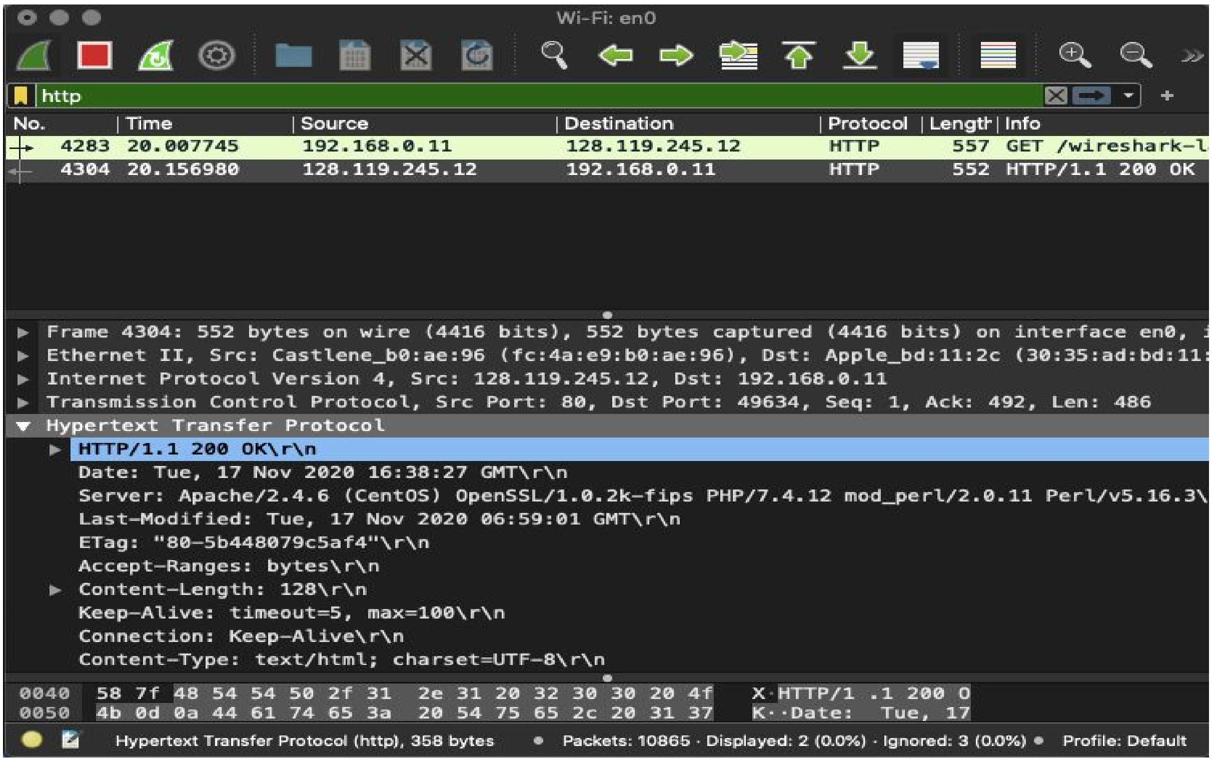
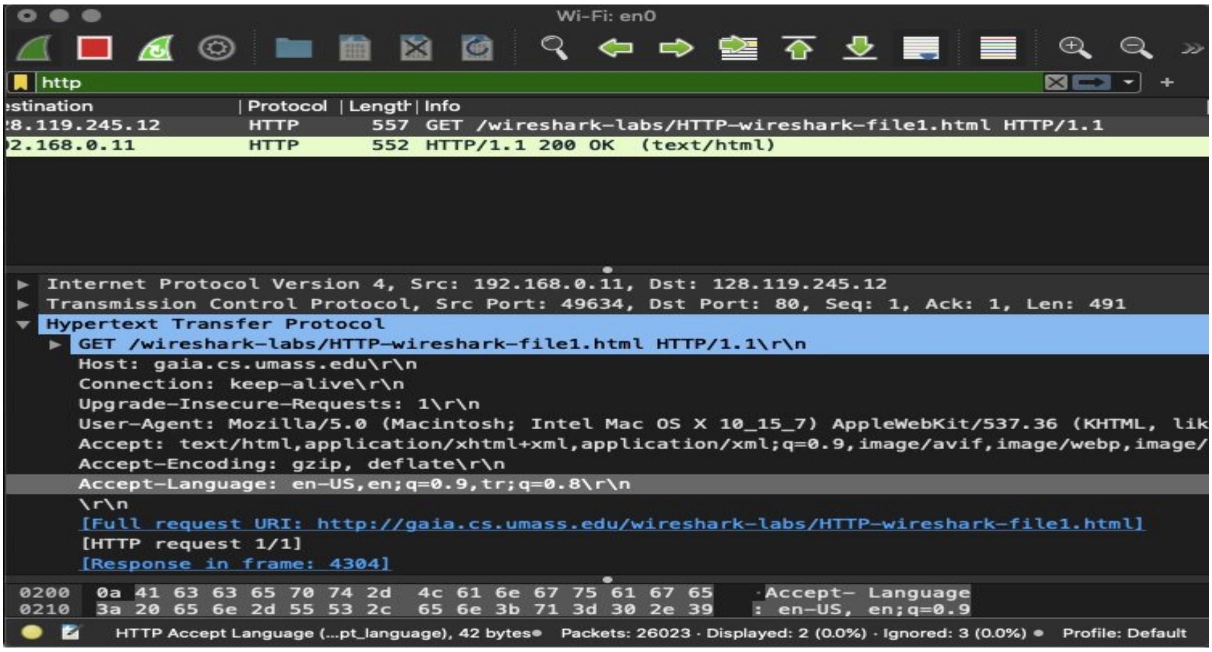
Senanur Güvercinoğlu
150119740

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



```
No.      | Time      | Source          | Destination     | Protocol | Length | Info
4283  20.007745   192.168.0.11      128.119.245.12    HTTP       557  GET /wireshark-l
4304  20.156980   128.119.245.12    192.168.0.11      HTTP       552  HTTP/1.1 200 OK

▶ Frame 4304: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, i
▶ Ethernet II, Src: Castlene_b0:ae:96 (fc:4a:e9:b0:ae:96), Dst: Apple_bd:11:2c (30:35:ad:bd:11:
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.11
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49634, Seq: 1, Ack: 492, Len: 486
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Tue, 17 Nov 2020 16:38:27 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\
    Last-Modified: Tue, 17 Nov 2020 06:59:01 GMT\r\n
    ETag: "80-5b448079c5af4"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n

0040  58 7f 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   X·HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 54 75 65 2c 20 31 37   K··Date:  Tue, 17

Hypertext Transfer Protocol (http), 358 bytes  •  Packets: 10865 · Displayed: 2 (0.0%) · Ignored: 3 (0.0%)  •  Profile: Default
```

