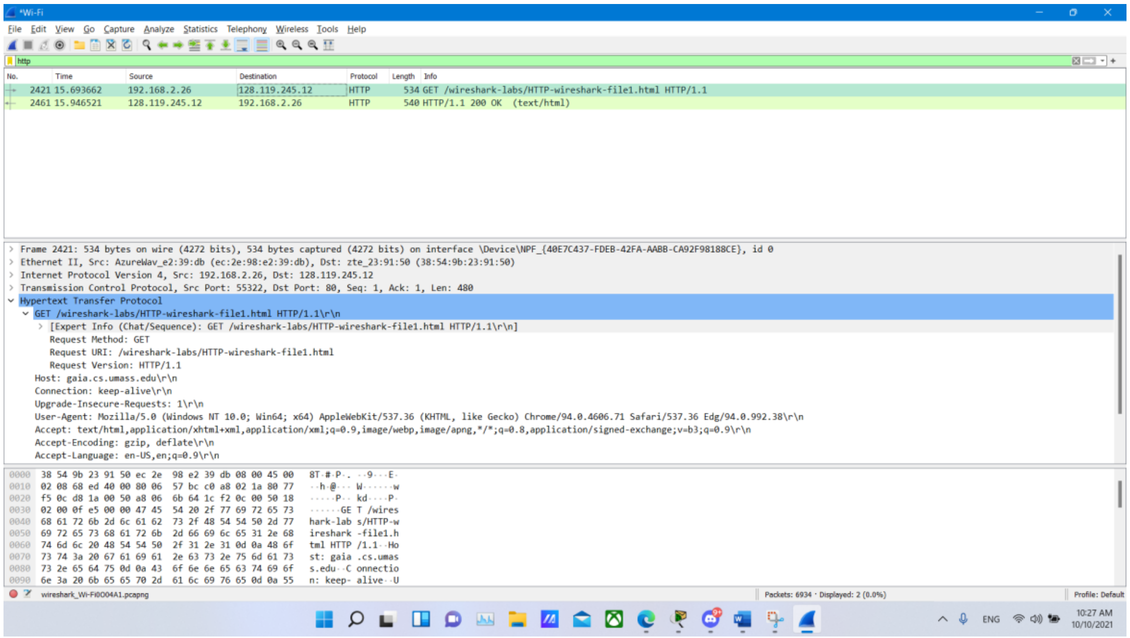
Wireshark Lab 2a

Name: Nguyễn Minh Hùng

ID: 1952737

1. The Basic HTTP GET/response interaction

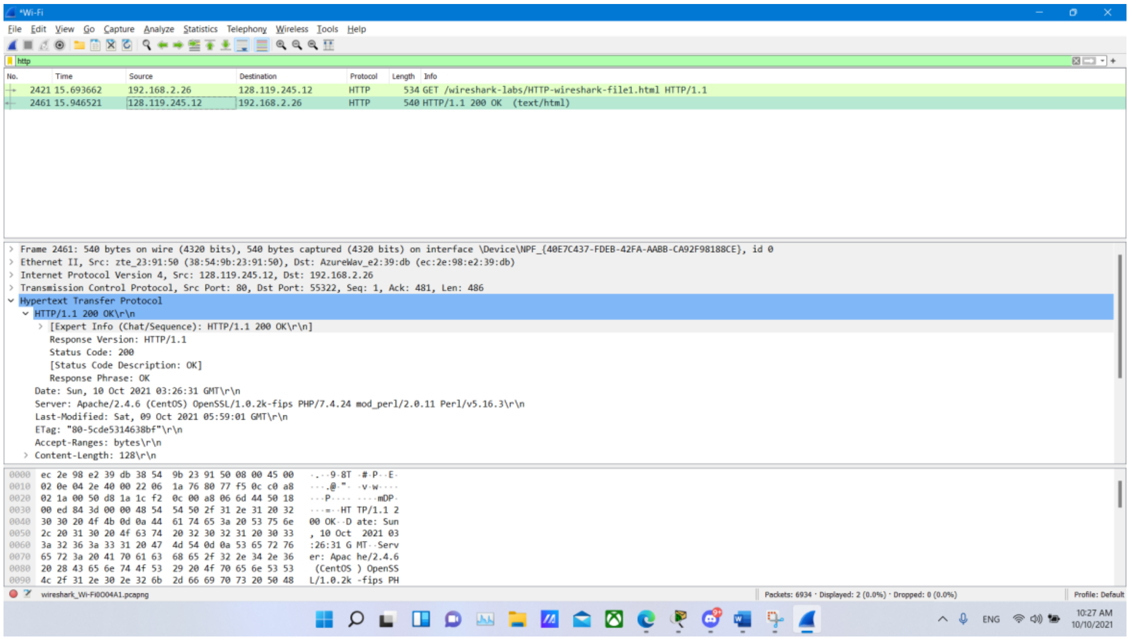

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.     Time        Source           Destination      Protocol  Length  Info
  2421 15.693662   192.168.2.26     128.119.245.12   HTTP        534  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  2461 15.946521   128.119.245.12   192.168.2.26     HTTP        540  HTTP/1.1 200 OK  (text/html)
```

```
> Frame 2421: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: AzureWav_e2:39:db (ec:2e:98:e2:39:db), Dst: zte_23:91:50 (38:54:9b:23:91:50)
> Internet Protocol Version 4, Src: 192.168.2.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55322, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
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-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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
```

```
0000  38 54 9b 23 91 50 ec 2e  98 e2 39 db 08 00 45 00   8T·#·P·. ··9···E·
0010  02 08 68 ed 40 00 80 06  57 bc c0 a8 02 1a 80 77   ··h·@··· W······w
0020  f5 0c d8 1a 00 50 a8 06  6b 64 1c f2 0c 00 50 18   ·····P·· kd····P·
0030  02 00 0f e5 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
```

wireshark_Wi-Fi0OO4A1.pcapng | Packets: 6934 · Displayed: 2 (0.0%) | Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

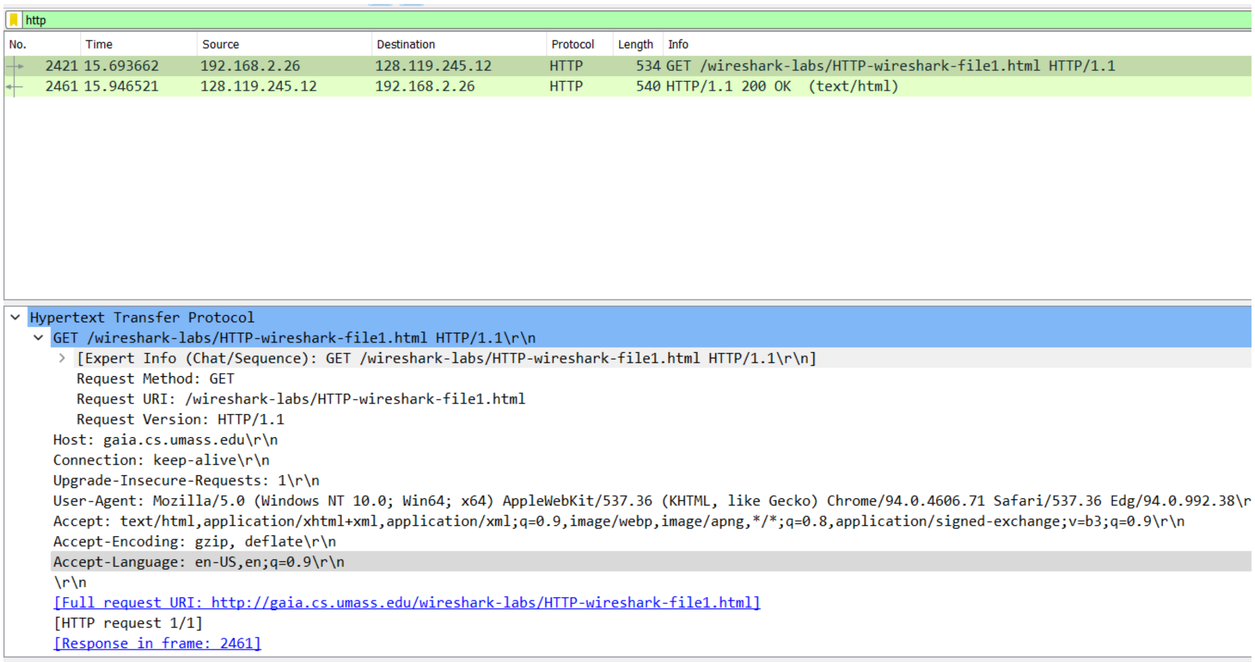
```
No.     Time        Source           Destination      Protocol  Length  Info
  2421 15.693662   192.168.2.26     128.119.245.12   HTTP        534  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  2461 15.946521   128.119.245.12   192.168.2.26     HTTP        540  HTTP/1.1 200 OK  (text/html)
```

