26946 17:25:24.416356 192.114.46.173    10.9.8.186       UDP   1292 443 → 58637 Len=1250
 29862 17:25:27.447671 10.9.8.186        104.21.47.107    HTTP   427 GET /api?key=ffda35a2d88b11ad5f5c3233cd2ed474a31a9549&out=https%3A%2F%2Fen.wikipedia.org&format=tx
  5088 17:25:00.746264 10.9.2.31         10.9.15.254      ICMP    98 Echo (ping) request  id=0x5806, seq=2/512, ttl=64 (no response found!)
```

2. Duration of time to receive a response from the receiving party is about 0.253592 ms which is about 2.54 × 10-4 s.
Time calculation was performed by examining the time difference between the time of sending the request to the point where the response returned from the server and therefore the difference expresses the time of receiving the answer.

3.



```
2682… 17:10:57.120708 10.9.8.186      128.119.245.12   HTTP   530 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2683… 17:10:57.374300 128.119.245.12  10.9.8.186       HTTP   492 HTTP/1.1 200 OK  (text/html)
```

System time in which the answer was received 57.374300

-

System time at which the request was sent 57.120708

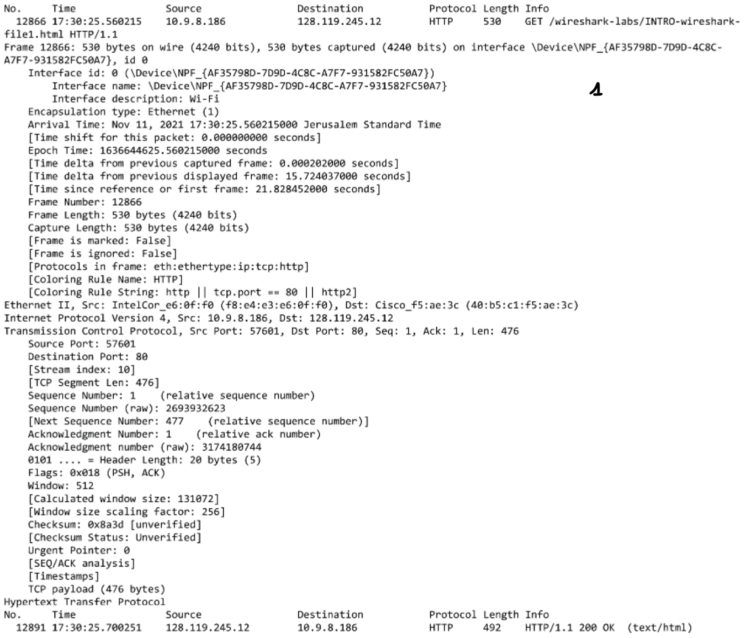
=

0.253592

The computer or server address that receives the request (gaia.cs.umass.edu

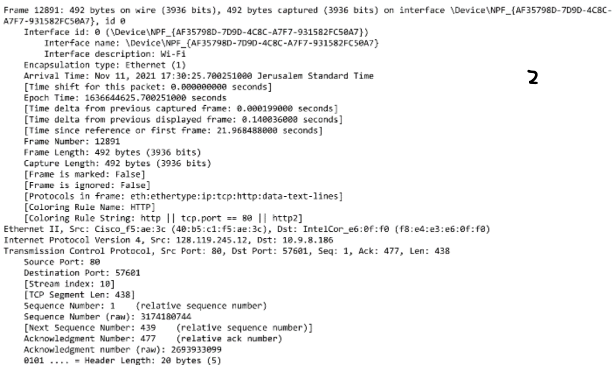
The computer that sends the request (My IP address)

4.



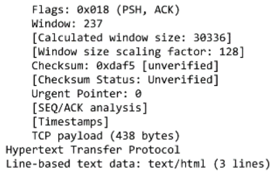
1

```
No.     Time               Source                Destination           Protocol Length Info
  12866 17:30:25.560215    10.9.8.186            128.119.245.12        HTTP     530    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 12866: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-
A7F7-931582FC50A7}, id 0
    Interface id: 0 (\Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7})
        Interface name: \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 11, 2021 17:30:25.560215000 Jerusalem Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1636644625.560215000 seconds
    [Time delta from previous captured frame: 0.000202000 seconds]
    [Time delta from previous displayed frame: 15.724037000 seconds]
    [Time since reference or first frame: 21.828452000 seconds]
    Frame Number: 12866
    Frame Length: 530 bytes (4240 bits)
    Capture Length: 530 bytes (4240 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: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: Cisco_f5:ae:3c (40:b5:c1:f5:ae:3c)
Internet Protocol Version 4, Src: 10.9.8.186, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57601, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
    Source Port: 57601
    Destination Port: 80
    [Stream index: 10]
    [TCP Segment Len: 476]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2693932623
    [Next Sequence Number: 477    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3174180744
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0x8a3d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (476 bytes)
Hypertext Transfer Protocol
No.     Time               Source                Destination           Protocol Length Info
  12891 17:30:25.700251    128.119.245.12        10.9.8.186            HTTP     492    HTTP/1.1 200 OK  (text/html)
```



2