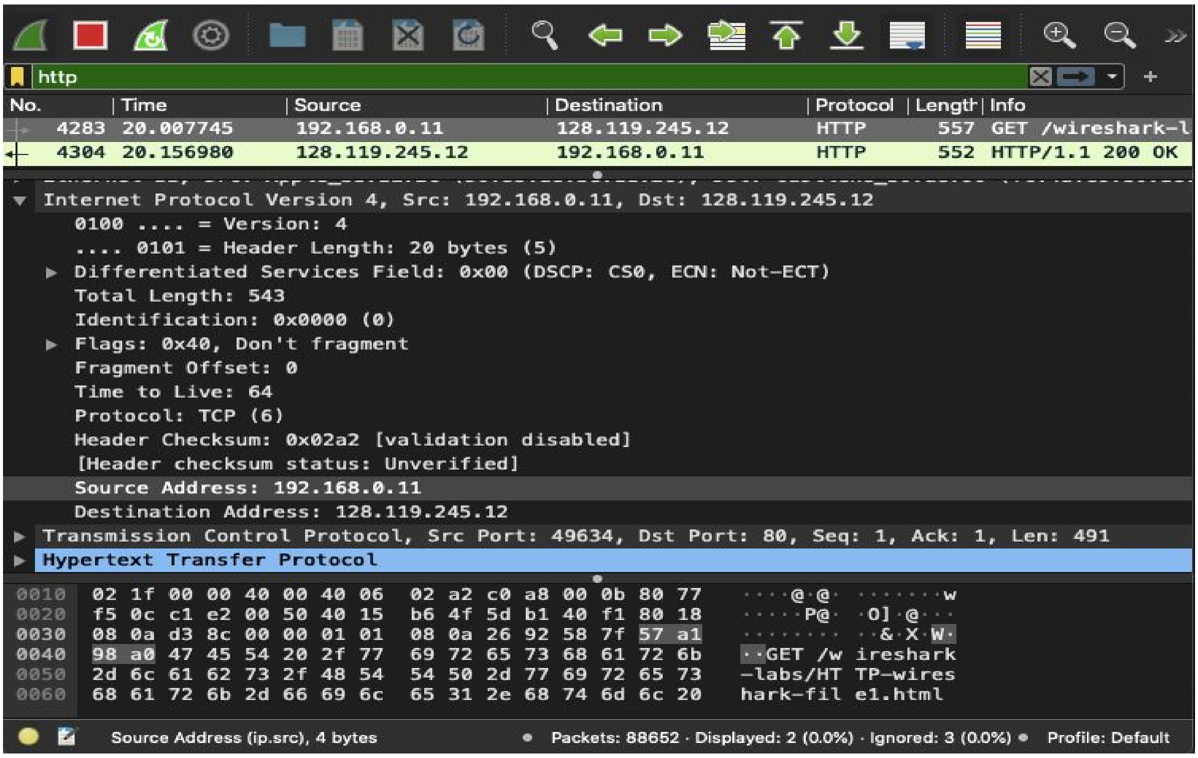
2. What languages (if any) does your browser indicate that it can accept to the server?
Answer: english-US



```
stination           | Protocol | Length | Info
8.119.245.12          HTTP       557  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2.168.0.11            HTTP       552  HTTP/1.1 200 OK  (text/html)

▶ Internet Protocol Version 4, Src: 192.168.0.11, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 49634, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, lik
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 4304]

0200  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept- Language
0210  3a 20 65 6e 2d 55 53 2c  65 6e 3b 71 3d 30 2e 39   : en-US, en;q=0.9

HTTP Accept Language (...pt_language), 42 bytes •  Packets: 26023 · Displayed: 2 (0.0%) · Ignored: 3 (0.0%)  •  Profile: Default
```

Senanur Güvercinoğlu
150119740

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
Answer: My computer is 192.168.0.11 and the destination is 128.119.245.12



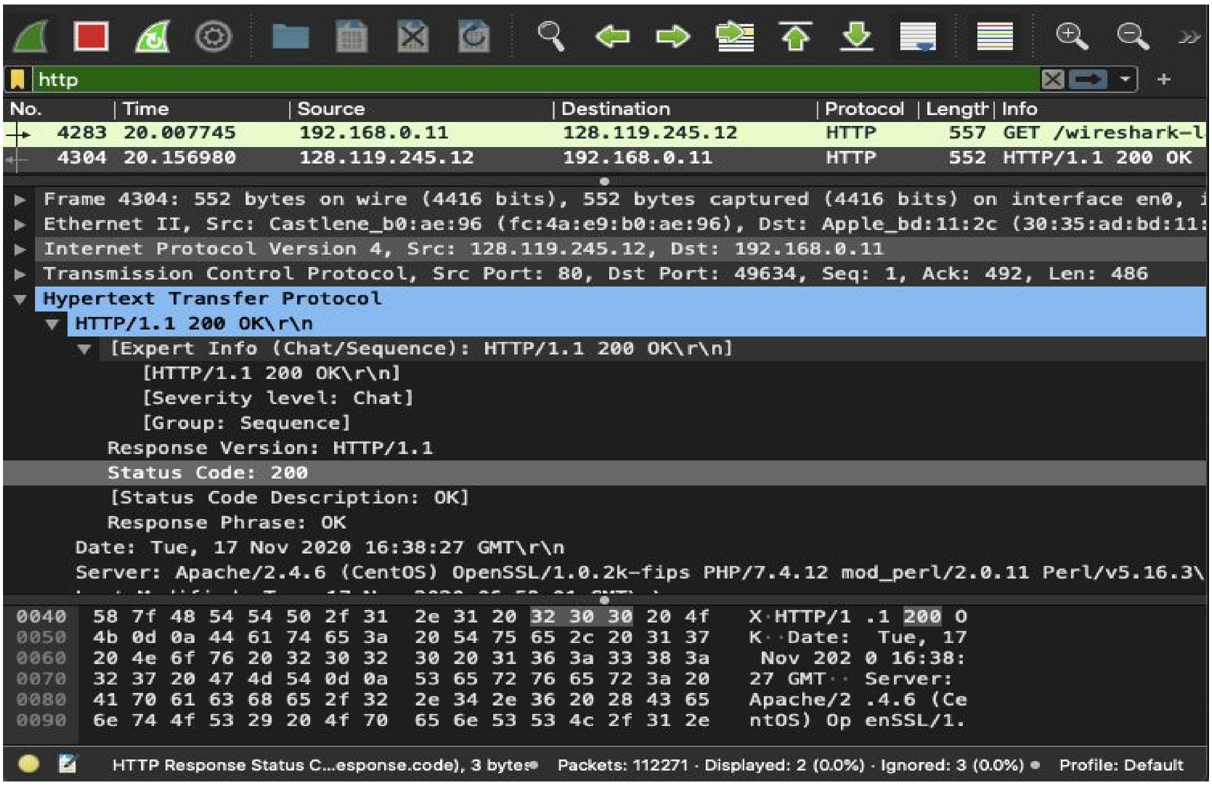
```
http
No.    | Time       | Source          | Destination     | Protocol | Length | Info
  4283  20.007745    192.168.0.11      128.119.245.12    HTTP        557  GET /wireshark-l
  4304  20.156980    128.119.245.12    192.168.0.11      HTTP        552  HTTP/1.1 200 OK
```

```
▼ Internet Protocol Version 4, Src: 192.168.0.11, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 543
    Identification: 0x0000 (0)
  ▶ Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x02a2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.11
    Destination Address: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 49634, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▶ Hypertext Transfer Protocol
```

```
0010  02 1f 00 00 40 00 40 06  02 a2 c0 a8 00 0b 80 77   ····@·@· ·······w
0020  f5 0c c1 e2 00 50 40 15  b6 4f 5d b1 40 f1 80 18   ·····P@· ·O]·@···
0030  08 0a d3 8c 00 00 01 01  08 0a 26 92 58 7f 57 a1   ········ ··&·X·W·
0040  98 a0 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 31 2e 68 74 6d 6c 20   hark-fil e1.html
```

Source Address (ip.src), 4 bytes • Packets: 88652 · Displayed: 2 (0.0%) · Ignored: 3 (0.0%) • Profile: Default

4. What is the status code returned from the server to your browser?
Answer: 200 OK



```
http
No.    | Time       | Source          | Destination     | Protocol | Length | Info
  4283  20.007745    192.168.0.11      128.119.245.12    HTTP        557  GET /wireshark-l
  4304  20.156980    128.119.245.12    192.168.0.11      HTTP        552  HTTP/1.1 200 OK
```