```
> Frame 2461: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: zte_23:91:50 (38:54:9b:23:91:50), Dst: AzureWav_e2:39:db (ec:2e:98:e2:39:db)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 55322, Seq: 1, Ack: 481, Len: 486
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, 10 Oct 2021 03:26:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 09 Oct 2021 05:59:01 GMT\r\n
    ETag: "80-5cde5314638bf"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
```

```
0000  ec 2e 98 e2 39 db 38 54  9b 23 91 50 08 00 45 00   ·.··9·8T ·#·P··E·
0010  02 0e 04 2e 40 00 22 06  1a 76 80 77 f5 0c c0 a8   ···.@·"· ·v·w····
0020  02 1a 00 50 d8 1a 1c f2  0c 00 a8 06 6d 44 50 18   ···P···· ····mDP·
0030  00 ed 84 3d 00 00 48 54  54 50 2f 31 2e 31 20 32   ···=··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
0050  2c 20 31 30 20 4f 63 74  20 32 30 32 31 20 30 33   , 10 Oct  2021 03
0060  3a 32 36 3a 33 31 20 47  4d 54 0d 0a 53 65 72 76   :26:31 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
```

wireshark_Wi-Fi0OO4A1.pcapng | Packets: 6934 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   Answer: My browser is running HTTP version 1.1 (request version HTTP/1.1)
   The server is running HTTP version 1.1 (response version HTTP/1.1)
2. What languages (if any) does your browser indicate that it can accept to the server?



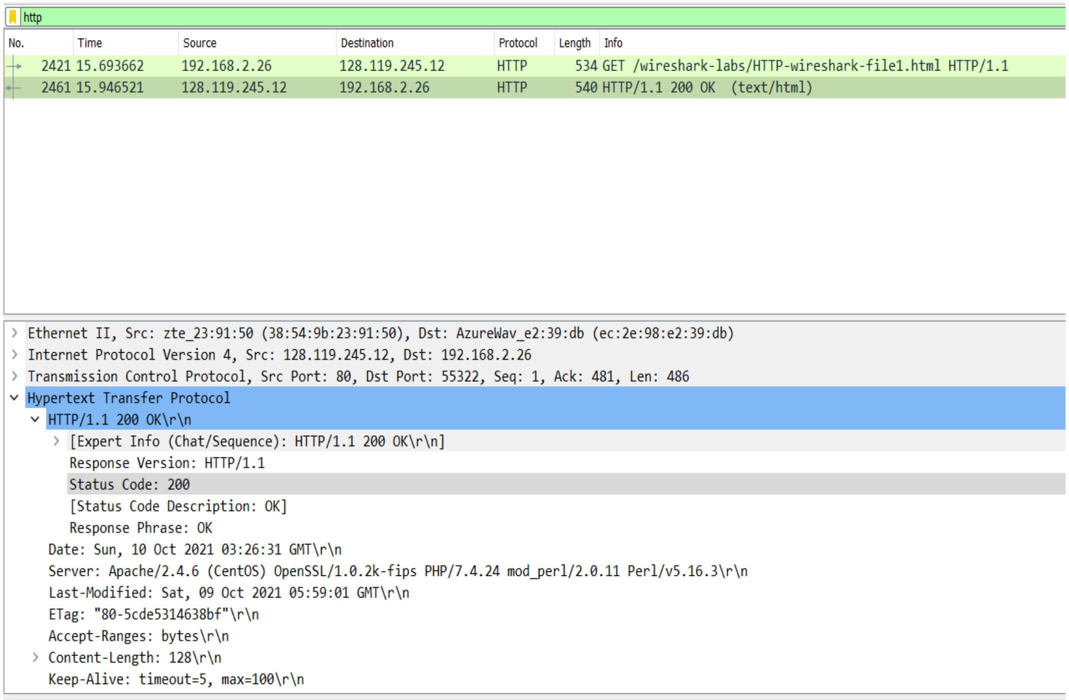
```
http

No.    Time       Source         Destination     Protocol  Length Info
  2421 15.693662  192.168.2.26   128.119.245.12  HTTP         534 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  2461 15.946521  128.119.245.12 192.168.2.26    HTTP         540 HTTP/1.1 200 OK  (text/html)

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-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\r
    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/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 2461]
```

Answer: Accept Language: en-US,en;q=0.9\r\n

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   Answer: Computer IP address: 192.168.2.26
   Server IP address: 128.119.245.12
4. What is the status code returned from the server to your browser?
   Answer:



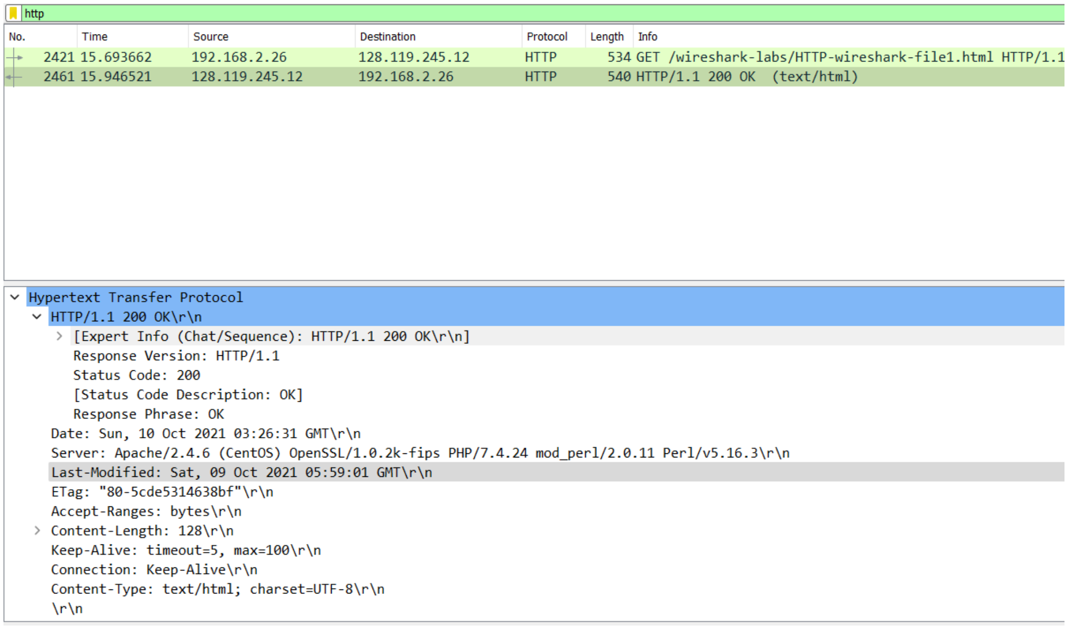
```
http
No.      Time        Source          Destination      Protocol  Length  Info
   2421 15.693662   192.168.2.26    128.119.245.12   HTTP       534 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   2461 15.946521   128.119.245.12  192.168.2.26     HTTP       540 HTTP/1.1 200 OK  (text/html)