```
Frame 12891: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-
A7F7-931582FC50A7}, id 0
    Interface id: 0 (\Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7})
        Interface name: \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 11, 2021 17:30:25.700251000 Jerusalem Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1636644625.700251000 seconds
    [Time delta from previous captured frame: 0.000199000 seconds]
    [Time delta from previous displayed frame: 0.140036000 seconds]
    [Time since reference or first frame: 21.968488000 seconds]
    Frame Number: 12891
    Frame Length: 492 bytes (3936 bits)
    Capture Length: 492 bytes (3936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Cisco_f5:ae:3c (40:b5:c1:f5:ae:3c), Dst: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.9.8.186
Transmission Control Protocol, Src Port: 80, Dst Port: 57601, Seq: 1, Ack: 477, Len: 438
    Source Port: 80
    Destination Port: 57601
    [Stream index: 10]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3174180744
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 477    (relative ack number)
    Acknowledgment number (raw): 2693933099
    0101 .... = Header Length: 20 bytes (5)
```

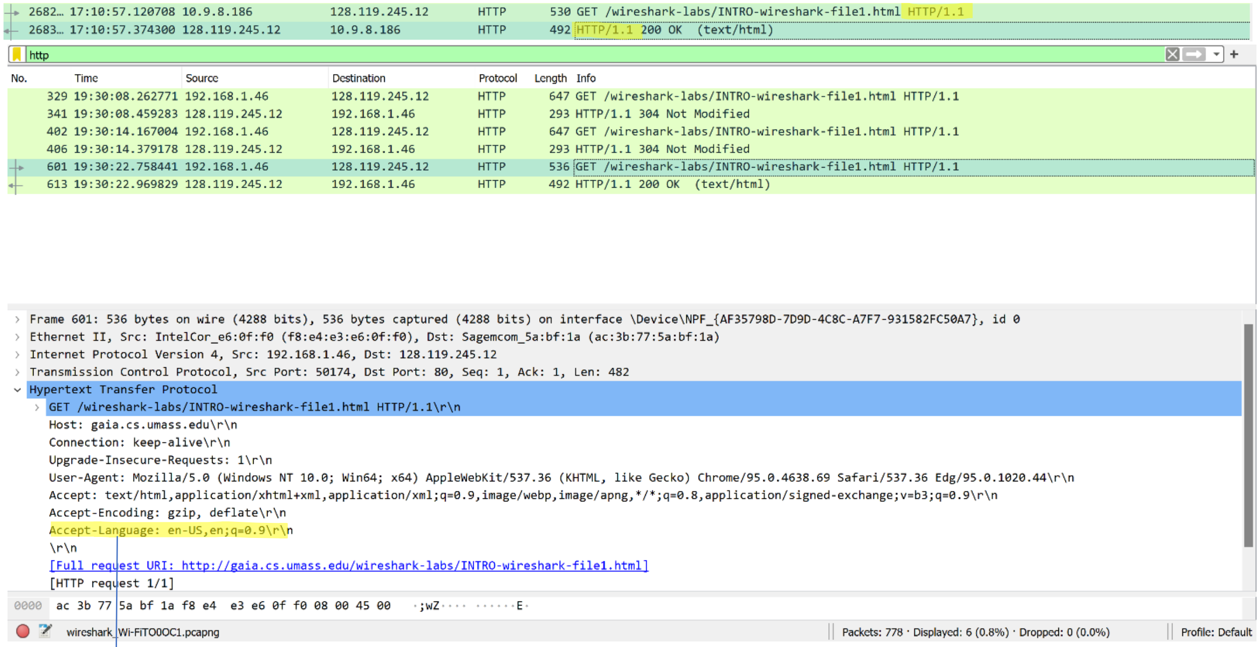


3

```
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xdaf5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

Assignment-1

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



```
2682… 17:10:57.120708 10.9.8.186       128.119.245.12   HTTP   530 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2683… 17:10:57.374300 128.119.245.12   10.9.8.186       HTTP   492 HTTP/1.1 200 OK  (text/html)

http

No.   Time            Source          Destination     Protocol Length Info
  329 19:30:08.262771 192.168.1.46    128.119.245.12  HTTP     647 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  341 19:30:08.459283 128.119.245.12  192.168.1.46    HTTP     293 HTTP/1.1 304 Not Modified
  402 19:30:14.167004 192.168.1.46    128.119.245.12  HTTP     647 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  406 19:30:14.379178 128.119.245.12  192.168.1.46    HTTP     293 HTTP/1.1 304 Not Modified
  601 19:30:22.758441 192.168.1.46    128.119.245.12  HTTP     536 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  613 19:30:22.969829 128.119.245.12  192.168.1.46    HTTP     492 HTTP/1.1 200 OK  (text/html)

> Frame 601: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0), Dst: Sagemcom_5a:bf:1a (ac:3b:77:5a:bf:1a)
> Internet Protocol Version 4, Src: 192.168.1.46, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50174, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-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, like Gecko) Chrome/95.0.4638.69 Safari/537.36 Edg/95.0.1020.44\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
0000  ac 3b 77 5a bf 1a f8 e4  e3 e6 0f f0 08 00 45 00   ·;wZ···· ······E·

wireshark_Wi-FiTO0OC1.pcapng          Packets: 778 · Displayed: 6 (0.8%) · Dropped: 0 (0.0%)          Profile: Default
```