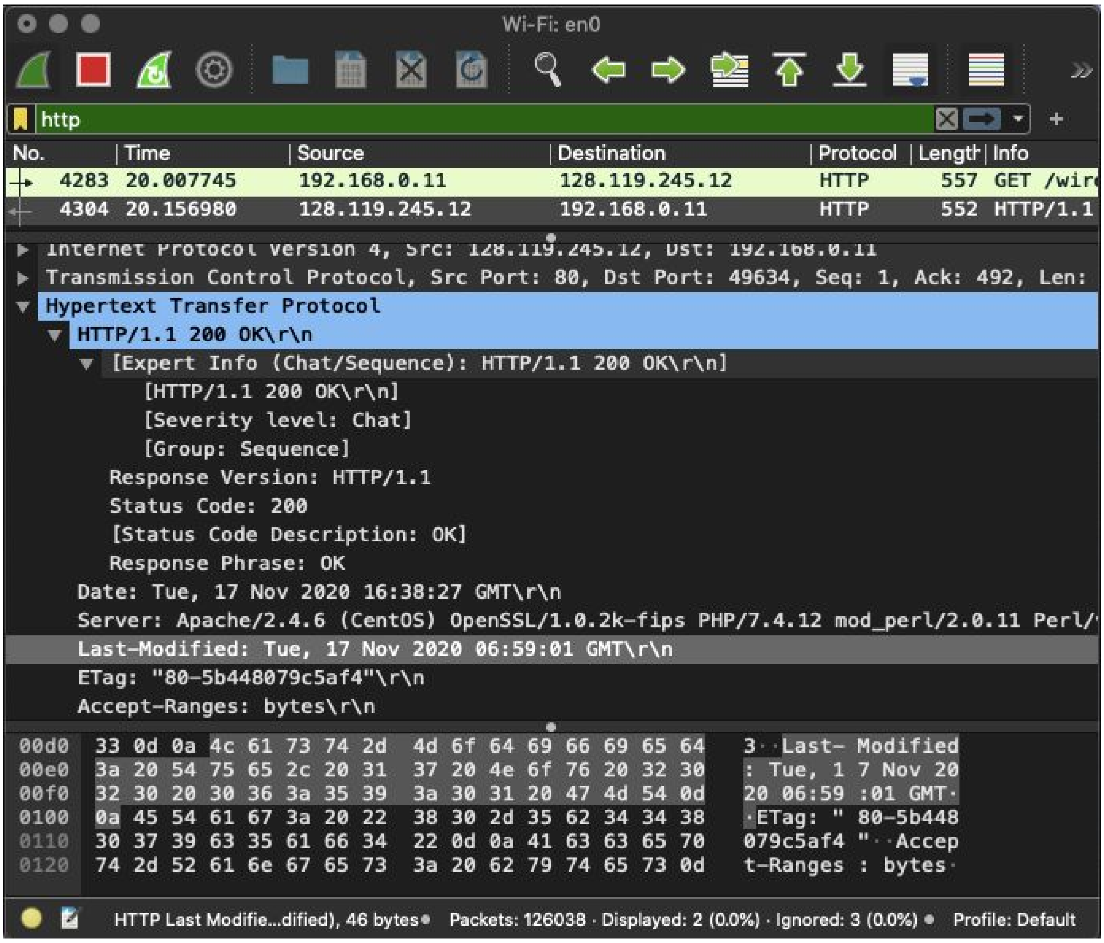
```
▶ Frame 4304: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, i
▶ Ethernet II, Src: Castlene_b0:ae:96 (fc:4a:e9:b0:ae:96), Dst: Apple_bd:11:2c (30:35:ad:bd:11:
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.11
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49634, Seq: 1, Ack: 492, Len: 486
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
          [HTTP/1.1 200 OK\r\n]
          [Severity level: Chat]
          [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 17 Nov 2020 16:38:27 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\
```

```
0040  58 7f 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   X·HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 54 75 65 2c 20 31 37   K··Date:  Tue, 17
0060  20 4e 6f 76 20 32 30 32  30 20 31 36 3a 33 38 3a    Nov 202 0 16:38:
0070  32 37 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   27 GMT·· Server:
0080  41 70 61 63 68 65 2f 32  2e 34 2e 36 20 28 43 65   Apache/2 .4.6 (Ce
0090  6e 74 4f 53 29 20 4f 70  65 6e 53 53 4c 2f 31 2e   ntOS) Op enSSL/1.
```

HTTP Response Status C...esponse.code), 3 bytes • Packets: 112271 · Displayed: 2 (0.0%) · Ignored: 3 (0.0%) • Profile: Default

Senanur Güvercinoğlu
150119740

5. When was the HTML file that you are retrieving last modified at the server?
Answer: Tue,17 Nov 2020 06:59:01



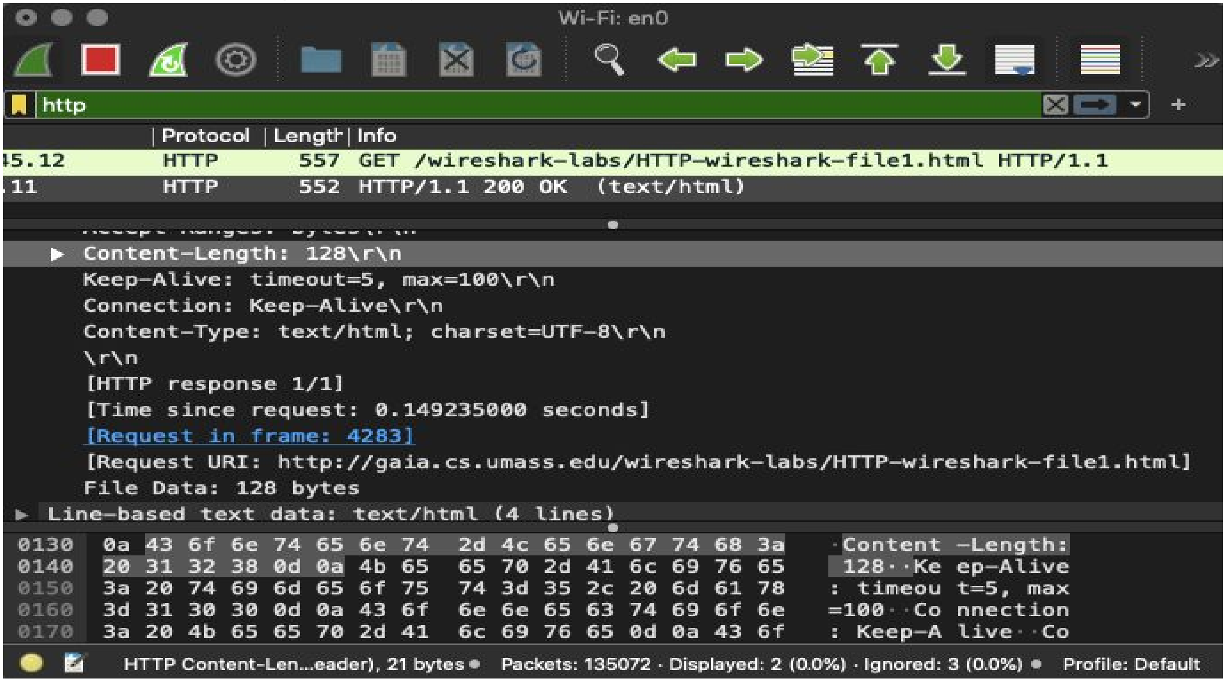
```
No.     Time        Source           Destination      Protocol  Length  Info
4283    20.007745   192.168.0.11     128.119.245.12   HTTP      557     GET /wire
4304    20.156980   128.119.245.12   192.168.0.11     HTTP      552     HTTP/1.1
```

```
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.11
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49634, Seq: 1, Ack: 492, Len:
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 17 Nov 2020 16:38:27 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/
    Last-Modified: Tue, 17 Nov 2020 06:59:01 GMT\r\n
    ETag: "80-5b448079c5af4"\r\n
    Accept-Ranges: bytes\r\n
```

```
00d0  33 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   3··Last- Modified
00e0  3a 20 54 75 65 2c 20 31  37 20 4e 6f 76 20 32 30   : Tue, 1 7 Nov 20
00f0  32 30 20 30 36 3a 35 39  3a 30 31 20 47 4d 54 0d   20 06:59 :01 GMT·
0100  0a 45 54 61 67 3a 20 22  38 30 2d 35 62 34 34 38   ·ETag: " 80-5b448
0110  30 37 39 63 35 61 66 34  22 0d 0a 41 63 63 65 70   079c5af4 "··Accep
0120  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes·
```

HTTP Last Modifie...dified), 46 bytes • Packets: 126038 · Displayed: 2 (0.0%) · Ignored: 3 (0.0%) • Profile: Default