> Ethernet II, Src: zte_23:91:50 (38:54:9b:23:91:50), Dst: AzureWav_e2:39:db (ec:2e:98:e2:39:db)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 55322, Seq: 1, Ack: 481, Len: 486
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, 10 Oct 2021 03:26:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 09 Oct 2021 05:59:01 GMT\r\n
    ETag: "80-5cde5314638bf"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

Status code: 200 OK

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

Answer:

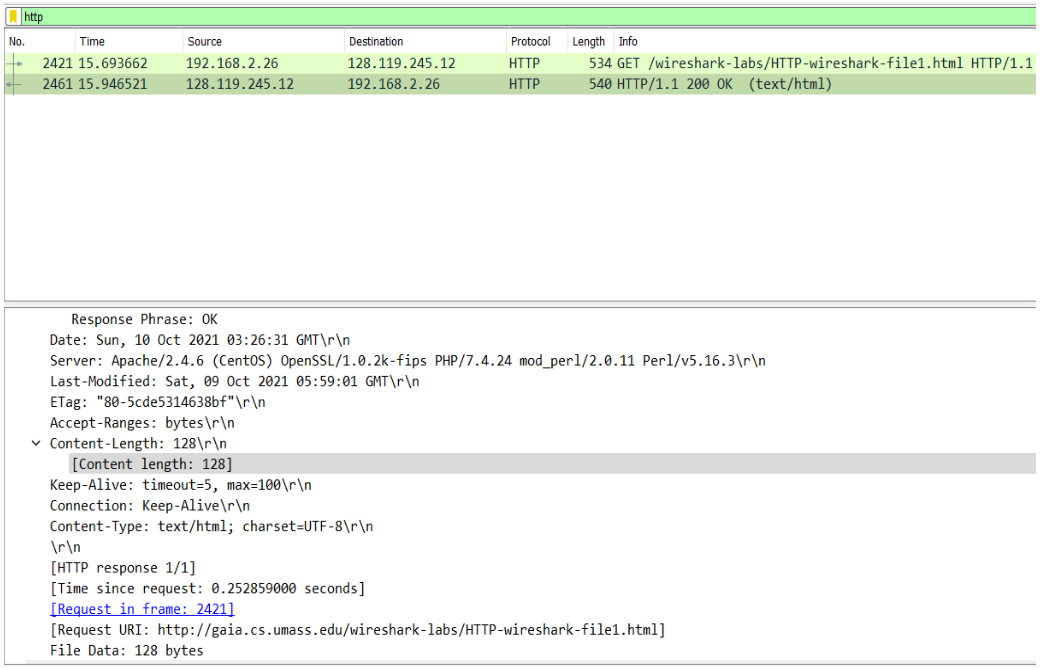


```
http
No.      Time        Source          Destination      Protocol  Length  Info
   2421 15.693662   192.168.2.26    128.119.245.12   HTTP       534 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   2461 15.946521   128.119.245.12  192.168.2.26     HTTP       540 HTTP/1.1 200 OK  (text/html)

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, 10 Oct 2021 03:26:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 09 Oct 2021 05:59:01 GMT\r\n
    ETag: "80-5cde5314638bf"\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
    \r\n
```

Last modified: Sat, 09 Oct 2021 05:59:01 GMT

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



```
http
No.       Time          Source            Destination       Protocol  Length  Info
  2421 15.693662     192.168.2.26      128.119.245.12    HTTP         534 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  2461 15.946521     128.119.245.12    192.168.2.26      HTTP         540 HTTP/1.1 200 OK  (text/html)
```

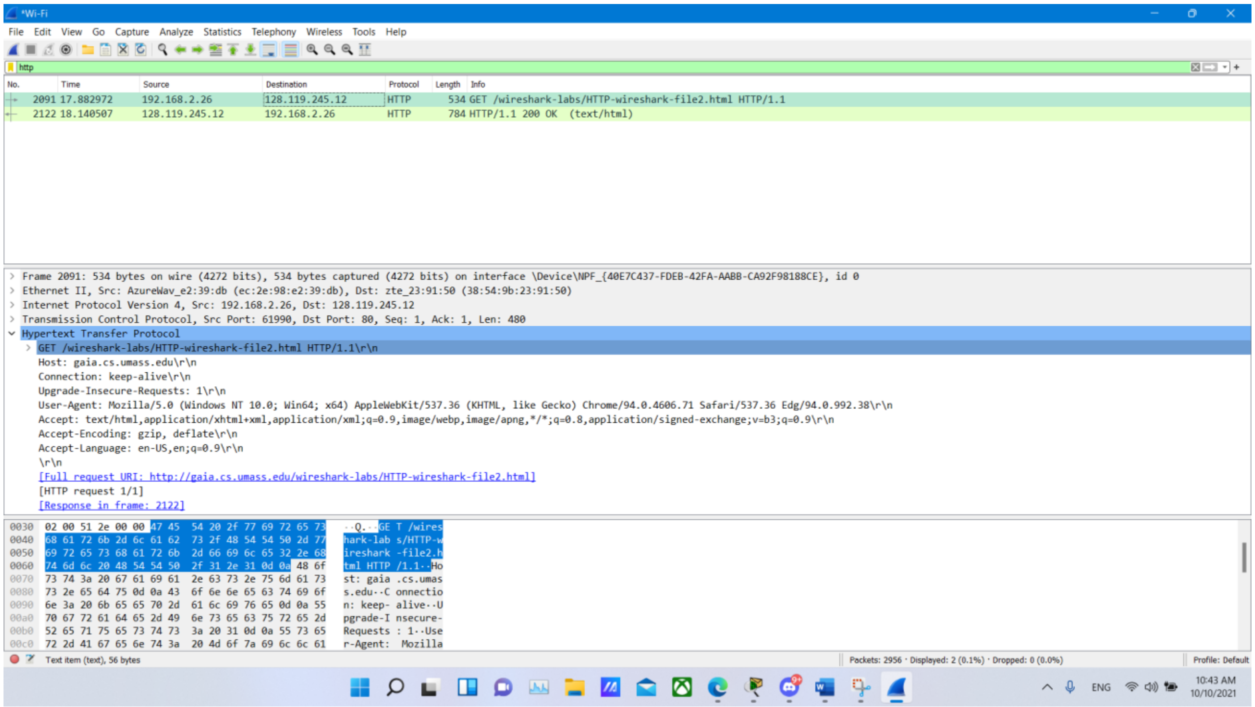
```
      Response Phrase: OK
   Date: Sun, 10 Oct 2021 03:26:31 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
   Last-Modified: Sat, 09 Oct 2021 05:59:01 GMT\r\n
   ETag: "80-5cde5314638bf"\r\n
   Accept-Ranges: bytes\r\n
 v Content-Length: 128\r\n
      [Content length: 128]
   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: 0.252859000 seconds]
   [Request in frame: 2421]
   [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
   File Data: 128 bytes
```

Content length: 128 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.