- HTTP 1.1

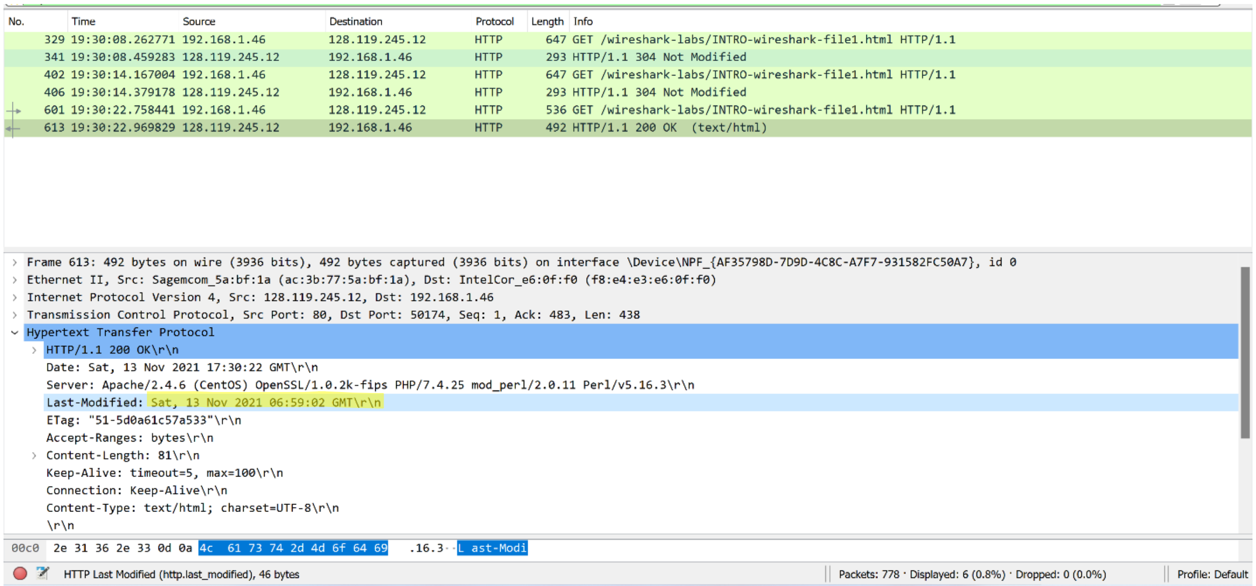
2. What languages (if any) does your browser indicate that it can accept to the server?
   - **Is en-US.**

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   - Of my computer is **192.168.1.46** and gaia.cs.umass.edu is **128.119.245.12**

4. What is the status code returned from the server to your browser?
   - Status code is **(200 OK)** success status response code indicates that the request has succeeded

Assignment-1

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



```
No.   Time             Source          Destination     Protocol  Length  Info
  329 19:30:08.262771 192.168.1.46    128.119.245.12  HTTP       647 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  341 19:30:08.459283 128.119.245.12  192.168.1.46    HTTP       293 HTTP/1.1 304 Not Modified
  402 19:30:14.167004 192.168.1.46    128.119.245.12  HTTP       647 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  406 19:30:14.379178 128.119.245.12  192.168.1.46    HTTP       293 HTTP/1.1 304 Not Modified
  601 19:30:22.758441 192.168.1.46    128.119.245.12  HTTP       536 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  613 19:30:22.969829 128.119.245.12  192.168.1.46    HTTP       492 HTTP/1.1 200 OK  (text/html)
```