6. How many bytes of content are being returned to your browser?
Answer: Content-Length=128 bytes



```
        Protocol  Length  Info
45.12   HTTP      557     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
11      HTTP      552     HTTP/1.1 200 OK  (text/html)
```

```
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.149235000 seconds]
    [Request in frame: 4283]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
▶ Line-based text data: text/html (4 lines)
```

```
0130  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0140  20 31 32 38 0d 0a 4b 65  65 70 2d 41 6c 69 76 65    128··Ke ep-Alive
0150  3a 20 74 69 6d 65 6f 75  74 3d 35 2c 20 6d 61 78   : timeou t=5, max
0160  3d 31 30 30 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   =100··Co nnection
0170  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 43 6f   : Keep-A live··Co
```

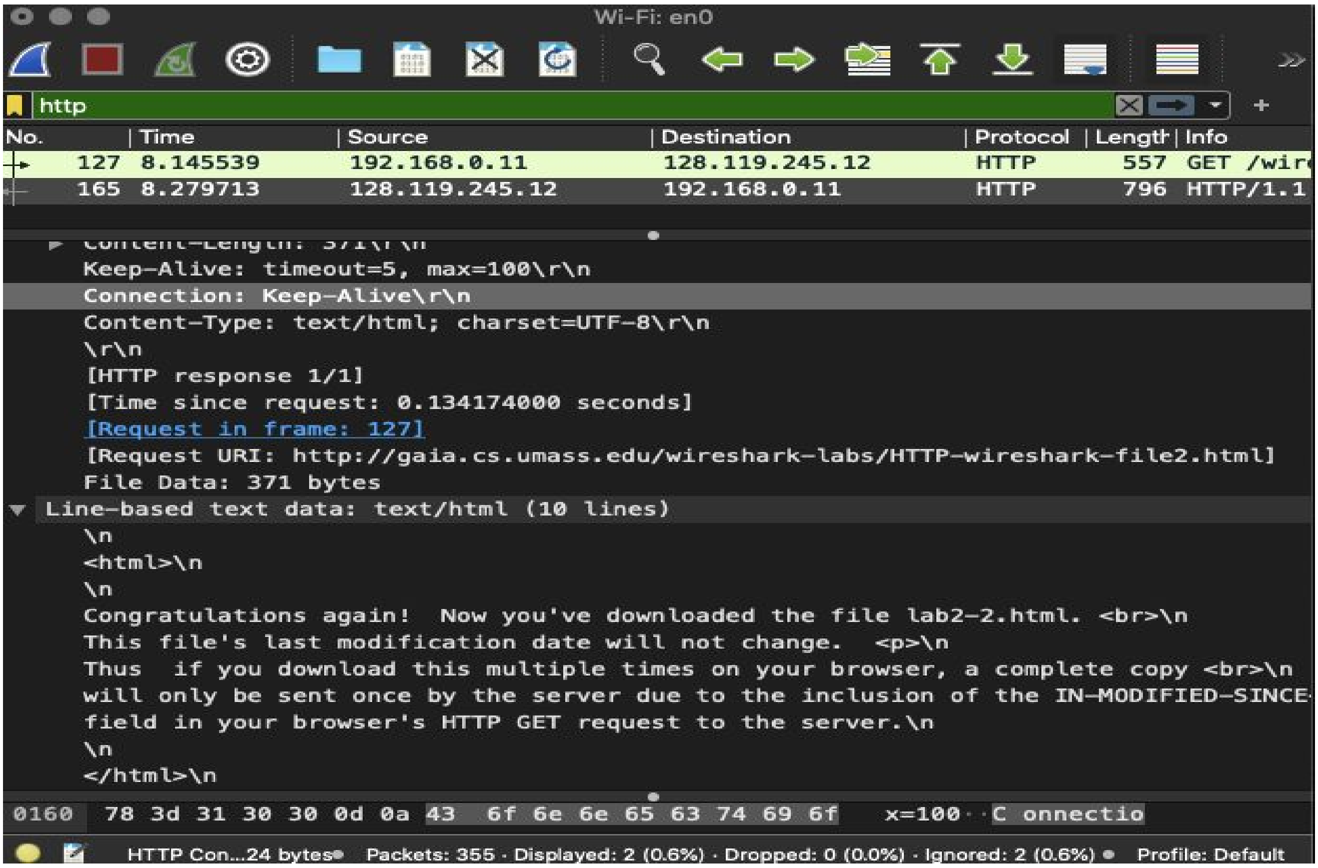
HTTP Content-Len...eader), 21 bytes • Packets: 135072 · Displayed: 2 (0.0%) · Ignored: 3 (0.0%) • Profile: Default

Senanur Güvercinoğlu
150119740

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.
Answer: No all of the headers can be found in the raw data.

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?
Answer: No

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

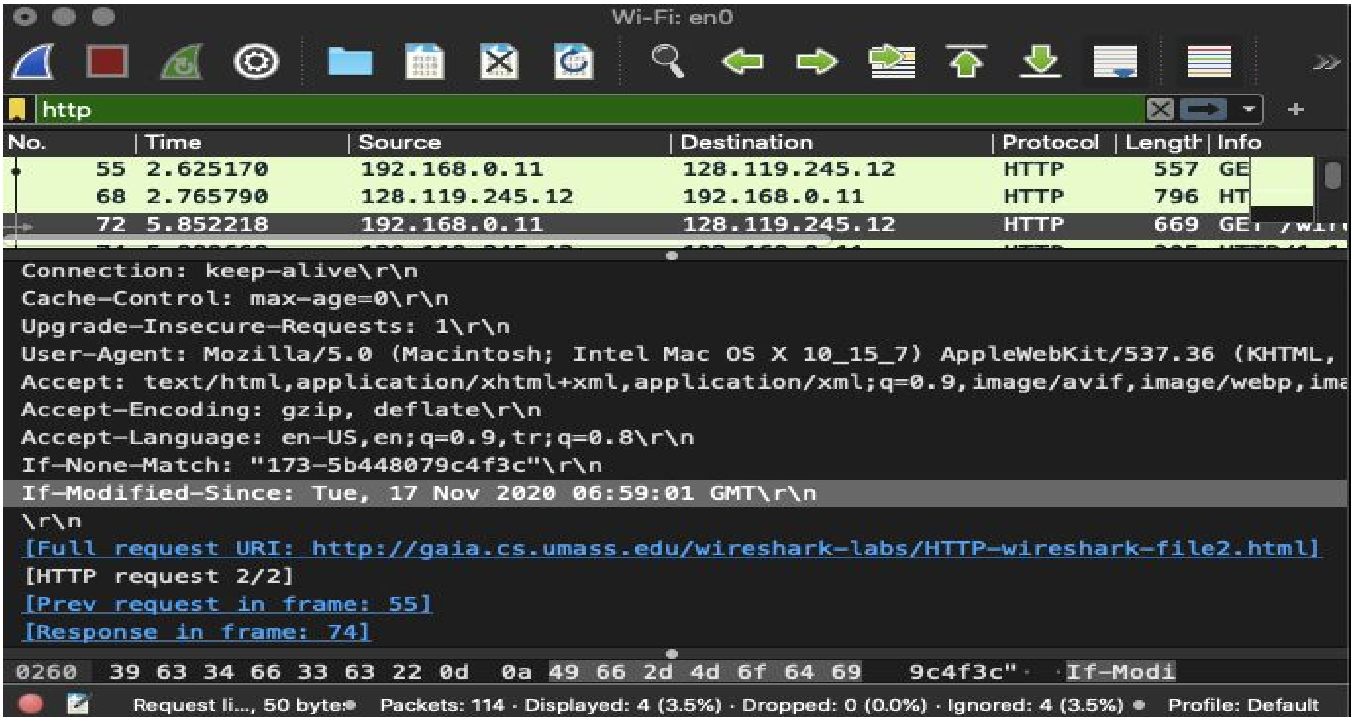


```
http

No.   | Time      | Source         | Destination    | Protocol | Length | Info
  127   8.145539    192.168.0.11     128.119.245.12   HTTP        557    GET /wir
  165   8.279713    128.119.245.12   192.168.0.11     HTTP        796    HTTP/1.1

  ▸ Content-Length: 371\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: 0.134174000 seconds]
    [Request in frame: 127]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
▾ 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
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n

0160  78 3d 31 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f    x=100··C onnectio

HTTP Con…24 bytes  Packets: 355 · Displayed: 2 (0.6%) · Dropped: 0 (0.0%) · Ignored: 2 (0.6%)  Profile: Default
```

Senanur Güvercinoğlu
150119740

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?