   Answer: After inspecting the raw data, I **don't see** any headers that are not displayed in the packet-listing window.

2. The HTTP CONDITIONAL GET/response interaction


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

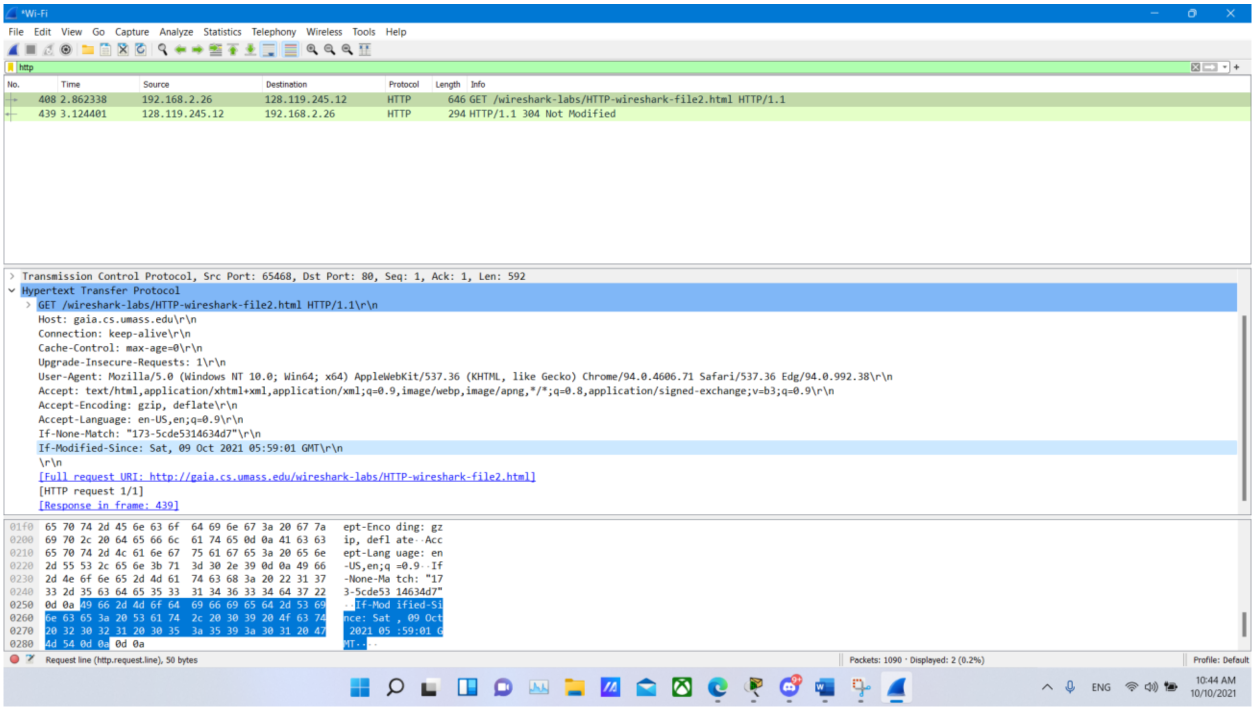
```
No.     Time       Source          Destination     Protocol  Length Info
  2091 17.882972   192.168.2.26    128.119.245.12  HTTP       534 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  2122 18.140507   128.119.245.12  192.168.2.26    HTTP       784 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 2091: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: AzureWav_e2:39:db (ec:2e:98:e2:39:db), Dst: zte_23:91:50 (38:54:9b:23:91:50)
> Internet Protocol Version 4, Src: 192.168.2.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61990, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
v 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 2122]
```

```
0030  02 00 51 2e 00 00 47 45  54 20 2f 77 69 72 65 73   ··Q.··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
```

```
Text item (text), 56 bytes    Packets: 2956 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

After quickly refresh and capture the again


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.     Time       Source          Destination     Protocol  Length Info
   408 2.862338    192.168.2.26    128.119.245.12  HTTP       646 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   439 3.124401    128.119.245.12  192.168.2.26    HTTP       294 HTTP/1.1 304 Not Modified
```

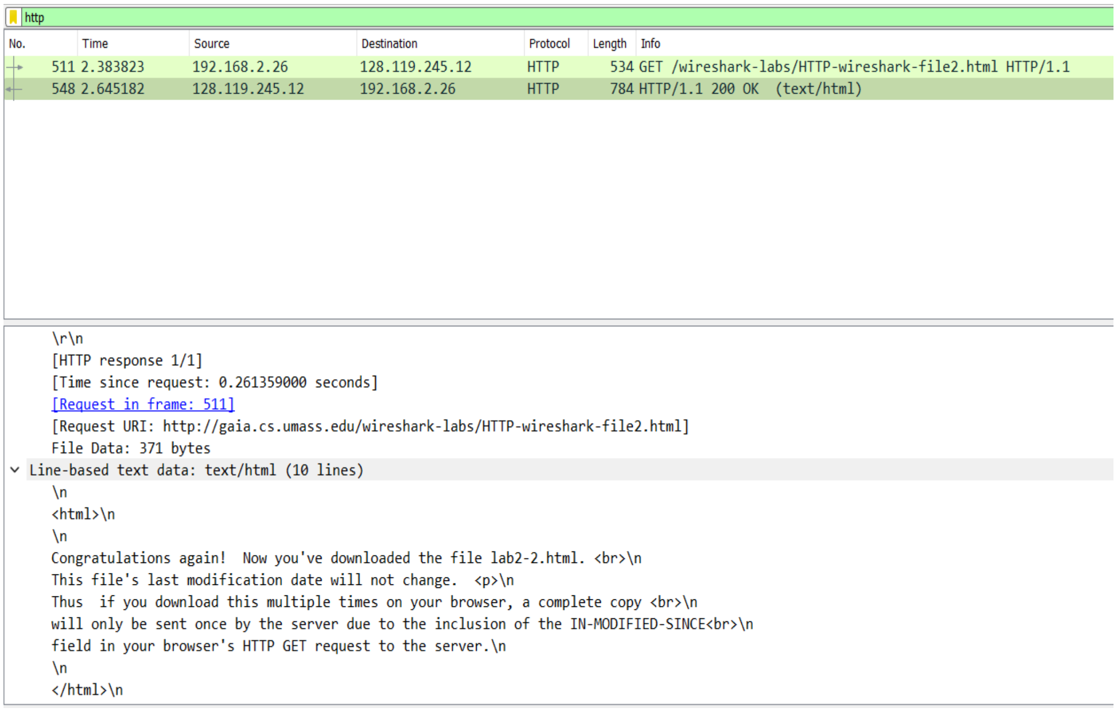
```
> Transmission Control Protocol, Src Port: 65468, Dst Port: 80, Seq: 1, Ack: 1, Len: 592
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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: "173-5cde5314634d7"\r\n
    If-Modified-Since: Sat, 09 Oct 2021 05:59:01 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: 439]
```

```
01f0  65 70 74 2d 45 6e 63 6f  64 69 6e 67 3a 20 67 7a   ept-Enco ding: gz
0200  69 70 2c 20 64 65 66 6c  61 74 65 0d 0a 41 63 63   ip, defl ate··Acc
0210  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
0220  2d 55 53 2c 65 6e 3b 71  3d 30 2e 39 0d 0a 49 66   -US,en;q =0.9··If
0230  2d 4e 6f 6e 65 2d 4d 61  74 63 68 3a 20 22 31 37   -None-Ma tch: "17
0240  33 2d 35 63 64 65 35 33  31 34 36 33 34 64 37 22   3-5cde53 14634d7"
0250  0d 0a 49 66 2d 4d 6f 64  69 66 69 65 64 2d 53 69   ··If-Mod ified-Si
0260  6e 63 65 3a 20 53 61 74  2c 20 30 39 20 4f 63 74   nce: Sat , 09 Oct
0270  20 32 30 32 31 20 30 35  3a 35 39 3a 30 31 20 47    2021 05 :59:01 G
0280  4d 54 0d 0a 0d 0a                                  MT····
```

```
Request line (http.request.line), 50 bytes    Packets: 1090 · Displayed: 2 (0.2%)    Profile: Default
```

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: In the First HTTP GET request, I saw no “IF-MODIFIED-SINCE” line.

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

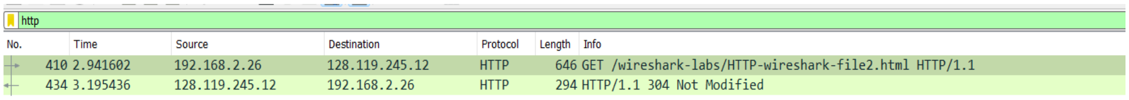


```
http
No.    Time        Source          Destination     Protocol  Length  Info
511    2.383823    192.168.2.26    128.119.245.12  HTTP      534     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
548    2.645182    128.119.245.12  192.168.2.26    HTTP      784     HTTP/1.1 200 OK  (text/html)
```

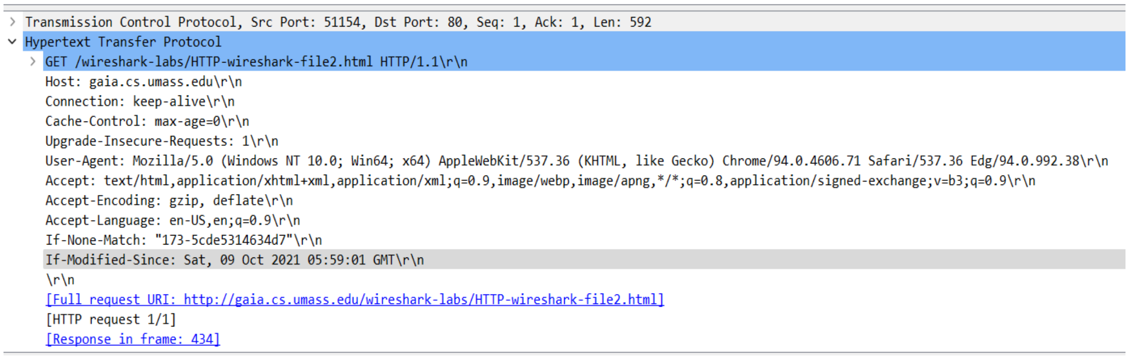
```
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.261359000 seconds]
      [Request in frame: 511]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      File Data: 371 bytes
   Line-based text data: text/html (10 lines)
      \n
      <html>\n
      \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<br>\n
      field in your browser's HTTP GET request to the server.\n
      \n
      </html>\n
```

   Yes, the server return explicitly the file content.

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:
    Yes.



```
http
No.   Time        Source          Destination     Protocol  Length  Info
  410 2.941602    192.168.2.26    128.119.245.12  HTTP         646  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  434 3.195436    128.119.245.12  192.168.2.26    HTTP         294  HTTP/1.1 304 Not Modified
```



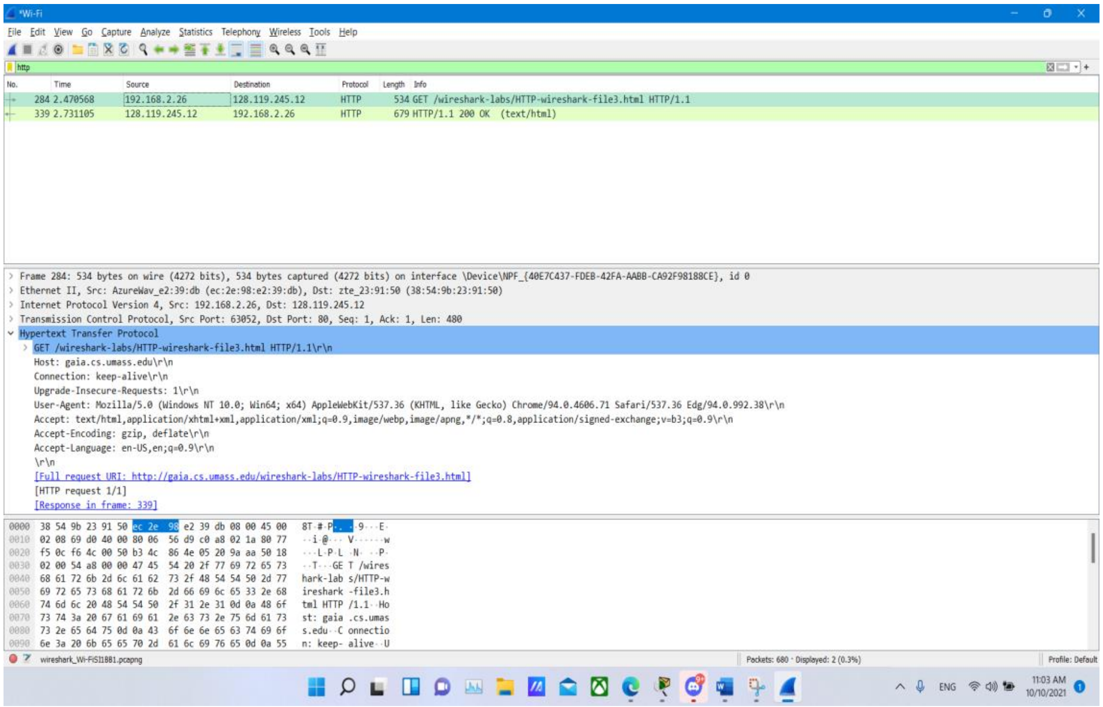
```
> Transmission Control Protocol, Src Port: 51154, Dst Port: 80, Seq: 1, Ack: 1, Len: 592
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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: "173-5cde5314634d7"\r\n
    If-Modified-Since: Sat, 09 Oct 2021 05:59:01 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: 434]
```

If-Modified-Since: Sat, 09 Oct 2021 05:59:01 GMT

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer:
Second HTTP GET status code: 304 Not Modified.
The server doesn't explicitly return the contents. Explain: Because, first time we HTTP GET from the server, the server will return the content of file and the browser will save the content of file into the cache for faster request next time. Hence, second HTTP GET in the browser will return from the cache not the server, the server doesn't need to return the content of file.

3. Retrieving Long Documents


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.       Time        Source          Destination      Protocol  Length  Info
    284 2.470568    192.168.2.26    128.119.245.12   HTTP        534 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    339 2.731105    128.119.245.12  192.168.2.26     HTTP        679 HTTP/1.1 200 OK  (text/html)
```

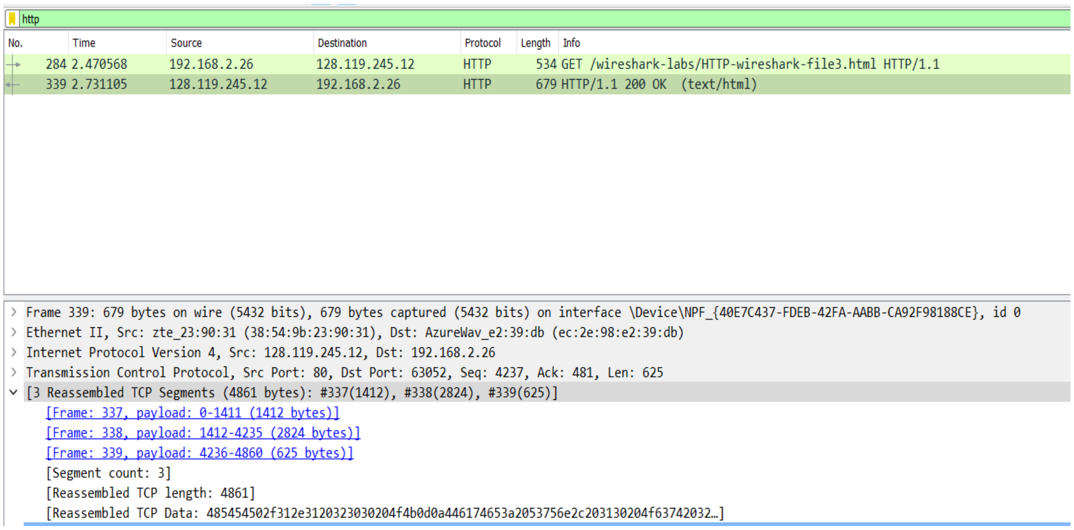
```
> Frame 284: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: AzureWav_e2:39:db (ec:2e:98:e2:39:db), Dst: zte_23:91:50 (38:54:9b:23:91:50)
> Internet Protocol Version 4, Src: 192.168.2.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63052, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.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/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 339]
```

```
0000  38 54 9b 23 91 50 ec 2e  98 e2 39 db 08 00 45 00   8T·#·P.. ·9···E·
0010  02 08 69 d0 40 00 80 06  56 d9 c0 a8 02 1a 80 77   ··i·@··· V······w
0020  f5 0c f6 4c 00 50 b3 4c  86 4e 05 20 9a aa 50 18   ···L·P·L ·N· ··P·
0030  02 00 54 a8 00 00 47 45  54 20 2f 77 69 72 65 73   ··T···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 33 2e 68   ireshark -file3.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
```

wireshark_Wi-FiSI1881.pcapng
Packets: 680 · Displayed: 2 (0.3%)
Profile: Default
ENG
11:03 AM
10/10/2021

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:
    There is 1 HTTP GET. The packet number: 84

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: 339
14. What is the status code and phrase in the response?
    Answer:
    Status code: 200 OK
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
    Answer:

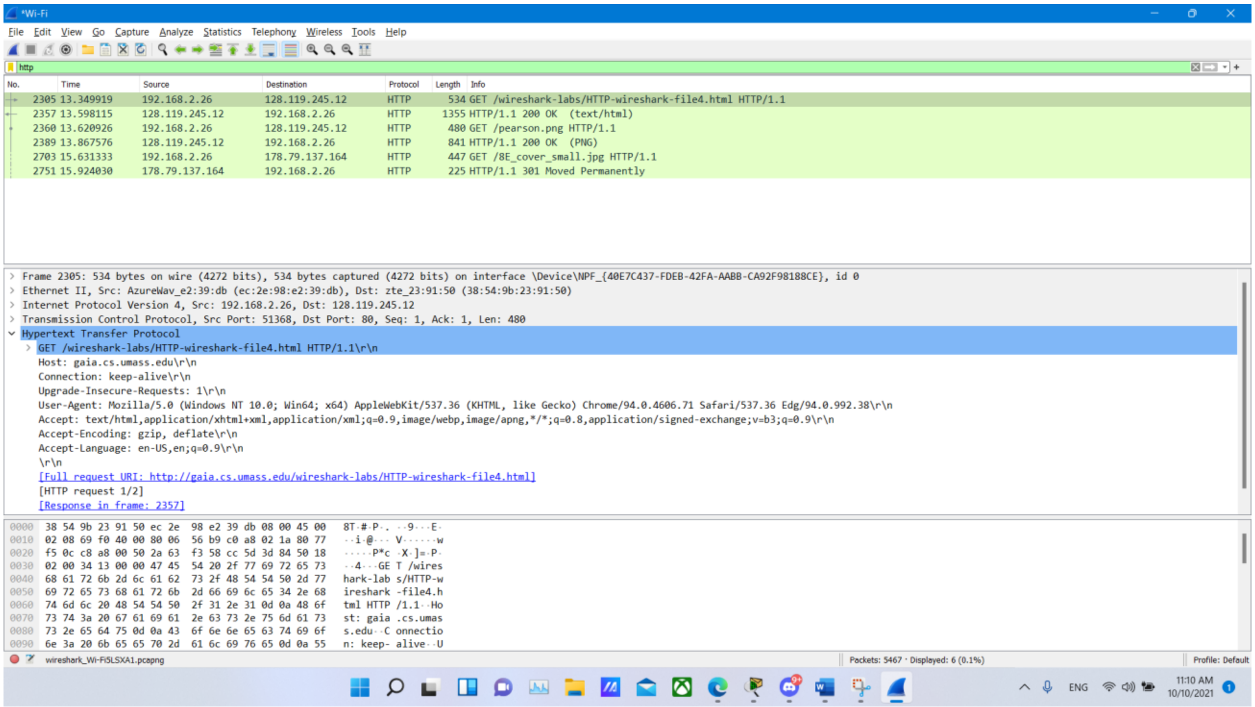


```
No.     Time        Source          Destination     Protocol  Length  Info
284 2.470568    192.168.2.26    128.119.245.12  HTTP      534 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
339 2.731105    128.119.245.12  192.168.2.26    HTTP      679 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 339: 679 bytes on wire (5432 bits), 679 bytes captured (5432 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: zte_23:90:31 (38:54:9b:23:90:31), Dst: AzureWav_e2:39:db (ec:2e:98:e2:39:db)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 63052, Seq: 4237, Ack: 481, Len: 625
v [3 Reassembled TCP Segments (4861 bytes): #337(1412), #338(2824), #339(625)]
     [Frame: 337, payload: 0-1411 (1412 bytes)]
     [Frame: 338, payload: 1412-4235 (2824 bytes)]
     [Frame: 339, payload: 4236-4860 (625 bytes)]
     [Segment count: 3]
     [Reassembled TCP length: 4861]
     [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203130204f63742032…]
```

There are 3 reassembled TCP segments.

4. HTML Documents with Embedded Objects


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
ENG
11:10 AM
10/10/2021

```
No.     Time         Source          Destination     Protocol  Length  Info
2305 13.349919   192.168.2.26    128.119.245.12  HTTP      534 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
2357 13.598115   128.119.245.12  192.168.2.26    HTTP     1355 HTTP/1.1 200 OK  (text/html)
2360 13.620926   192.168.2.26    128.119.245.12  HTTP      480 GET /pearson.png HTTP/1.1
2389 13.867576   128.119.245.12  192.168.2.26    HTTP      841 HTTP/1.1 200 OK  (PNG)
2703 15.631333   192.168.2.26    178.79.137.164  HTTP      447 GET /8E_cover_small.jpg HTTP/1.1
2751 15.924030   178.79.137.164  192.168.2.26    HTTP      225 HTTP/1.1 301 Moved Permanently
```

```
> Frame 2305: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: AzureWav_e2:39:db (ec:2e:98:e2:39:db), Dst: zte_23:91:50 (38:54:9b:23:91:50)
> Internet Protocol Version 4, Src: 192.168.2.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51368, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file4.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/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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/HTTP-wireshark-file4.html]
    [HTTP request 1/2]
    [Response in frame: 2357]
```

```
0000  38 54 9b 23 91 50 ec 2e  98 e2 39 db 08 00 45 00   8T·#·P·. ··9···E·
0010  02 08 69 f0 40 00 80 06  56 b9 c0 a8 02 1a 80 77   ··i·@··· V······w
0020  f5 0c c8 a8 00 50 2a 63  f3 58 cc 5d 3d 84 50 18   ·····P*c ·X·]=·P·
0030  02 00 34 13 00 00 47 45  54 20 2f 77 69 72 65 73   ··4···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 34 2e 68   ireshark -file4.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
```

wireshark_Wi-FiSLSXA1.pcapng | Packets: 5467 · Displayed: 6 (0.1%) | Profile: Default

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

Answer:

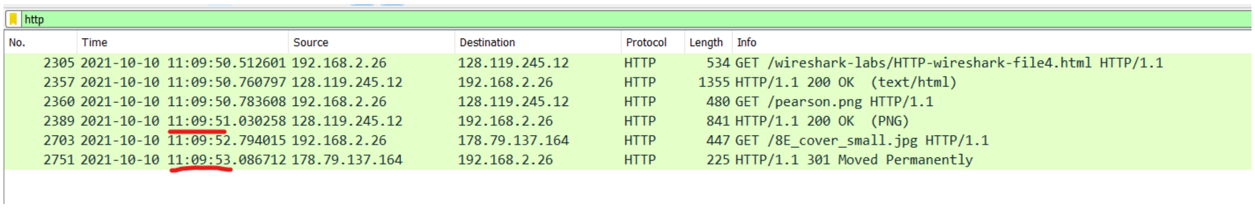
There are 3 HTTP GET.

First sent to: 128.119.245.12

Second sent to: 128.119.245.12

Third sent to: 178.79.137.164

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.

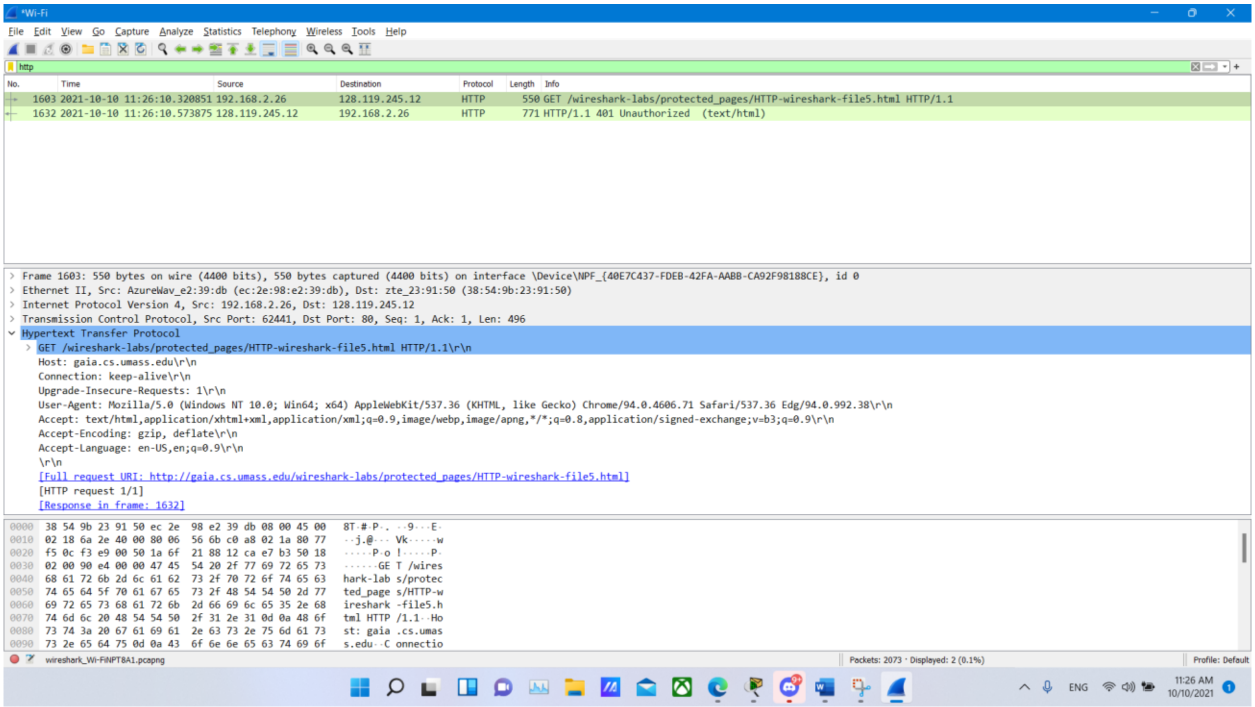


```
http
No.    Time                        Source          Destination     Protocol  Length  Info
  2305 2021-10-10 11:09:50.512601 192.168.2.26    128.119.245.12  HTTP       534 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  2357 2021-10-10 11:09:50.760797 128.119.245.12  192.168.2.26    HTTP      1355 HTTP/1.1 200 OK  (text/html)
  2360 2021-10-10 11:09:50.783608 192.168.2.26    128.119.245.12  HTTP       480 GET /pearson.png HTTP/1.1
  2389 2021-10-10 11:09:51.030258 128.119.245.12  192.168.2.26    HTTP       841 HTTP/1.1 200 OK  (PNG)
  2703 2021-10-10 11:09:52.794015 192.168.2.26    178.79.137.164  HTTP       447 GET /8E_cover_small.jpg HTTP/1.1
  2751 2021-10-10 11:09:53.086712 178.79.137.164  192.168.2.26    HTTP       225 HTTP/1.1 301 Moved Permanently
```

Answer:

Comparing the date that the server responses between 2 images. The request time of the jpg image come after the response time of first png picture. Hence, the browser downloaded these **serially**.

5. HTTP Authentication



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time                        Source          Destination     Protocol  Length  Info
  1603 2021-10-10 11:26:10.320851 192.168.2.26    128.119.245.12  HTTP       550 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  1632 2021-10-10 11:26:10.573875 128.119.245.12  192.168.2.26    HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
```

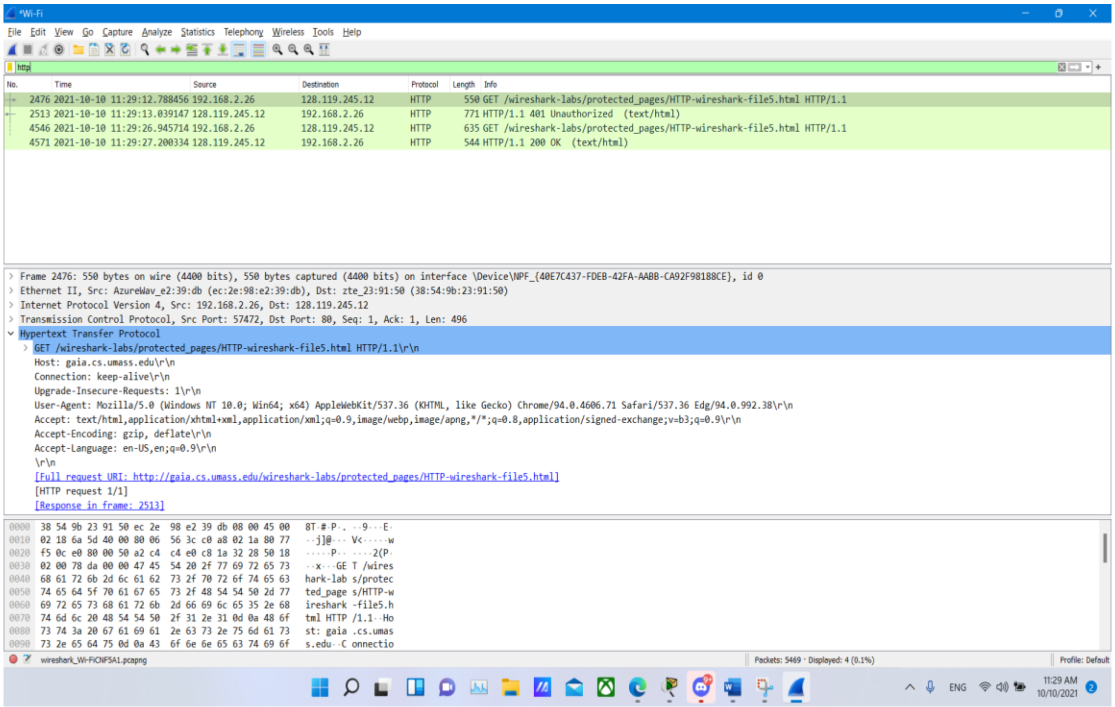
```
> Frame 1603: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: AzureWav_e2:39:db (ec:2e:98:e2:39:db), Dst: zte_23:91:50 (38:54:9b:23:91:50)
> Internet Protocol Version 4, Src: 192.168.2.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62441, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
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/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 1632]
```

```
0000  38 54 9b 23 91 50 ec 2e  98 e2 39 db 08 00 45 00   8T·#·P·. ··9···E·
0010  02 18 6a 2e 40 00 80 06  56 6b c0 a8 02 1a 80 77   ··j.@··· Vk·····w
0020  f5 0c f3 e9 00 50 1a 6f  21 88 12 ca e7 b3 50 18   ·····P·o !·····P·
0030  02 00 90 e4 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 35 2e 68   ireshark -file5.h
0070  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0080  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0090  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
```

wireshark_Wi-FiNPT8A1.pcapng
Packets: 2073 · Displayed: 2 (0.1%)
Profile: Default
ENG
11:26 AM
10/10/2021

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

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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

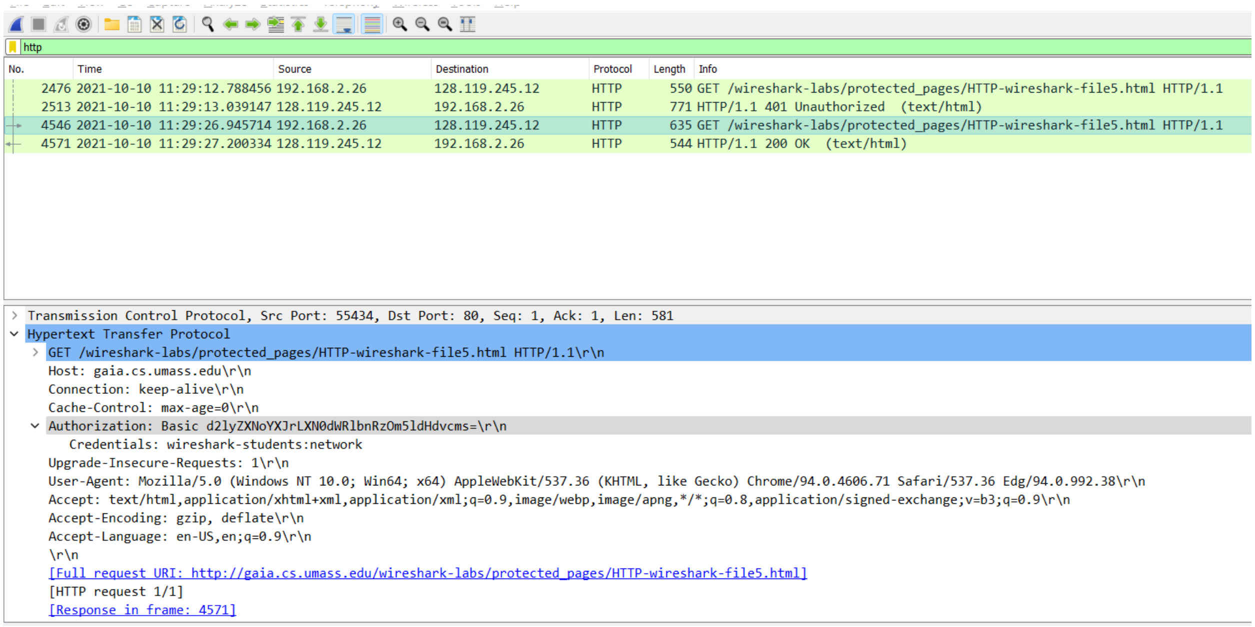
```
No.   Time                       Source          Destination     Protocol Length Info
2476 2021-10-10 11:29:12.788456 192.168.2.26    128.119.245.12  HTTP      550 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2513 2021-10-10 11:29:13.039147 128.119.245.12  192.168.2.26    HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
4546 2021-10-10 11:29:26.945714 192.168.2.26    128.119.245.12  HTTP      635 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4571 2021-10-10 11:29:27.200334 128.119.245.12  192.168.2.26    HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 2476: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{40E7C437-FDEB-42FA-AABB-CA92F98188CE}, id 0
> Ethernet II, Src: AzureWav_e2:39:db (ec:2e:98:e2:39:db), Dst: zte_23:91:50 (38:54:9b:23:91:50)
> Internet Protocol Version 4, Src: 192.168.2.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 57472, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
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/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 2513]
```

```
0000  38 54 9b 23 91 50 ec 2e  98 e2 39 db 08 00 45 00   8T·#·P·. ··9···E·
0010  02 18 6a 5d 40 00 80 06  56 3c c0 a8 02 1a 80 77   ··j]@··· V<·····w
0020  f5 0c e0 80 00 50 a2 c4  c4 e0 c8 1a 32 28 50 18   ·····P·· ····2(P·
0030  02 00 78 da 00 00 47 45  54 20 2f 77 69 72 65 73   ··x···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 35 2e 68   ireshark -file5.h
0070  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0080  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0090  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
```

wireshark_Wi-FiCNF5A1.pcapng
Packets: 5469 · Displayed: 4 (0.1%)
Profile: Default
ENG
11:29 AM
10/10/2021

Answer:



```
No.   Time                       Source          Destination     Protocol Length Info
2476 2021-10-10 11:29:12.788456 192.168.2.26    128.119.245.12  HTTP      550 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2513 2021-10-10 11:29:13.039147 128.119.245.12  192.168.2.26    HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
4546 2021-10-10 11:29:26.945714 192.168.2.26    128.119.245.12  HTTP      635 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4571 2021-10-10 11:29:27.200334 128.119.245.12  192.168.2.26    HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
> Transmission Control Protocol, Src Port: 55434, Dst Port: 80, Seq: 1, Ack: 1, Len: 581
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/94.0.4606.71 Safari/537.36 Edg/94.0.992.38\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/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 4571]
```

New field is included: Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms= (encrypted string) with Credentials: wireshark-students:network