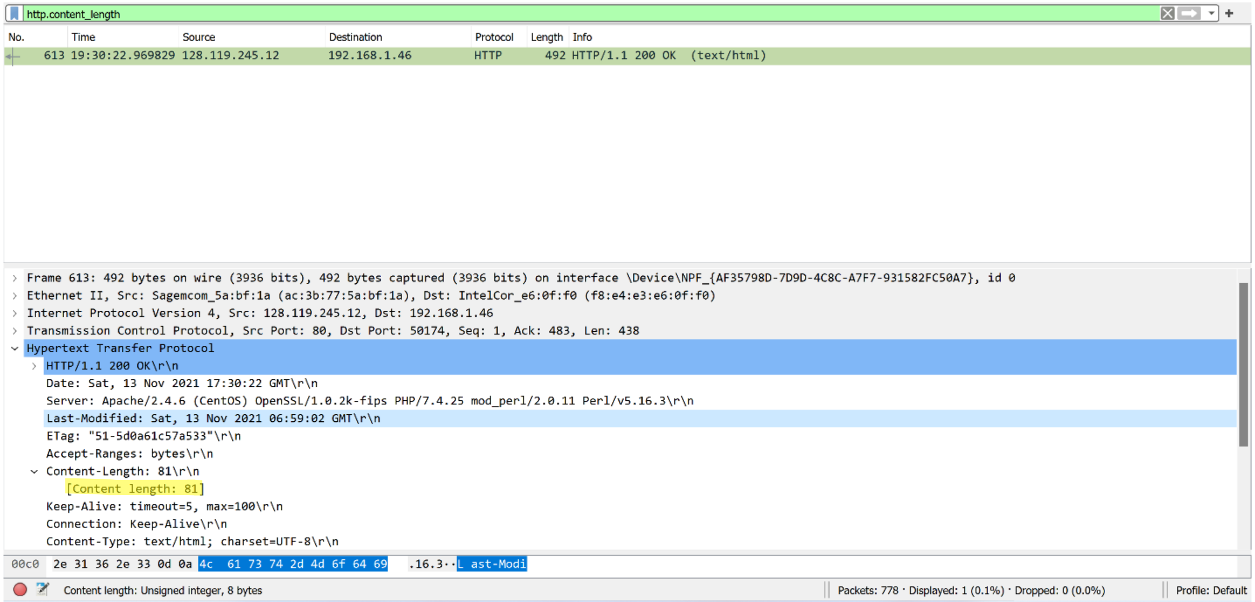
```
> Frame 613: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: Sagemcom_5a:bf:1a (ac:3b:77:5a:bf:1a), Dst: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.46
> Transmission Control Protocol, Src Port: 80, Dst Port: 50174, Seq: 1, Ack: 483, Len: 438
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 13 Nov 2021 17:30:22 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: Sat, 13 Nov 2021 06:59:02 GMT\r\n
    ETag: "51-5d0a61c57a533"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 81\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
```

```
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
```

HTTP Last Modified (http.last_modified), 46 bytes | Packets: 778 · Displayed: 6 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

- on Sat, 13 Nov 2021 06:59:02.
- We can filter messages by http.last_modified

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



http.content_length

```
No.   Time             Source          Destination     Protocol  Length  Info
  613 19:30:22.969829 128.119.245.12  192.168.1.46    HTTP       492 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 613: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{AF35798D-7D9D-4C8C-A7F7-931582FC50A7}, id 0
> Ethernet II, Src: Sagemcom_5a:bf:1a (ac:3b:77:5a:bf:1a), Dst: IntelCor_e6:0f:f0 (f8:e4:e3:e6:0f:f0)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.46
> Transmission Control Protocol, Src Port: 80, Dst Port: 50174, Seq: 1, Ack: 483, Len: 438
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 13 Nov 2021 17:30:22 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: Sat, 13 Nov 2021 06:59:02 GMT\r\n
    ETag: "51-5d0a61c57a533"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 81\r\n
      [Content length: 81]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
```

```
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
```

Content length: Unsigned integer, 8 bytes | Packets: 778 · Displayed: 1 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

- We can filter messages by http.content_length
- Content length is 81 bytes.