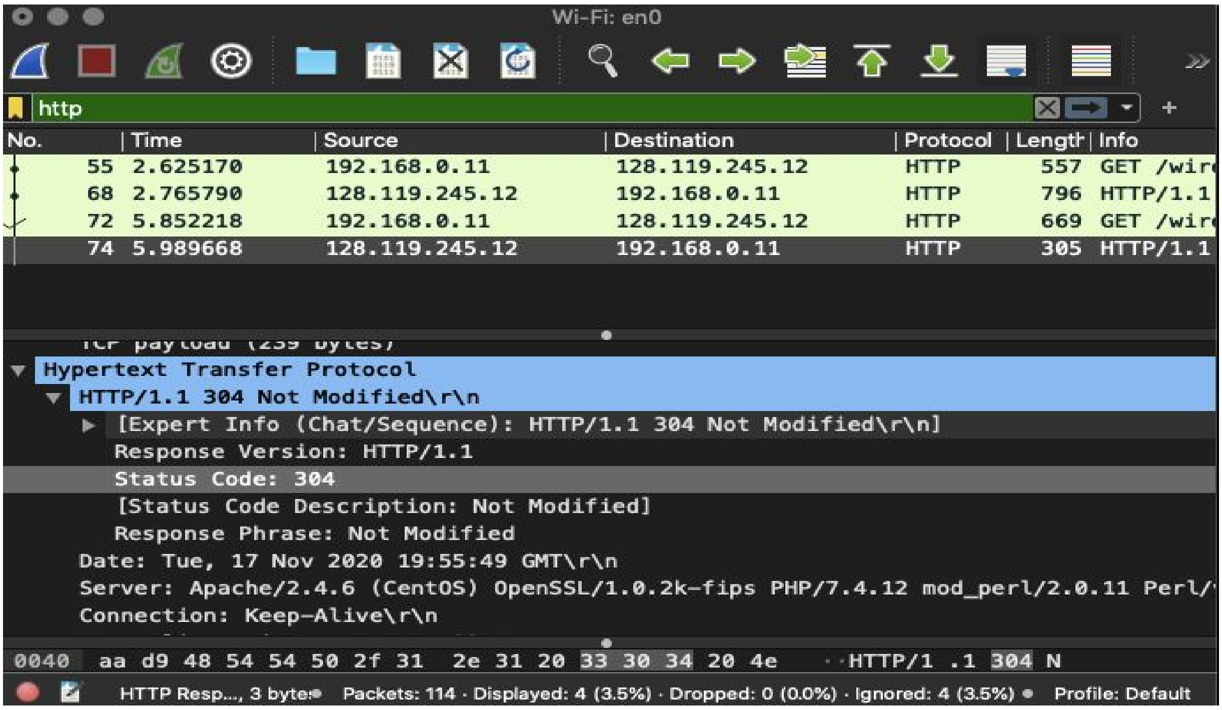
Answer: if-modified-since: Tue, 17 Nov 2020 06:59:01 GMT\r\n



```
Wi-Fi: en0
http

No.    | Time      | Source          | Destination     | Protocol | Length | Info
   55  2.625170    192.168.0.11      128.119.245.12    HTTP       557  GE
   68  2.765790    128.119.245.12    192.168.0.11      HTTP       796  HT
   72  5.852218    192.168.0.11      128.119.245.12    HTTP       669  GET /wir

Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
If-None-Match: "173-5b448079c4f3c"\r\n
If-Modified-Since: Tue, 17 Nov 2020 06:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]
[Prev request in frame: 55]
[Response in frame: 74]

0260  39 63 34 66 33 63 22 0d  0a 49 66 2d 4d 6f 64 69   9c4f3c"· ·If-Modi

Request li..., 50 bytes  Packets: 114 · Displayed: 4 (3.5%) · Dropped: 0 (0.0%) · Ignored: 4 (3.5%)  Profile: Default
```

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.

Answer:Status Code:304 The server did not return the contents of the file the second time around because it says it's not modified.

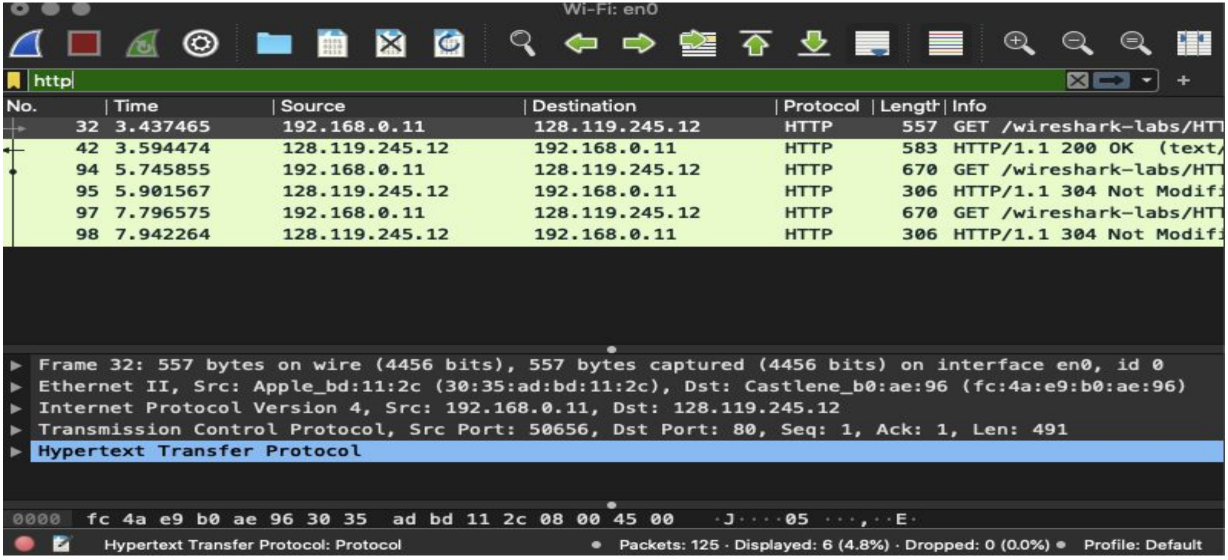


```
Wi-Fi: en0
http

No.    | Time      | Source          | Destination     | Protocol | Length | Info
   55  2.625170    192.168.0.11      128.119.245.12    HTTP       557  GET /wir
   68  2.765790    128.119.245.12    192.168.0.11      HTTP       796  HTTP/1.1
   72  5.852218    192.168.0.11      128.119.245.12    HTTP       669  GET /wir
   74  5.989668    128.119.245.12    192.168.0.11      HTTP       305  HTTP/1.1

TCP payload (239 bytes)
▼ Hypertext Transfer Protocol
  ▼ 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: Tue, 17 Nov 2020 19:55:49 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/
    Connection: Keep-Alive\r\n

0040  aa d9 48 54 54 50 2f 31  2e 31 20 33 30 34 20 4e   ··HTTP/1 .1 304 N

HTTP Resp..., 3 bytes  Packets: 114 · Displayed: 4 (3.5%) · Dropped: 0 (0.0%) · Ignored: 4 (3.5%)  Profile: Default
```

Senanur Güvercinoğlu
150119740

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?