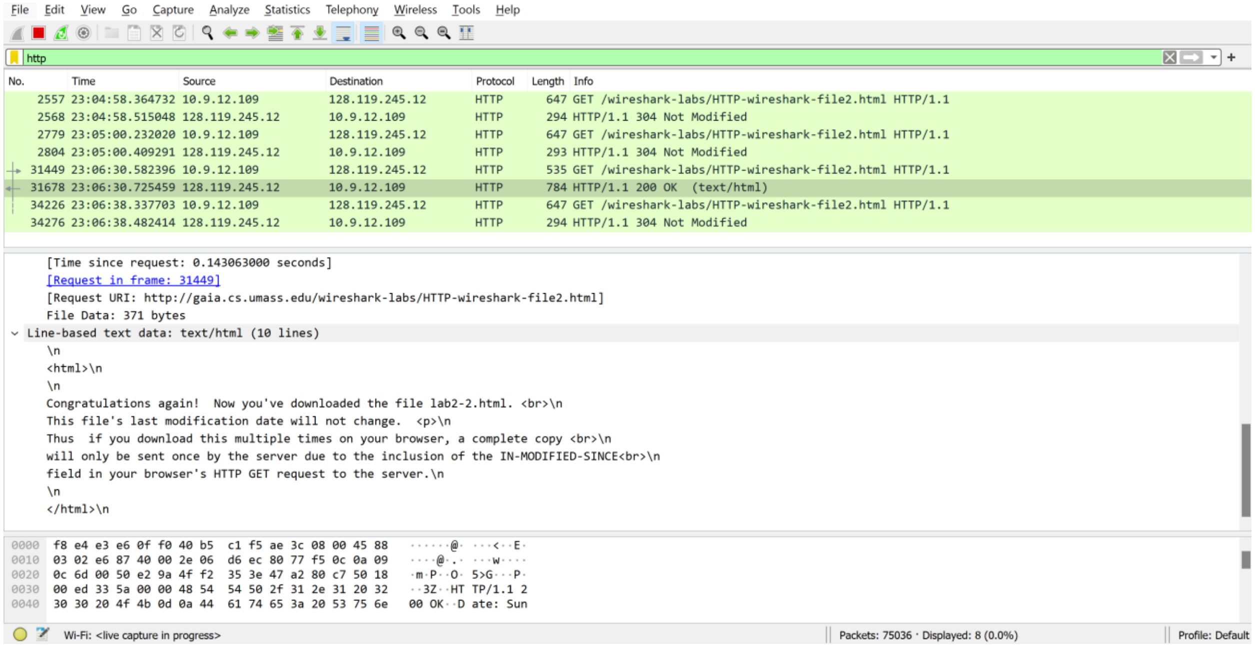
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
   - **<u>I do not see any different headings between the two windows</u>**

Assignment-1

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?

   - **No, I do not see anything.**

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



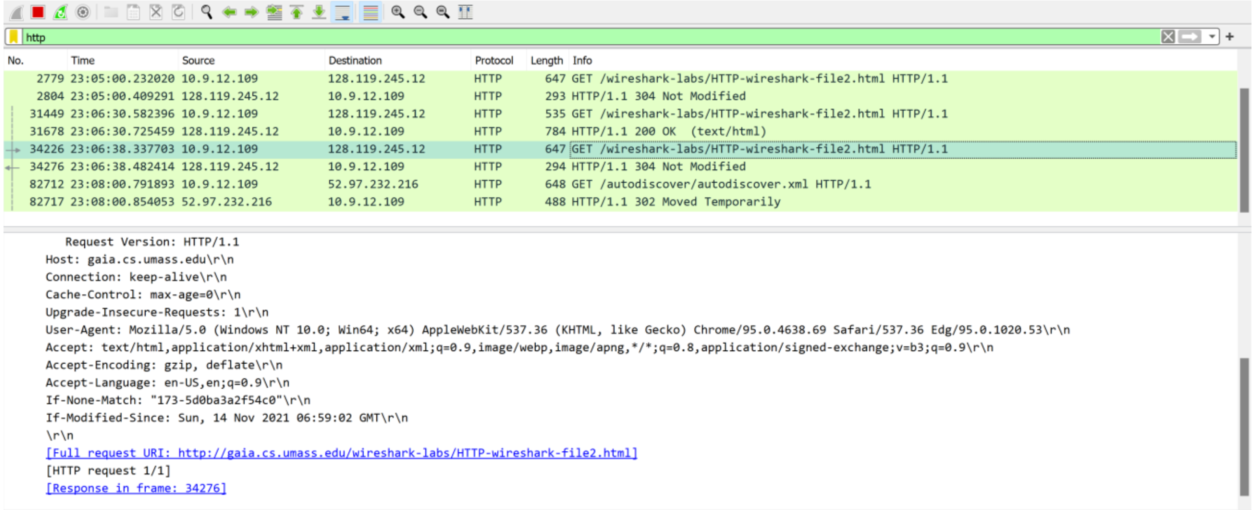
No.	Time	Source	Destination	Protocol	Length	Info
2557	23:04:58.364732	10.9.12.109	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2568	23:04:58.515048	128.119.245.12	10.9.12.109	HTTP	294	HTTP/1.1 304 Not Modified
2779	23:05:00.232020	10.9.12.109	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2804	23:05:00.409291	128.119.245.12	10.9.12.109	HTTP	293	HTTP/1.1 304 Not Modified
31449	23:06:30.582396	10.9.12.109	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
31678	23:06:30.725459	128.119.245.12	10.9.12.109	HTTP	784	HTTP/1.1 200 OK (text/html)
34226	23:06:38.337703	10.9.12.109	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
34276	23:06:38.482414	128.119.245.12	10.9.12.109	HTTP	294	HTTP/1.1 304 Not Modified

```
    [Time since request: 0.143063000 seconds]
    [Request in frame: 31449]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
v 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
```

```
0000  f8 e4 e3 e6 0f f0 40 b5  c1 f5 ae 3c 08 00 45 88   ······@· ···<··E·
0010  03 02 e6 87 40 00 2e 06  d6 ec 80 77 f5 0c 0a 09   ····@·.· ···w····
0020  0c 6d 00 50 e2 9a 4f f2  35 3e 47 a2 80 c7 50 18   ·m·P··O· 5>G···P·
0030  00 ed 33 5a 00 00 48 54  54 50 2f 31 2e 31 20 32   ··3Z··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK··D ate: Sun
```

   - **Line-based text data.**

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?