Answer: just one, packet 32



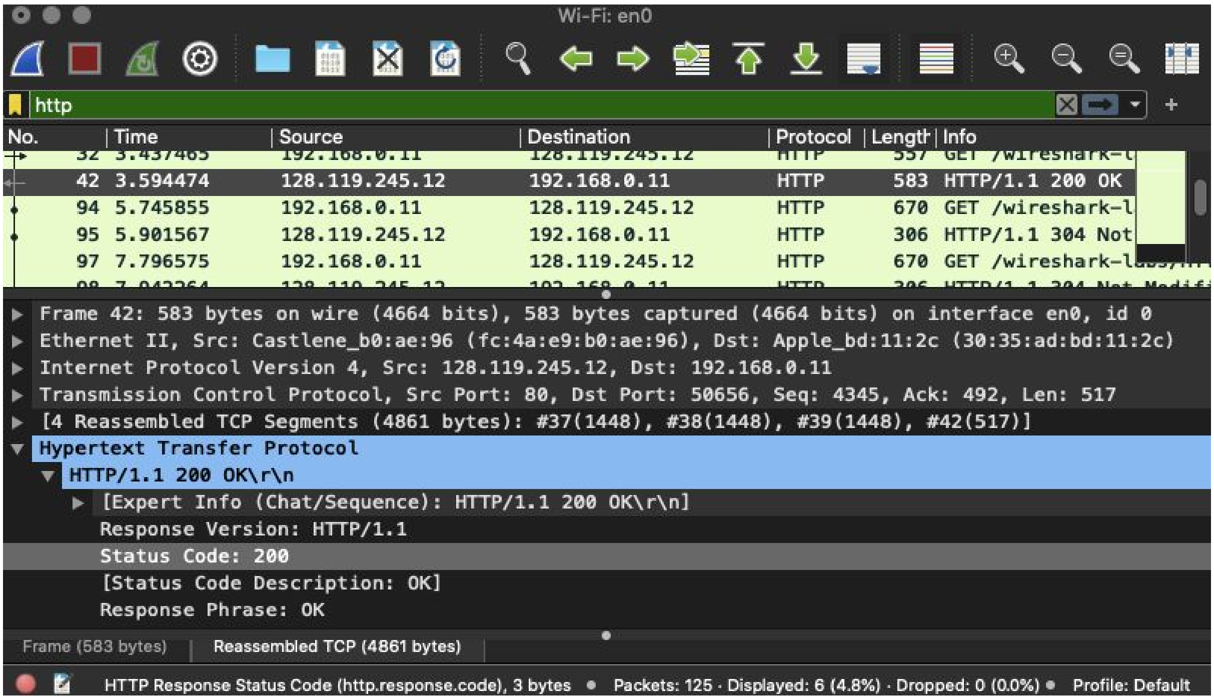
```
No.   | Time     | Source          | Destination     | Protocol | Length | Info
  32  3.437465   192.168.0.11      128.119.245.12    HTTP        557  GET /wireshark-labs/HT
  42  3.594474   128.119.245.12    192.168.0.11      HTTP        583  HTTP/1.1 200 OK  (text/
  94  5.745855   192.168.0.11      128.119.245.12    HTTP        670  GET /wireshark-labs/HT
  95  5.901567   128.119.245.12    192.168.0.11      HTTP        306  HTTP/1.1 304 Not Modifi
  97  7.796575   192.168.0.11      128.119.245.12    HTTP        670  GET /wireshark-labs/HT
  98  7.942264   128.119.245.12    192.168.0.11      HTTP        306  HTTP/1.1 304 Not Modifi

▶ Frame 32: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_bd:11:2c (30:35:ad:bd:11:2c), Dst: Castlene_b0:ae:96 (fc:4a:e9:b0:ae:96)
▶ Internet Protocol Version 4, Src: 192.168.0.11, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 50656, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▶ Hypertext Transfer Protocol

0000  fc 4a e9 b0 ae 96 30 35  ad bd 11 2c 08 00 45 00   ·J····05 ···,··E·

Hypertext Transfer Protocol: Protocol    Packets: 125 · Displayed: 6 (4.8%) · Dropped: 0 (0.0%)    Profile: Default
```

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

Answer: packet number is 42

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

Answer: Status code:200 and the response is 200 OK.

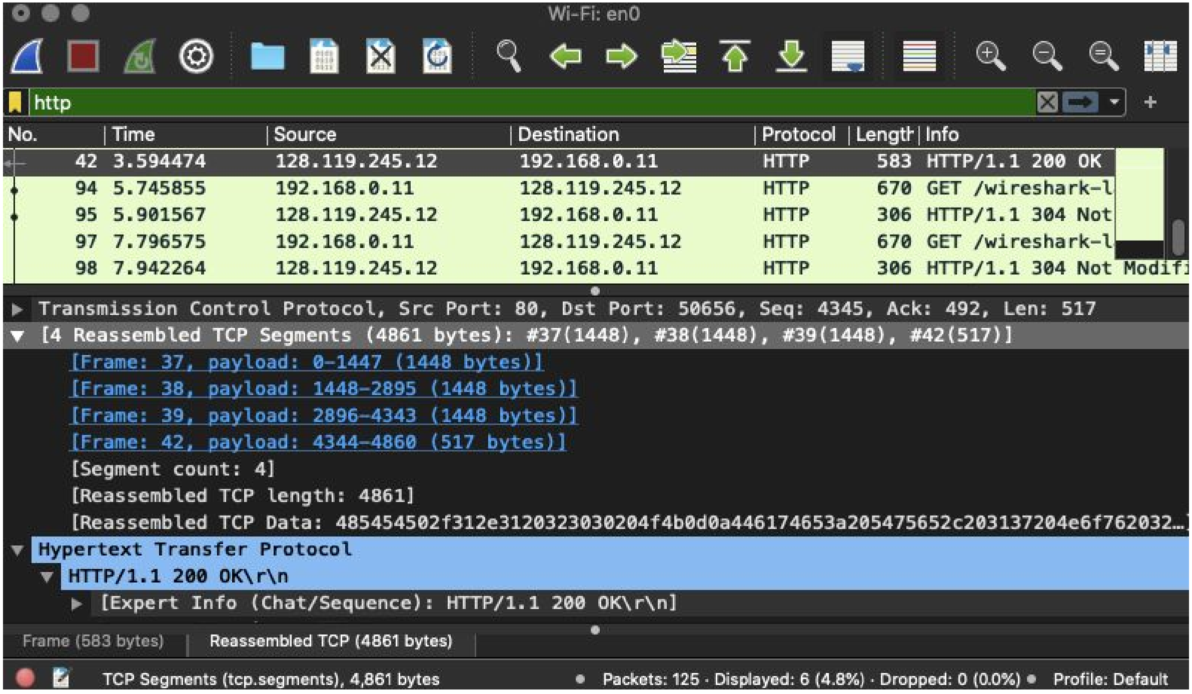


```
No.   | Time     | Source          | Destination     | Protocol | Length | Info
  32  3.437465   192.168.0.11      128.119.245.12    HTTP        557  GET /wireshark-l
  42  3.594474   128.119.245.12    192.168.0.11      HTTP        583  HTTP/1.1 200 OK
  94  5.745855   192.168.0.11      128.119.245.12    HTTP        670  GET /wireshark-l
  95  5.901567   128.119.245.12    192.168.0.11      HTTP        306  HTTP/1.1 304 Not
  97  7.796575   192.168.0.11      128.119.245.12    HTTP        670  GET /wireshark-labs/HT
  98  7.942264   128.119.245.12    192.168.0.11      HTTP        306  HTTP/1.1 304 Not Modifi

▶ Frame 42: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0
▶ Ethernet II, Src: Castlene_b0:ae:96 (fc:4a:e9:b0:ae:96), Dst: Apple_bd:11:2c (30:35:ad:bd:11:2c)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.11
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50656, Seq: 4345, Ack: 492, Len: 517
▶ [4 Reassembled TCP Segments (4861 bytes): #37(1448), #38(1448), #39(1448), #42(517)]
▼ 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

Frame (583 bytes)  |  Reassembled TCP (4861 bytes)

HTTP Response Status Code (http.response.code), 3 bytes    Packets: 125 · Displayed: 6 (4.8%) · Dropped: 0 (0.0%)    Profile: Default
```

Senanur Güvercinoğlu
150119740

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

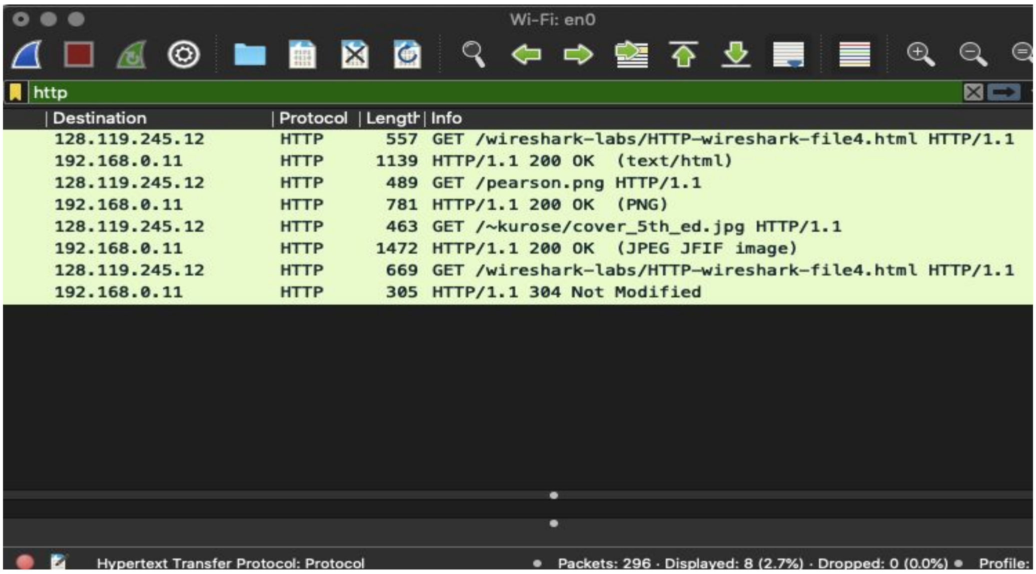
Answer: there are 4 TCP segments.



```
http

No.   | Time     | Source          | Destination     | Protocol | Length | Info
   42  3.594474  128.119.245.12    192.168.0.11      HTTP       583  HTTP/1.1 200 OK
   94  5.745855  192.168.0.11      128.119.245.12    HTTP       670  GET /wireshark-l
   95  5.901567  128.119.245.12    192.168.0.11      HTTP       306  HTTP/1.1 304 Not
   97  7.796575  192.168.0.11      128.119.245.12    HTTP       670  GET /wireshark-l
   98  7.942264  128.119.245.12    192.168.0.11      HTTP       306  HTTP/1.1 304 Not Modifi

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50656, Seq: 4345, Ack: 492, Len: 517
▼ [4 Reassembled TCP Segments (4861 bytes): #37(1448), #38(1448), #39(1448), #42(517)]
    [Frame: 37, payload: 0-1447 (1448 bytes)]
    [Frame: 38, payload: 1448-2895 (1448 bytes)]
    [Frame: 39, payload: 2896-4343 (1448 bytes)]
    [Frame: 42, payload: 4344-4860 (517 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205475652c203137204e6f762032…]
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Frame (583 bytes) | Reassembled TCP (4861 bytes)

TCP Segments (tcp.segments), 4,861 bytes     • Packets: 125 · Displayed: 6 (4.8%) · Dropped: 0 (0.0%) • Profile: Default
```

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

Answer: Four ; 1)wireshark-file4.html 2)pearson.png 3)cover_5th_ed.jpg 4)wireshark-file4.html

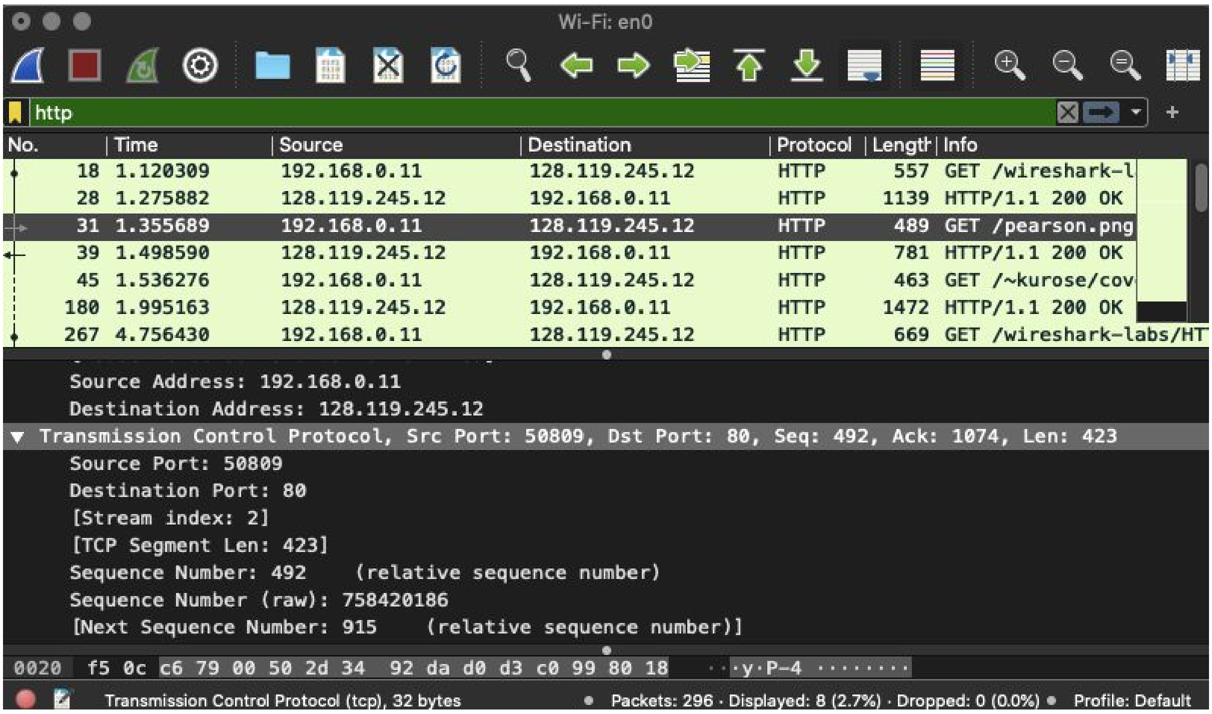


```
http

| Destination      | Protocol | Length | Info
  128.119.245.12     HTTP        557  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  192.168.0.11       HTTP       1139  HTTP/1.1 200 OK  (text/html)
  128.119.245.12     HTTP        489  GET /pearson.png HTTP/1.1
  192.168.0.11       HTTP        781  HTTP/1.1 200 OK  (PNG)
  128.119.245.12     HTTP        463  GET /~kurose/cover_5th_ed.jpg HTTP/1.1
  192.168.0.11       HTTP       1472  HTTP/1.1 200 OK  (JPEG JFIF image)
  128.119.245.12     HTTP        669  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  192.168.0.11       HTTP        305  HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol: Protocol     • Packets: 296 · Displayed: 8 (2.7%) · Dropped: 0 (0.0%) • Profile:
```

Senanur Güvercinoğlu
150119740

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

Answer: Based on timestamps, it appears the images were downloaded serially. Also the source port incrementing each time from 50809,50810,20811 which means that the images were received serially over separate TCP connections.