No.	Time	Source	Destination	Protocol	Length	Info
2779	23:05:00.232020	10.9.12.109	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2804	23:05:00.409291	128.119.245.12	10.9.12.109	HTTP	293	HTTP/1.1 304 Not Modified
31449	23:06:30.582396	10.9.12.109	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
31678	23:06:30.725459	128.119.245.12	10.9.12.109	HTTP	784	HTTP/1.1 200 OK (text/html)
34226	23:06:38.337703	10.9.12.109	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
34276	23:06:38.482414	128.119.245.12	10.9.12.109	HTTP	294	HTTP/1.1 304 Not Modified
82712	23:08:00.791893	10.9.12.109	52.97.232.216	HTTP	648	GET /autodiscover/autodiscover.xml HTTP/1.1
82717	23:08:00.854053	52.97.232.216	10.9.12.109	HTTP	488	HTTP/1.1 302 Moved Temporarily

```
      Request Version: HTTP/1.1
   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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36 Edg/95.0.1020.53\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: en-US,en;q=0.9\r\n
   If-None-Match: "173-5d0ba3a2f54c0"\r\n
   If-Modified-Since: Sun, 14 Nov 2021 06:59:02 GMT\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: 34276]
```

   - **Yes, If-Modified-Since: on Sat, 14 Nov 2021 06:59:02.**

Assignment-1

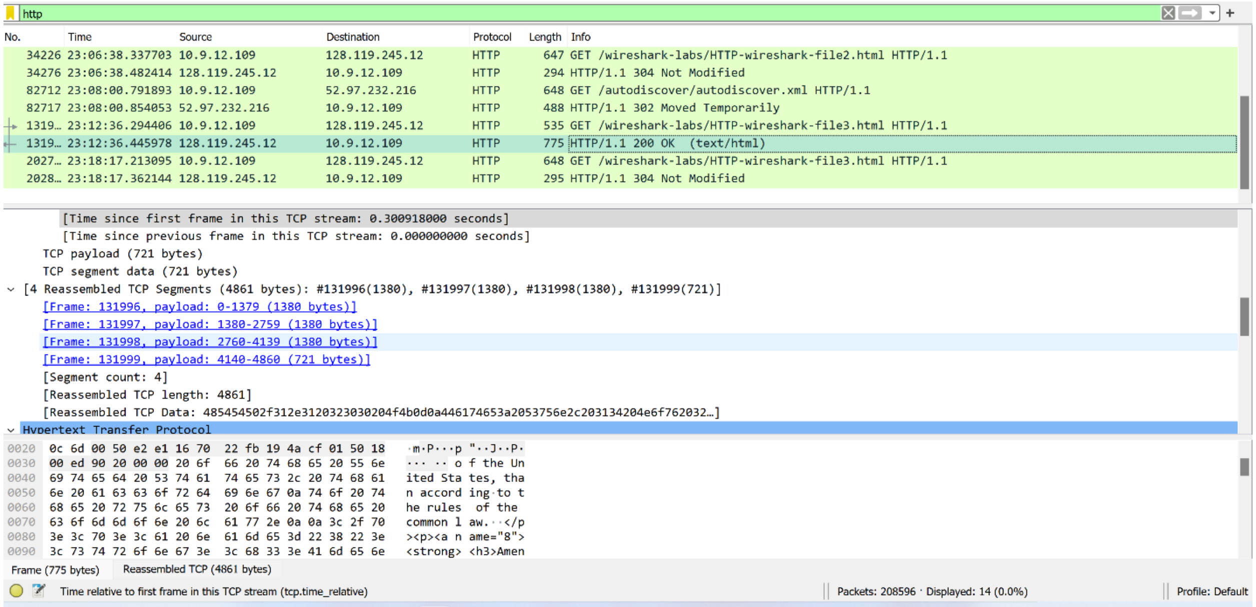
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
    - Screenshot shows that the status code returning from the second capacitor requested operation is 304
    - The HTTP **304 Not Modified** client redirection response code indicates that there is no need to retransmit the requested resources

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?
    - **Single request**

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    - 10

14. What is the status code and phrase in the response?
    - **200 Ok Status code.**

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



```
No.     Time            Source          Destination     Protocol Length Info
  34226 23:06:38.337703 10.9.12.109     128.119.245.12  HTTP      647 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  34276 23:06:38.482414 128.119.245.12  10.9.12.109     HTTP      294 HTTP/1.1 304 Not Modified
  82712 23:08:00.791893 10.9.12.109     52.97.232.216   HTTP      648 GET /autodiscover/autodiscover.xml HTTP/1.1
  82717 23:08:00.854053 52.97.232.216   10.9.12.109     HTTP      488 HTTP/1.1 302 Moved Temporarily
  1319… 23:12:36.294406 10.9.12.109     128.119.245.12  HTTP      535 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  1319… 23:12:36.445978 128.119.245.12  10.9.12.109     HTTP      775 HTTP/1.1 200 OK  (text/html)
  2027… 23:18:17.213095 10.9.12.109     128.119.245.12  HTTP      648 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  2028… 23:18:17.362144 128.119.245.12  10.9.12.109     HTTP      295 HTTP/1.1 304 Not Modified
```

```
        [Time since first frame in this TCP stream: 0.300918000 seconds]
        [Time since previous frame in this TCP stream: 0.000000000 seconds]
     TCP payload (721 bytes)
     TCP segment data (721 bytes)
  [4 Reassembled TCP Segments (4861 bytes): #131996(1380), #131997(1380), #131998(1380), #131999(721)]
     [Frame: 131996, payload: 0-1379 (1380 bytes)]
     [Frame: 131997, payload: 1380-2759 (1380 bytes)]
     [Frame: 131998, payload: 2760-4139 (1380 bytes)]
     [Frame: 131999, payload: 4140-4860 (721 bytes)]
     [Segment count: 4]
     [Reassembled TCP length: 4861]
     [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203134204e6f762032…]
  Hypertext Transfer Protocol
```

```
0020  0c 6d 00 50 e2 e1 16 70  22 fb 19 4a cf 01 50 18   ·m·P···p "··J··P·
0030  00 ed 90 20 00 00 20 6f  66 20 74 68 65 20 55 6e   ··· ·· o f the Un
0040  69 74 65 64 20 53 74 61  74 65 73 2c 20 74 68 61   ited Sta tes, tha
0050  6e 20 61 63 63 6f 72 64  69 6e 67 0a 74 6f 20 74   n accord ing·to t
0060  68 65 20 72 75 6c 65 73  20 6f 66 20 74 68 65 20   he rules  of the
0070  63 6f 6d 6d 6f 6e 20 6c  61 77 2e 0a 0a 3c 2f 70   common l aw.··</p
0080  3e 3c 70 3e 3c 61 20 6e  61 6d 65 3d 22 38 22 3e   ><p><a n ame="8">
0090  3c 73 74 72 6f 6e 67 3e  3c 68 33 3e 41 6d 65 6e   <strong> <h3>Amen
```

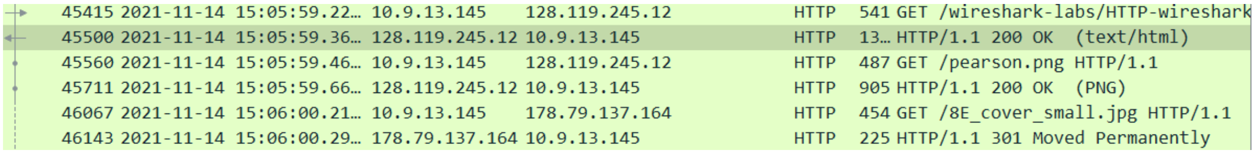
Frame (775 bytes)
Reassembled TCP (4861 bytes)
Time relative to first frame in this TCP stream (tcp.time_relative)
Packets: 208596 · Displayed: 14 (0.0%)
Profile: Default

- It took four TCP segment to carry the single HTTP response and the text of the bill of Rights.

Assignment-1

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

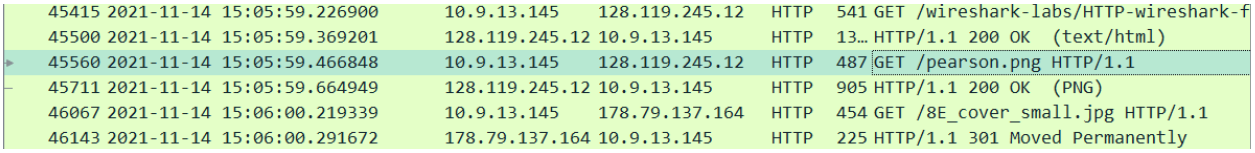
    - Our browser sent three HTTP Get request message, and it sent it to two different addresses And he sent them two addresses (128.119.245.12 , 178.79.137.164).



```
45415 2021-11-14 15:05:59.22… 10.9.13.145     128.119.245.12          HTTP   541 GET /wireshark-labs/HTTP-wireshark
45500 2021-11-14 15:05:59.36… 128.119.245.12 10.9.13.145              HTTP   13… HTTP/1.1 200 OK  (text/html)
45560 2021-11-14 15:05:59.46… 10.9.13.145     128.119.245.12          HTTP   487 GET /pearson.png HTTP/1.1
45711 2021-11-14 15:05:59.66… 128.119.245.12 10.9.13.145              HTTP   905 HTTP/1.1 200 OK  (PNG)
46067 2021-11-14 15:06:00.21… 10.9.13.145     178.79.137.164          HTTP   454 GET /8E_cover_small.jpg HTTP/1.1
46143 2021-11-14 15:06:00.29… 178.79.137.164 10.9.13.145              HTTP   225 HTTP/1.1 301 Moved Permanently
```

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.

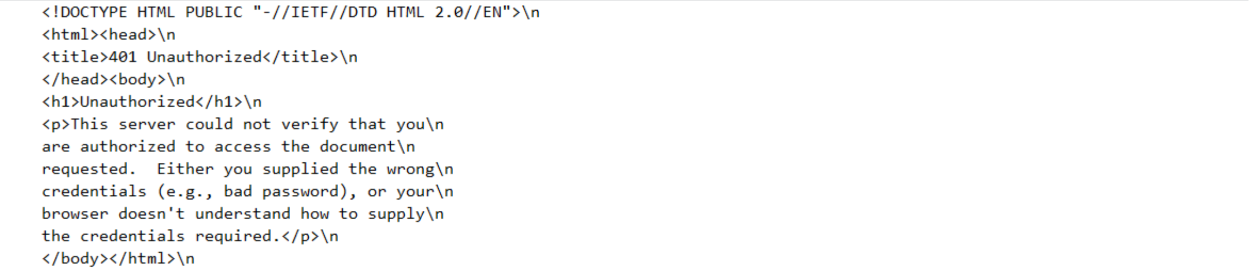
    - We can infer thar our browser downloaded the two images serially by looking at the time section, since the first request responded before the request for the second request even sent, it is pretty obvious the they were downloaded serially separate.



```
45415 2021-11-14 15:05:59.226900      10.9.13.145     128.119.245.12   HTTP   541 GET /wireshark-labs/HTTP-wireshark-f
45500 2021-11-14 15:05:59.369201      128.119.245.12 10.9.13.145       HTTP   13… HTTP/1.1 200 OK  (text/html)
45560 2021-11-14 15:05:59.466848      10.9.13.145     128.119.245.12   HTTP   487 GET /pearson.png HTTP/1.1
45711 2021-11-14 15:05:59.664949      128.119.245.12 10.9.13.145       HTTP   905 HTTP/1.1 200 OK  (PNG)
46067 2021-11-14 15:06:00.219339      10.9.13.145     178.79.137.164   HTTP   454 GET /8E_cover_small.jpg HTTP/1.1
46143 2021-11-14 15:06:00.291672      178.79.137.164 10.9.13.145       HTTP   225 HTTP/1.1 301 Moved Permanently
```

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

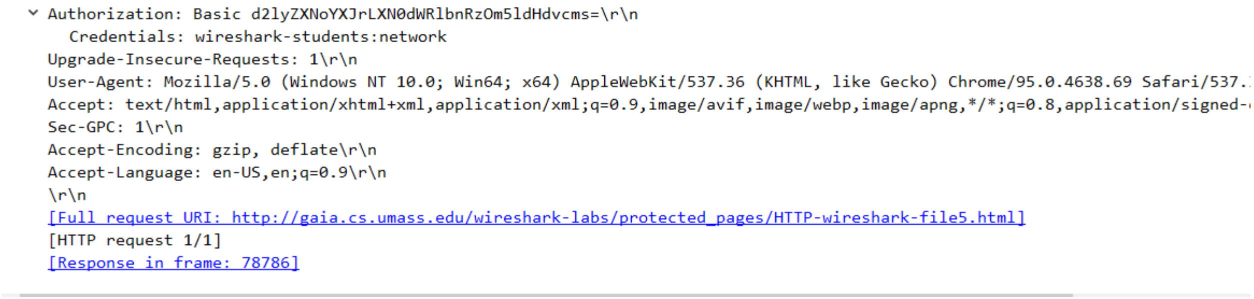
    - Since the page we are willing to reach is protected the first respond we receive is "This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials(…),or your browser doesn't understand how to supply the credentials required " with the status code of 401(unauthorized).



```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
<html><head>\n
<title>401 Unauthorized</title>\n
</head><body>\n
<h1>Unauthorized</h1>\n
<p>This server could not verify that you\n
are authorized to access the document\n
requested.  Either you supplied the wrong\n
credentials (e.g., bad password), or your\n
browser doesn't understand how to supply\n
the credentials required.</p>\n
</body></html>\n
```

Assignment-1

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
    - The new field we now can see is the authorization field which contains the password and the user-name required to reach the page.



```
⌄ 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/95.0.4638.69 Safari/537.
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
  Sec-GPC: 1\r\n
  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/protected_pages/HTTP-wireshark-file5.html]
  [HTTP request 1/1]
  [Response in frame: 78786]
```