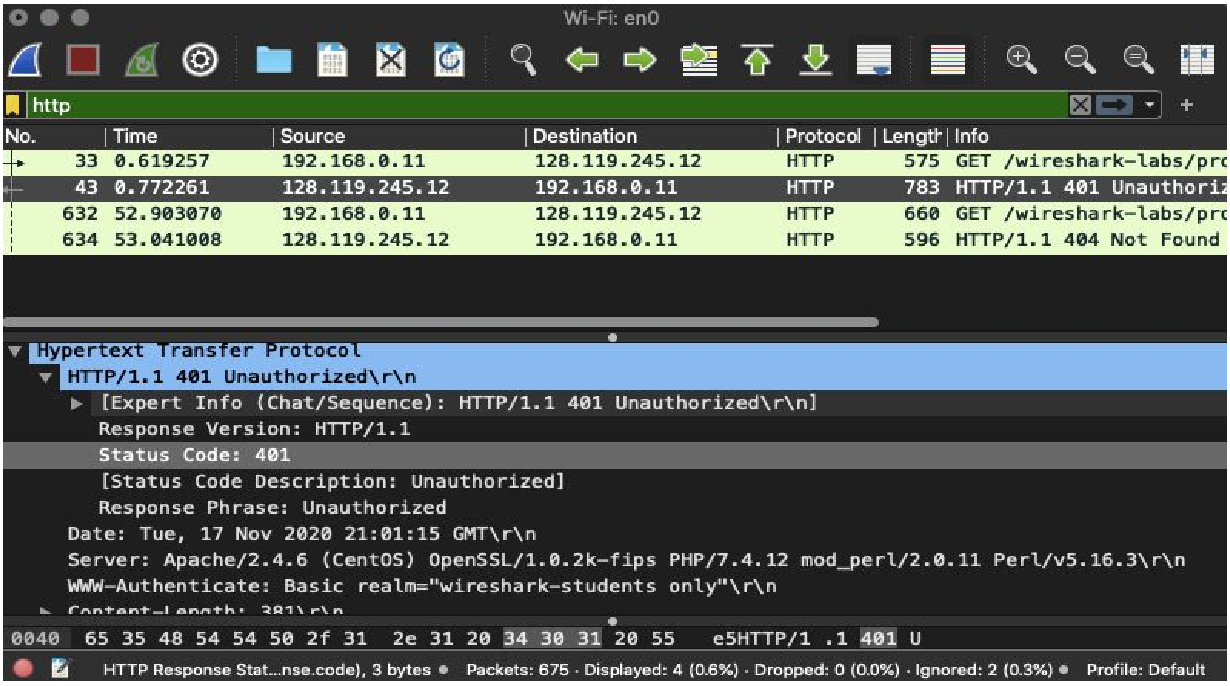
```
No.   Time       Source          Destination     Protocol  Length  Info
 18   1.120309   192.168.0.11    128.119.245.12  HTTP       557    GET /wireshark-l
 28   1.275882   128.119.245.12  192.168.0.11    HTTP      1139    HTTP/1.1 200 OK
 31   1.355689   192.168.0.11    128.119.245.12  HTTP       489    GET /pearson.png
 39   1.498590   128.119.245.12  192.168.0.11    HTTP       781    HTTP/1.1 200 OK
 45   1.536276   192.168.0.11    128.119.245.12  HTTP       463    GET /~kurose/cov
180   1.995163   128.119.245.12  192.168.0.11    HTTP      1472    HTTP/1.1 200 OK
267   4.756430   192.168.0.11    128.119.245.12  HTTP       669    GET /wireshark-labs/HT
```

```
    Source Address: 192.168.0.11
    Destination Address: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 50809, Dst Port: 80, Seq: 492, Ack: 1074, Len: 423
    Source Port: 50809
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 423]
    Sequence Number: 492    (relative sequence number)
    Sequence Number (raw): 758420186
    [Next Sequence Number: 915    (relative sequence number)]
```

```
0020  f5 0c c6 79 00 50 2d 34  92 da d0 d3 c0 99 80 18   ··y·P-4 ········
```

Transmission Control Protocol (tcp), 32 bytes ● Packets: 296 · Displayed: 8 (2.7%) · Dropped: 0 (0.0%) ● Profile: Default

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
Answer: The status code is 401 and the phrase is Unauthorized.



```
No.   Time        Source          Destination     Protocol  Length  Info
 33   0.619257    192.168.0.11    128.119.245.12  HTTP       575    GET /wireshark-labs/pro
 43   0.772261    128.119.245.12  192.168.0.11    HTTP       783    HTTP/1.1 401 Unauthoriz
632   52.903070   192.168.0.11    128.119.245.12  HTTP       660    GET /wireshark-labs/pro
634   53.041008   128.119.245.12  192.168.0.11    HTTP       596    HTTP/1.1 404 Not Found
```

```
▼ Hypertext Transfer Protocol
  ▼ 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: Tue, 17 Nov 2020 21:01:15 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  ▶ Content-Length: 381\r\n
```

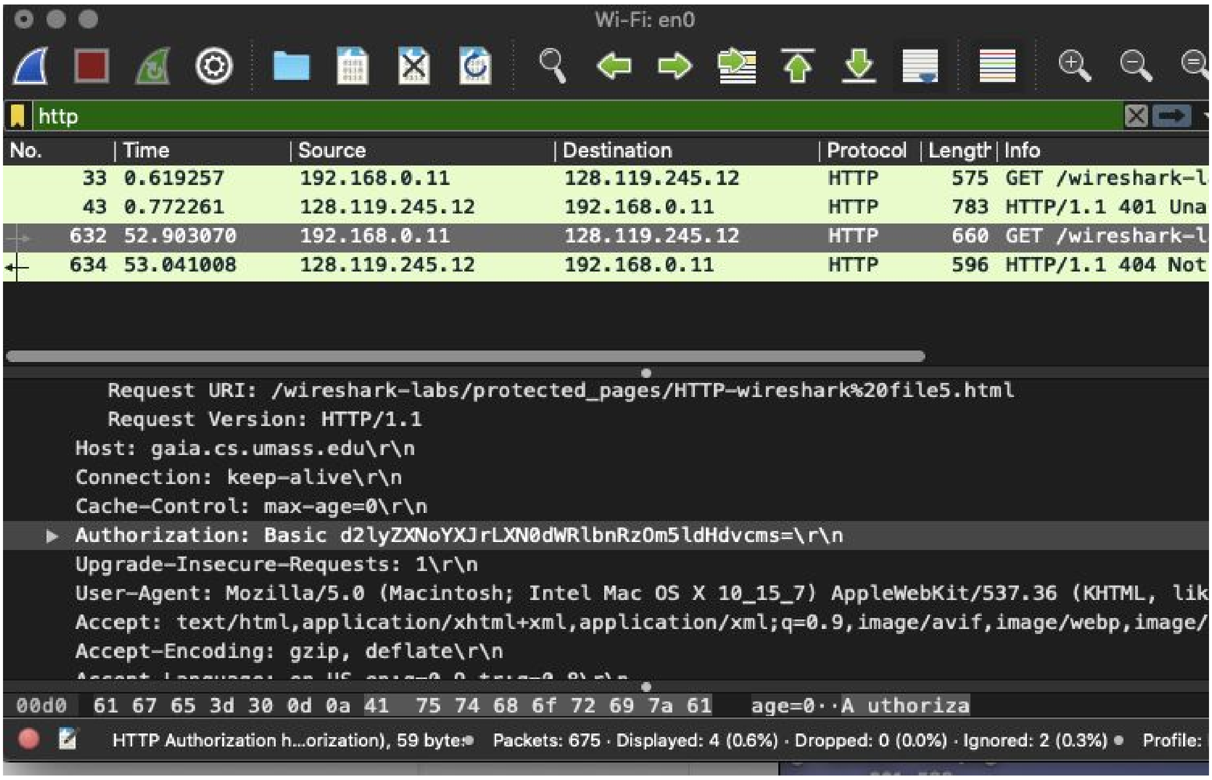
```
0040  65 35 48 54 54 50 2f 31  2e 31 20 34 30 31 20 55   e5HTTP/1 .1 401 U
```

HTTP Response Stat...nse.code), 3 bytes ● Packets: 675 · Displayed: 4 (0.6%) · Dropped: 0 (0.0%) · Ignored: 2 (0.3%) ● Profile: Default

Senanur Güvercinoğlu
150119740

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

Answer: Authorization: Basic



```
http
```

```
No.     Time        Source          Destination     Protocol  Length  Info
    33  0.619257    192.168.0.11    128.119.245.12  HTTP      575     GET /wireshark-l
    43  0.772261    128.119.245.12  192.168.0.11    HTTP      783     HTTP/1.1 401 Una
   632  52.903070   192.168.0.11    128.119.245.12  HTTP      660     GET /wireshark-l
   634  53.041008   128.119.245.12  192.168.0.11    HTTP      596     HTTP/1.1 404 Not
```

```
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark%20file5.html
        Request Version: HTTP/1.1
     Host: gaia.cs.umass.edu\r\n
     Connection: keep-alive\r\n
     Cache-Control: max-age=0\r\n
   ▶ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
     Upgrade-Insecure-Requests: 1\r\n
     User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, lik
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
     Accept-Encoding: gzip, deflate\r\n
     Accept-Language: en-US,en;q=0.9,tr;q=0.8)\r\n
```

```
00d0  61 67 65 3d 30 0d 0a 41  75 74 68 6f 72 69 7a 61   age=0··A uthoriza
```

HTTP Authorization h...orization), 59 byte • Packets: 675 · Displayed: 4 (0.6%) · Dropped: 0 (0.0%) · Ignored: 2 (0.3%) • Profile: