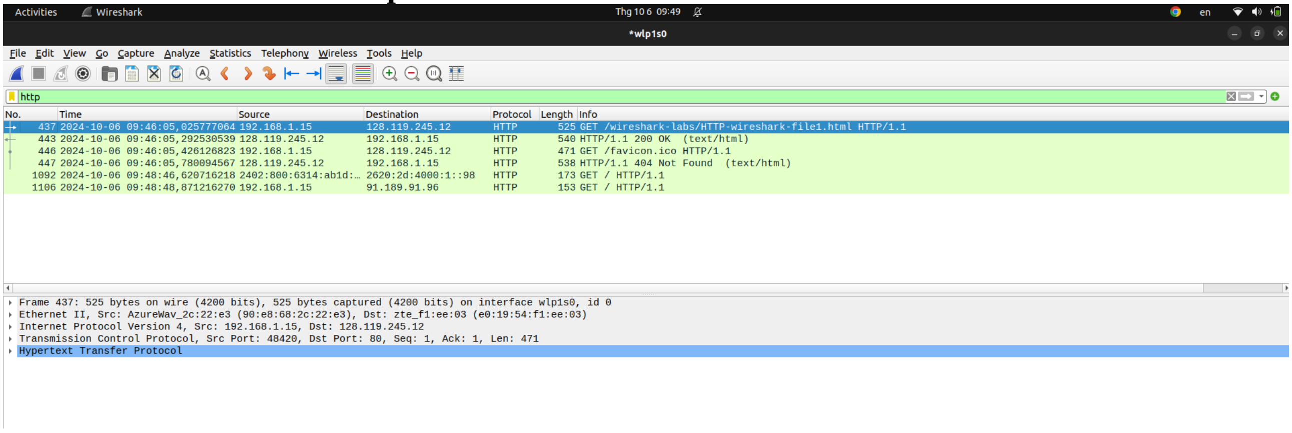
Computer Networks
Lab 2a

WIRESHARK LAB: HTTP v8.0

Student's name: Nguyễn Hữu Khang
Student's Id: 2011365
Class: L09

Please visit this link to view all my packet tracer capture for this lab: https://github.com/Khang-CS/HCMUT_Computer_Network_Lab/tree/main/Lab2a/packet_tracer_capture

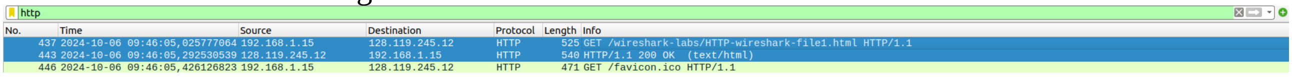
1. The Basic HTTP GET/response interaction


Activities
Wireshark
Thg 10 6 09:49
en
*wlp1s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time                          Source                Destination        Protocol Length Info
  437 2024-10-06 09:46:05,025777064 192.168.1.15          128.119.245.12     HTTP        525 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  443 2024-10-06 09:46:05,292530539 128.119.245.12        192.168.1.15       HTTP        540 HTTP/1.1 200 OK  (text/html)
  446 2024-10-06 09:46:05,426126823 192.168.1.15          128.119.245.12     HTTP        471 GET /favicon.ico HTTP/1.1
  447 2024-10-06 09:46:05,780094567 128.119.245.12        192.168.1.15       HTTP        538 HTTP/1.1 404 Not Found  (text/html)
 1092 2024-10-06 09:48:46,620716218 2402:800:6314:ab1d:… 2620:2d:4000:1::98 HTTP        173 GET / HTTP/1.1
 1106 2024-10-06 09:48:48,871216270 192.168.1.15          91.189.91.96       HTTP        153 GET / HTTP/1.1

› Frame 437: 525 bytes on wire (4200 bits), 525 bytes captured (4200 bits) on interface wlp1s0, id 0
› Ethernet II, Src: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3), Dst: zte_f1:ee:03 (e0:19:54:f1:ee:03)
› Internet Protocol Version 4, Src: 192.168.1.15, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 48420, Dst Port: 80, Seq: 1, Ack: 1, Len: 471
› Hypertext Transfer Protocol
```

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

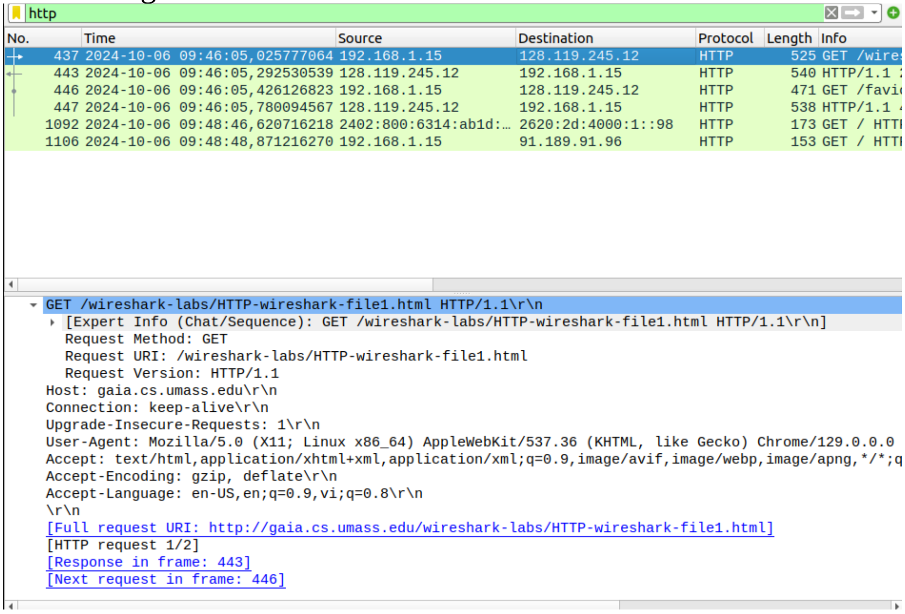
- My browser is running HTTP version 1.1
- The server is running HTTP version 1.1



```
http
No.   Time                          Source         Destination    Protocol Length Info
  437 2024-10-06 09:46:05,025777064 192.168.1.15   128.119.245.12 HTTP        525 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  443 2024-10-06 09:46:05,292530539 128.119.245.12 192.168.1.15   HTTP        540 HTTP/1.1 200 OK  (text/html)
  446 2024-10-06 09:46:05,426126823 192.168.1.15   128.119.245.12 HTTP        471 GET /favicon.ico HTTP/1.1
```

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

- It is "en-US, vi"
- Accepted language is displayed in "Accept-Language: en-US, en; q=0.9,vi;q=0.8\r\n" in the HTTP GET message.



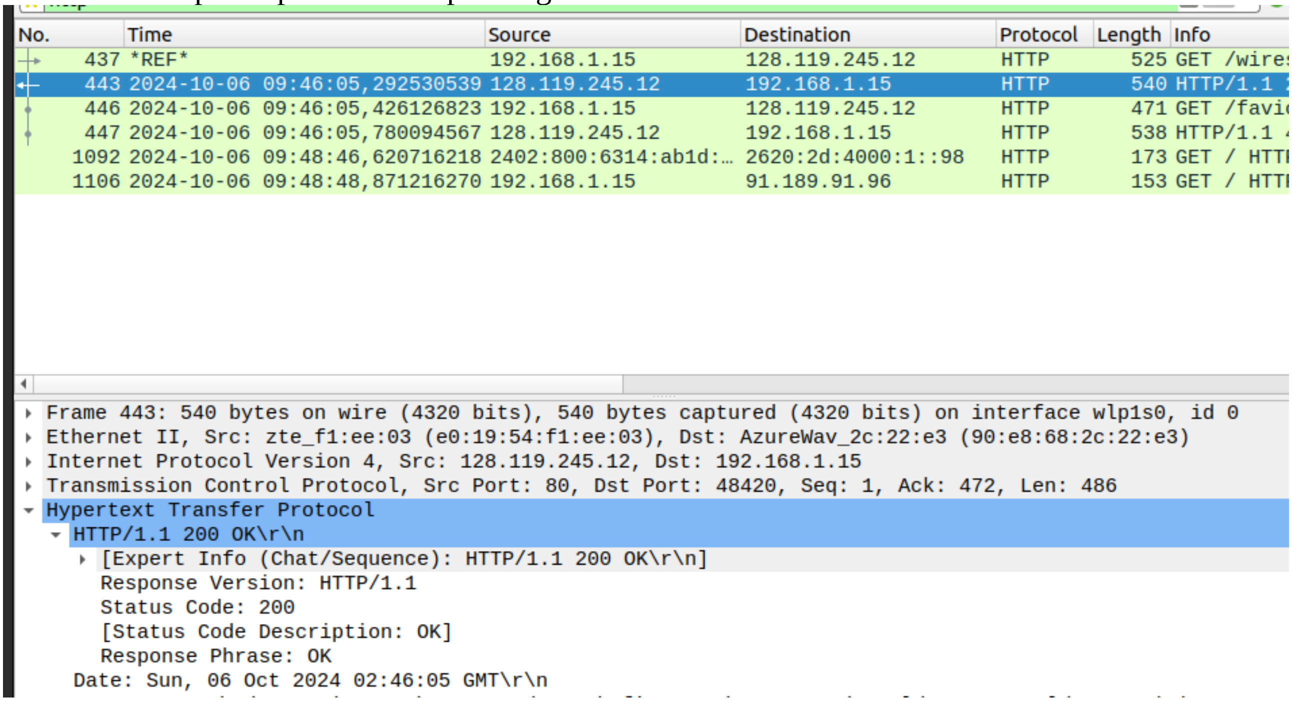
```
http
No.   Time                          Source                Destination        Protocol Length Info
  437 2024-10-06 09:46:05,025777064 192.168.1.15          128.119.245.12     HTTP        525 GET /wires
  443 2024-10-06 09:46:05,292530539 128.119.245.12        192.168.1.15       HTTP        540 HTTP/1.1 2
  446 2024-10-06 09:46:05,426126823 192.168.1.15          128.119.245.12     HTTP        471 GET /favic
  447 2024-10-06 09:46:05,780094567 128.119.245.12        192.168.1.15       HTTP        538 HTTP/1.1 4
 1092 2024-10-06 09:48:46,620716218 2402:800:6314:ab1d:… 2620:2d:4000:1::98 HTTP        173 GET / HTTP
 1106 2024-10-06 09:48:48,871216270 192.168.1.15          91.189.91.96       HTTP        153 GET / HTTP

  ⌄ 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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,vi;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 443]
    [Next request in frame: 446]
```

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

- The IP address of my computer is 192.168.1.15
- The IP address of gaia.cs.umass.edu.server is 128.119.245.12
- Those information are located in field "source" and "destination"

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

- The status code returned from the server is 200
- The response phrase corresponding the status code is OK

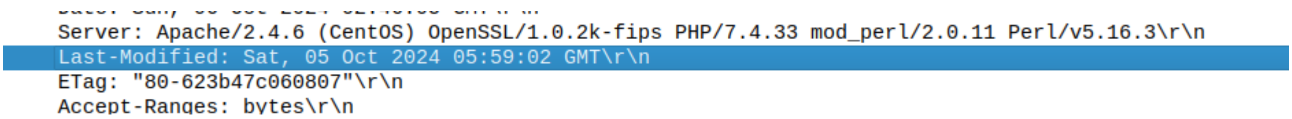


```
No.   Time                           Source                 Destination          Protocol Length Info
  437 *REF*                          192.168.1.15           128.119.245.12       HTTP     525 GET /wires
  443 2024-10-06 09:46:05,292530539  128.119.245.12         192.168.1.15         HTTP     540 HTTP/1.1 2
  446 2024-10-06 09:46:05,426126823  192.168.1.15           128.119.245.12       HTTP     471 GET /favic
  447 2024-10-06 09:46:05,780094567  128.119.245.12         192.168.1.15         HTTP     538 HTTP/1.1 4
 1092 2024-10-06 09:48:46,620716218  2402:800:6314:ab1d:…   2620:2d:4000:1::98   HTTP     173 GET / HTTP
 1106 2024-10-06 09:48:48,871216270  192.168.1.15           91.189.91.96         HTTP     153 GET / HTTP
```

```
▸ Frame 443: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface wlp1s0, id 0
▸ Ethernet II, Src: zte_f1:ee:03 (e0:19:54:f1:ee:03), Dst: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 48420, Seq: 1, Ack: 472, Len: 486
▾ 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
    Date: Sun, 06 Oct 2024 02:46:05 GMT\r\n
```

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

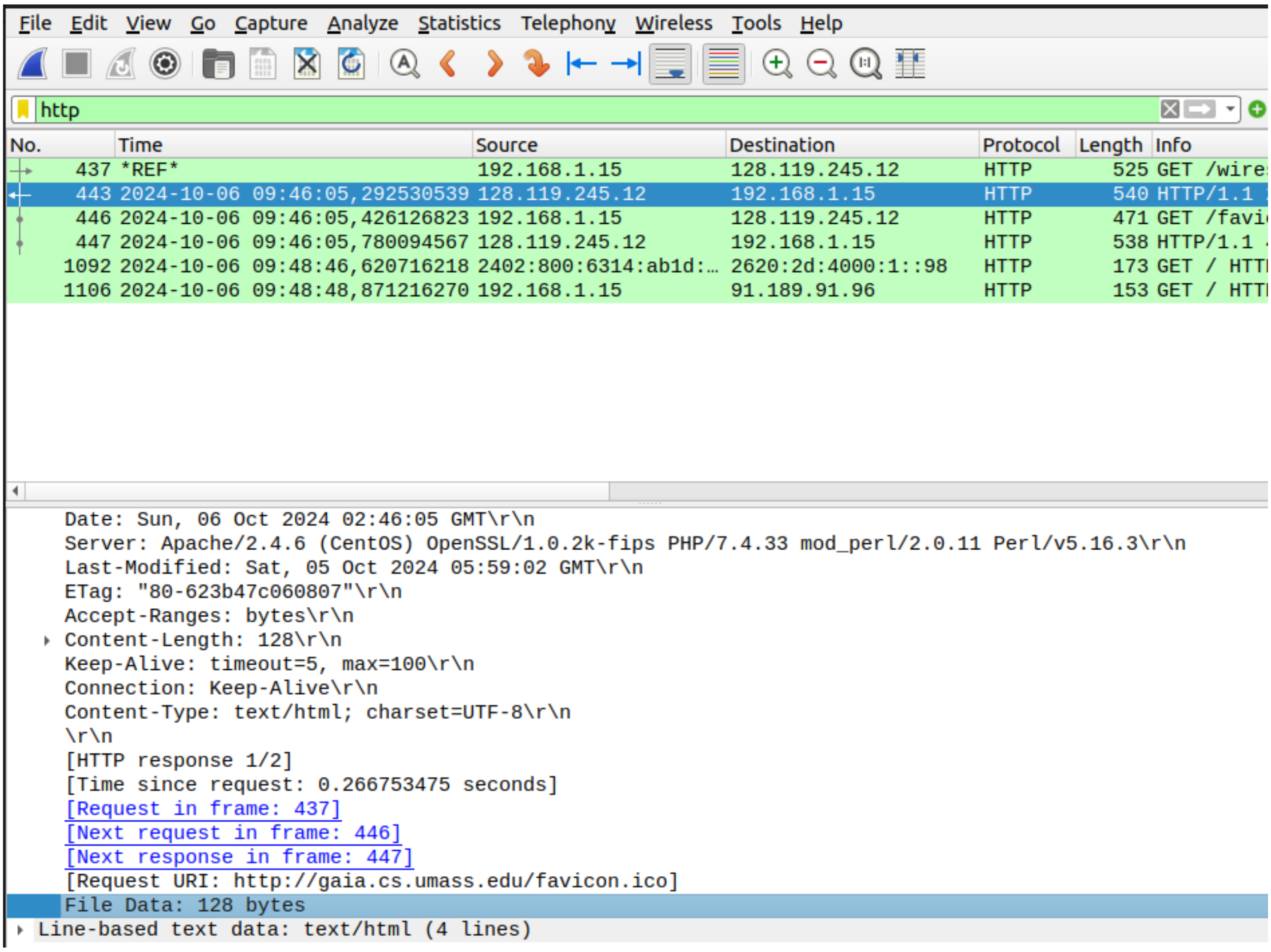
- It is Sat, 05 Oct 2024 05:59:02 GMT



```
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 05 Oct 2024 05:59:02 GMT\r\n
ETag: "80-623b47c060807"\r\n
Accept-Ranges: bytes\r\n
```

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

- There are 128 bytes

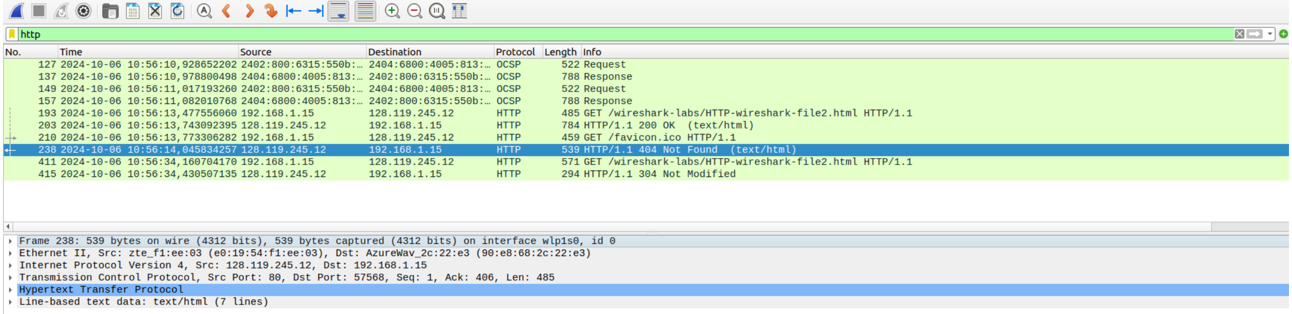

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.     Time                           Source               Destination          Protocol  Length Info
    437 *REF*                          192.168.1.15         128.119.245.12       HTTP         525 GET /wire
    443 2024-10-06 09:46:05,292530539 128.119.245.12       192.168.1.15         HTTP         540 HTTP/1.1
    446 2024-10-06 09:46:05,426126823 192.168.1.15         128.119.245.12       HTTP         471 GET /favi
    447 2024-10-06 09:46:05,780094567 128.119.245.12       192.168.1.15         HTTP         538 HTTP/1.1
   1092 2024-10-06 09:48:46,620716218 2402:800:6314:ab1d:… 2620:2d:4000:1::98   HTTP         173 GET / HTT
   1106 2024-10-06 09:48:48,871216270 192.168.1.15         91.189.91.96         HTTP         153 GET / HTT
```

```
    Date: Sun, 06 Oct 2024 02:46:05 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 05 Oct 2024 05:59:02 GMT\r\n
    ETag: "80-623b47c060807"\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
    [HTTP response 1/2]
    [Time since request: 0.266753475 seconds]
    [Request in frame: 437]
    [Next request in frame: 446]
    [Next response in frame: 447]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 128 bytes
› Line-based text data: text/html (4 lines)
```

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, everything are displayed.

2. The HTTP CONDITIONAL GET/response interaction

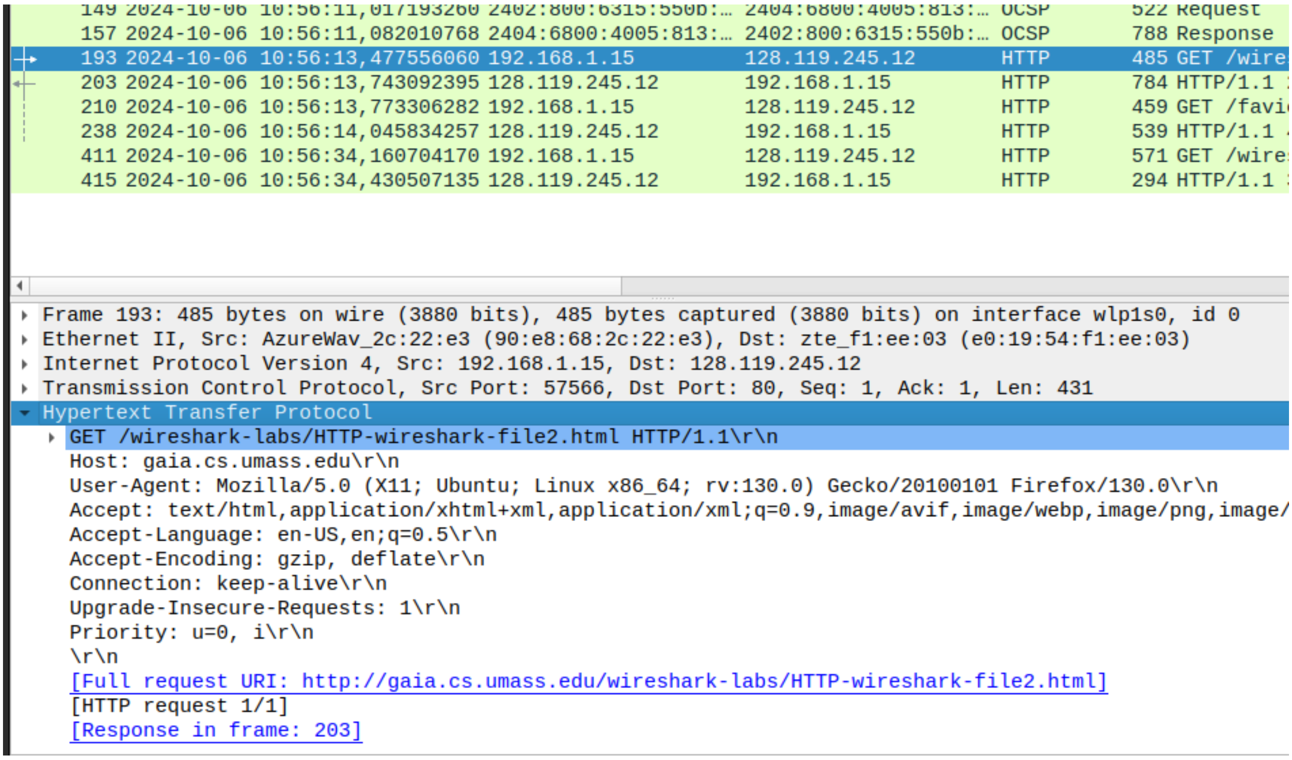


```
http
No.   Time                           Source               Destination          Protocol Length Info
  127 2024-10-06 10:56:10,928652202 2402:800:6315:550b:… 2404:6800:4005:813:… OCSP      522 Request
  137 2024-10-06 10:56:10,978800498 2404:6800:4005:813:… 2402:800:6315:550b:… OCSP      788 Response
  149 2024-10-06 10:56:11,017193260 2402:800:6315:550b:… 2404:6800:4005:813:… OCSP      522 Request
  157 2024-10-06 10:56:11,082010768 2404:6800:4005:813:… 2402:800:6315:550b:… OCSP      788 Response
  193 2024-10-06 10:56:13,477556060 192.168.1.15         128.119.245.12       HTTP      485 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  203 2024-10-06 10:56:13,743092395 128.119.245.12       192.168.1.15         HTTP      784 HTTP/1.1 200 OK  (text/html)
  210 2024-10-06 10:56:13,773306282 192.168.1.15         128.119.245.12       HTTP      459 GET /favicon.ico HTTP/1.1
  238 2024-10-06 10:56:14,045834257 128.119.245.12       192.168.1.15         HTTP      539 HTTP/1.1 404 Not Found  (text/html)
  411 2024-10-06 10:56:34,160704170 192.168.1.15         128.119.245.12       HTTP      571 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  415 2024-10-06 10:56:34,430507135 128.119.245.12       192.168.1.15         HTTP      294 HTTP/1.1 304 Not Modified
```

```
› Frame 238: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface wlp1s0, id 0
› Ethernet II, Src: zte_f1:ee:03 (e0:19:54:f1:ee:03), Dst: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3)
› Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.15
› Transmission Control Protocol, Src Port: 80, Dst Port: 57568, Seq: 1, Ack: 406, Len: 485
› Hypertext Transfer Protocol
› Line-based text data: text/html (7 lines)
```

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 there isn't any line "IF-MODIFIED-SINCE" in the first HTTP GET request.



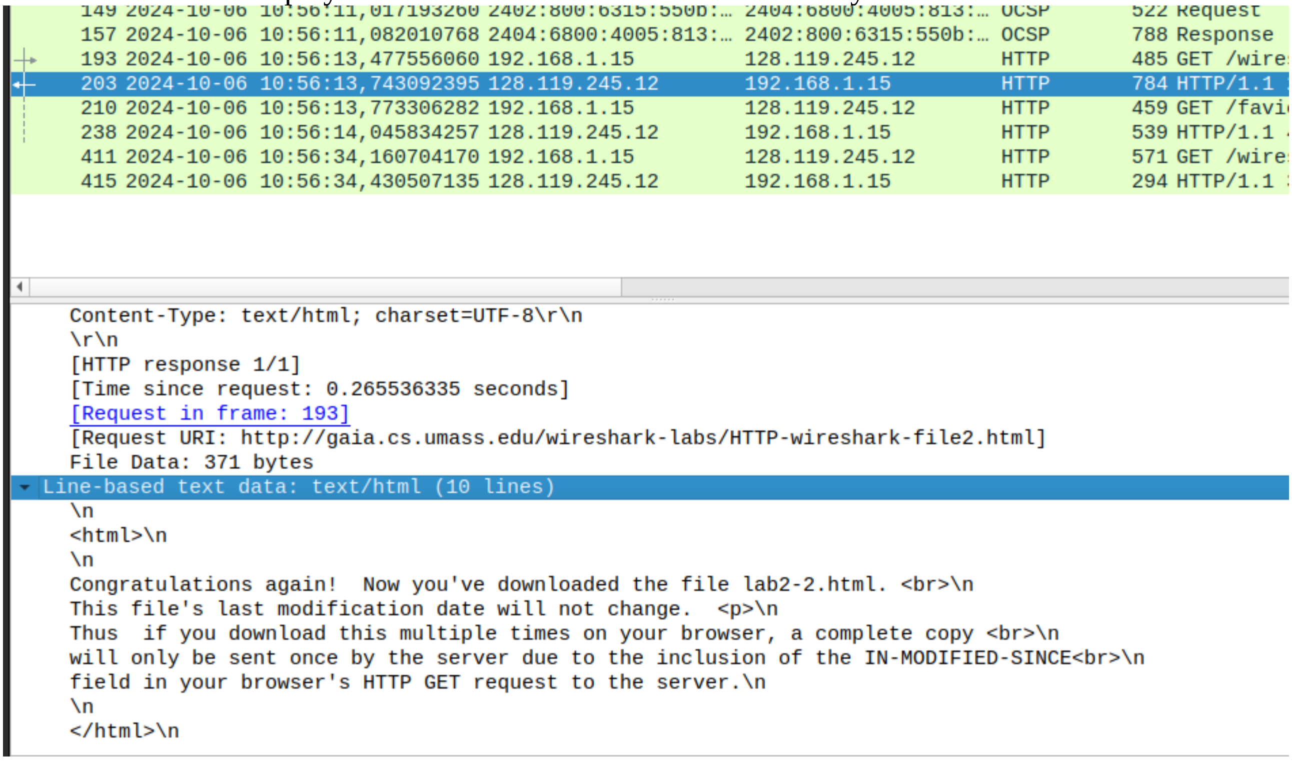
```
149 2024-10-06 10:56:11,017193260 2402:800:6315:550b:… 2404:6800:4005:813:… OCSP     522 Request
157 2024-10-06 10:56:11,082010768 2404:6800:4005:813:… 2402:800:6315:550b:… OCSP     788 Response
193 2024-10-06 10:56:13,477556060 192.168.1.15         128.119.245.12       HTTP     485 GET /wire
203 2024-10-06 10:56:13,743092395 128.119.245.12       192.168.1.15         HTTP     784 HTTP/1.1
210 2024-10-06 10:56:13,773306282 192.168.1.15         128.119.245.12       HTTP     459 GET /favi
238 2024-10-06 10:56:14,045834257 128.119.245.12       192.168.1.15         HTTP     539 HTTP/1.1
411 2024-10-06 10:56:34,160704170 192.168.1.15         128.119.245.12       HTTP     571 GET /wire
415 2024-10-06 10:56:34,430507135 128.119.245.12       192.168.1.15         HTTP     294 HTTP/1.1
```

```
Frame 193: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface wlp1s0, id 0
Ethernet II, Src: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3), Dst: zte_f1:ee:03 (e0:19:54:f1:ee:03)
Internet Protocol Version 4, Src: 192.168.1.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57566, Dst Port: 80, Seq: 1, Ack: 1, Len: 431
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\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: 203]
```

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

* Answer:

- The Server does explicity return the contents of the file. There is a line called line-based text data which display the same content as what i receive in my browser.



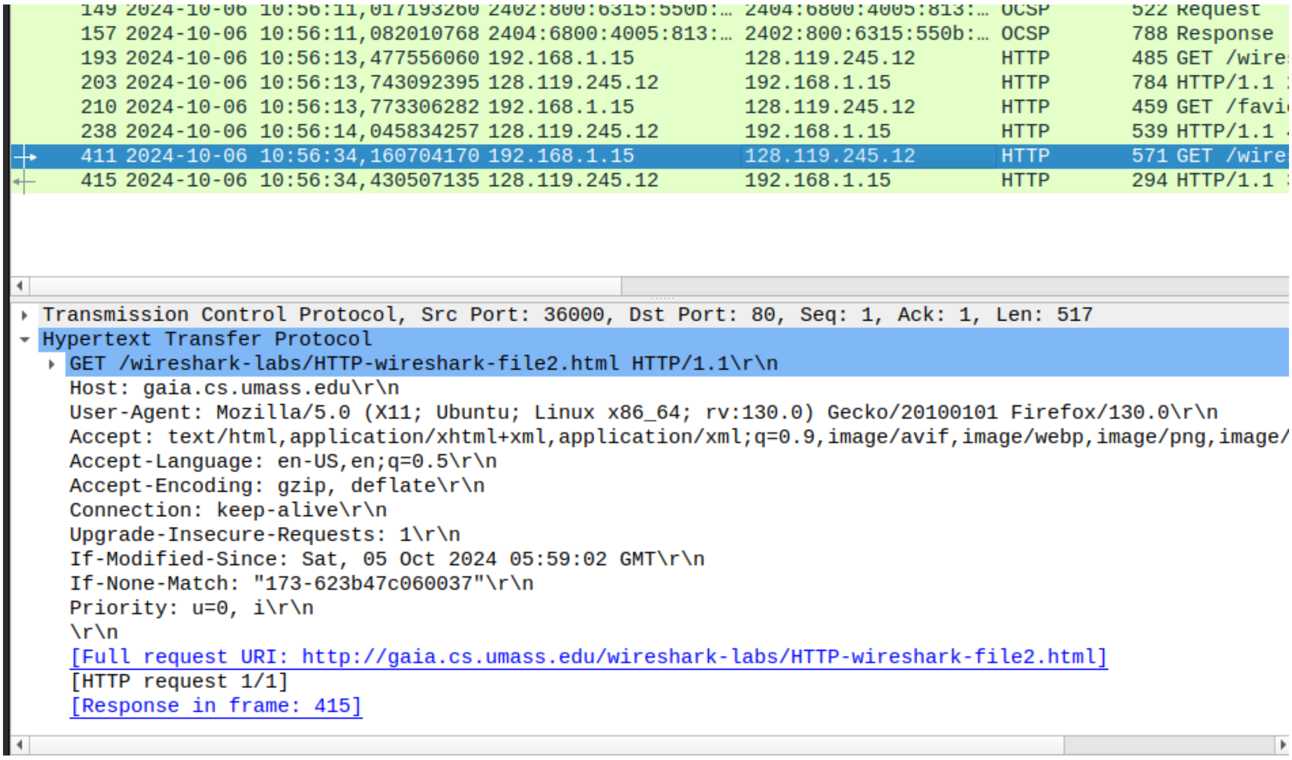
```
149 2024-10-06 10:56:11,017193260 2402:800:6315:550b:… 2404:6800:4005:813:… OCSP     522 Request
157 2024-10-06 10:56:11,082010768 2404:6800:4005:813:… 2402:800:6315:550b:… OCSP     788 Response
193 2024-10-06 10:56:13,477556060 192.168.1.15         128.119.245.12       HTTP     485 GET /wire
203 2024-10-06 10:56:13,743092395 128.119.245.12       192.168.1.15         HTTP     784 HTTP/1.1
210 2024-10-06 10:56:13,773306282 192.168.1.15         128.119.245.12       HTTP     459 GET /favi
238 2024-10-06 10:56:14,045834257 128.119.245.12       192.168.1.15         HTTP     539 HTTP/1.1
411 2024-10-06 10:56:34,160704170 192.168.1.15         128.119.245.12       HTTP     571 GET /wire
415 2024-10-06 10:56:34,430507135 128.119.245.12       192.168.1.15         HTTP     294 HTTP/1.1
```

```
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.265536335 seconds]
  [Request in frame: 193]
  [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
```

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:

- There is "IF-MODIFIED-SINCE" line.
- The If-Modified-Since HTTP header indicates the time for which a browser first downloaded a resource from the server.



```
149 2024-10-06 10:56:11,017193260 2402:800:6315:550b:… 2404:6800:4005:813:… OCSP      522 Request
157 2024-10-06 10:56:11,082010768 2404:6800:4005:813:… 2402:800:6315:550b:… OCSP      788 Response
193 2024-10-06 10:56:13,477556060 192.168.1.15         128.119.245.12       HTTP      485 GET /wire
203 2024-10-06 10:56:13,743092395 128.119.245.12       192.168.1.15         HTTP      784 HTTP/1.1 
210 2024-10-06 10:56:13,773306282 192.168.1.15         128.119.245.12       HTTP      459 GET /favi
238 2024-10-06 10:56:14,045834257 128.119.245.12       192.168.1.15         HTTP      539 HTTP/1.1 
411 2024-10-06 10:56:34,160704170 192.168.1.15         128.119.245.12       HTTP      571 GET /wire
415 2024-10-06 10:56:34,430507135 128.119.245.12       192.168.1.15         HTTP      294 HTTP/1.1 
```

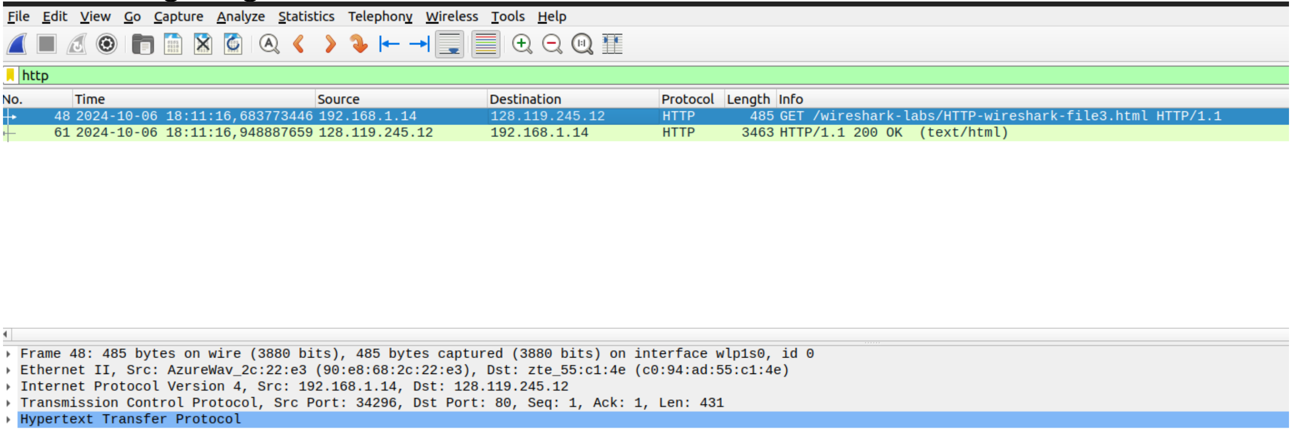
```
▸ Transmission Control Protocol, Src Port: 36000, Dst Port: 80, Seq: 1, Ack: 1, Len: 517
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Sat, 05 Oct 2024 05:59:02 GMT\r\n
    If-None-Match: "173-623b47c060037"\r\n
    Priority: u=0, i\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: 415]
```

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:

- The status code is “304” and the phrase response is “Not Modified”.
- No the server does not explicitly return the contents of the file. The reason is it simply retrieved the contents from its cache. If the file has been modified since it was last accessed, it would have returned the contents of the file, Otherwise it simply told my browser to retrieve the old file from its cached memory.

3. Retrieving Long Documents



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

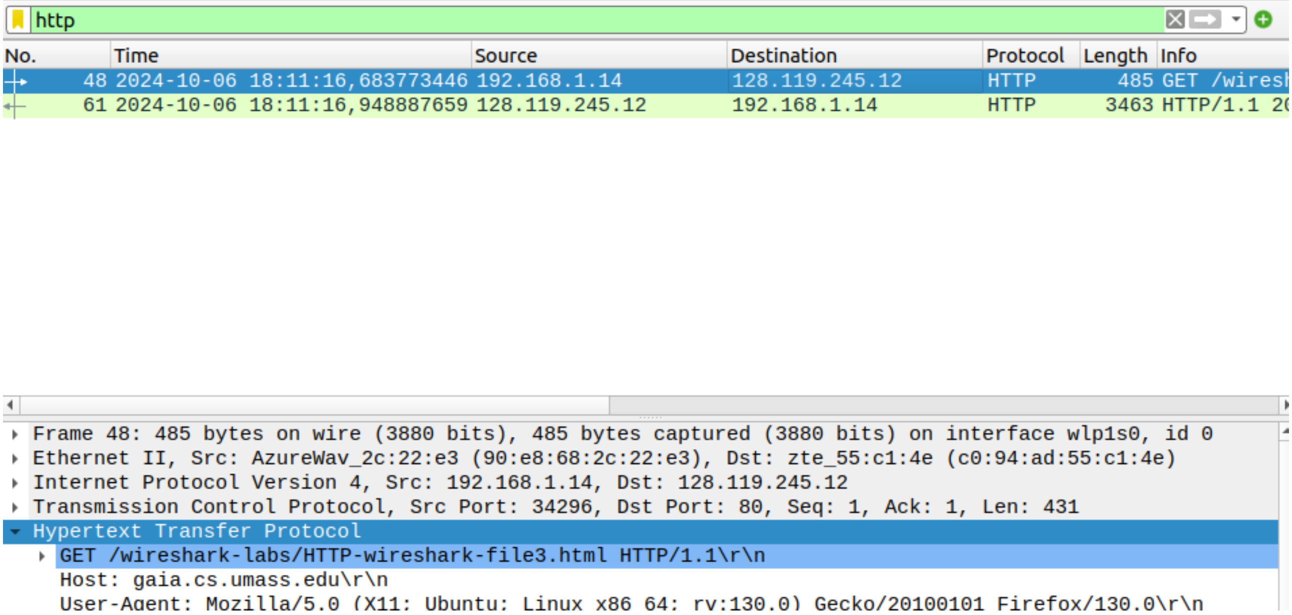
```
No.  Time                           Source          Destination     Protocol Length Info
  48 2024-10-06 18:11:16,683773446 192.168.1.14    128.119.245.12  HTTP      485 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  61 2024-10-06 18:11:16,948887659 128.119.245.12  192.168.1.14    HTTP     3463 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 48: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface wlp1s0, id 0
▸ Ethernet II, Src: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3), Dst: zte_55:c1:4e (c0:94:ad:55:c1:4e)
▸ Internet Protocol Version 4, Src: 192.168.1.14, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 34296, Dst Port: 80, Seq: 1, Ack: 1, Len: 431
▸ Hypertext Transfer Protocol
```

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

* Answer:

- My browser only sent 1 HTTP GET request to the server. The Packet that contained the GET message was packet number 48.



```
http
No.  Time                           Source          Destination      Protocol  Length Info
  48 2024-10-06 18:11:16,683773446 192.168.1.14    128.119.245.12   HTTP         485 GET /wiresh
  61 2024-10-06 18:11:16,948887659 128.119.245.12  192.168.1.14     HTTP        3463 HTTP/1.1 20

› Frame 48: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface wlp1s0, id 0
› Ethernet II, Src: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3), Dst: zte_55:c1:4e (c0:94:ad:55:c1:4e)
› Internet Protocol Version 4, Src: 192.168.1.14, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 34296, Dst Port: 80, Seq: 1, Ack: 1, Len: 431
▾ Hypertext Transfer Protocol
  › GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0\r\n
```

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

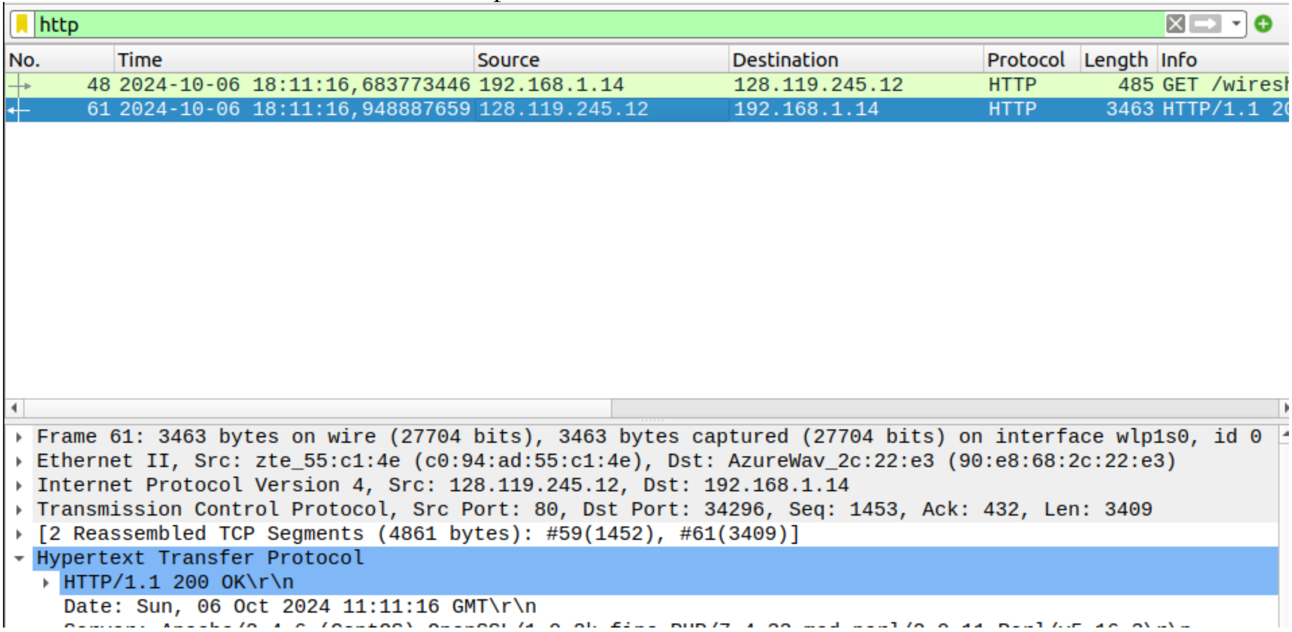
* Answer:

- The packet number is 61 (Please view the capture above)

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

* Answer:

- The status code is 200 and the phrase is OK

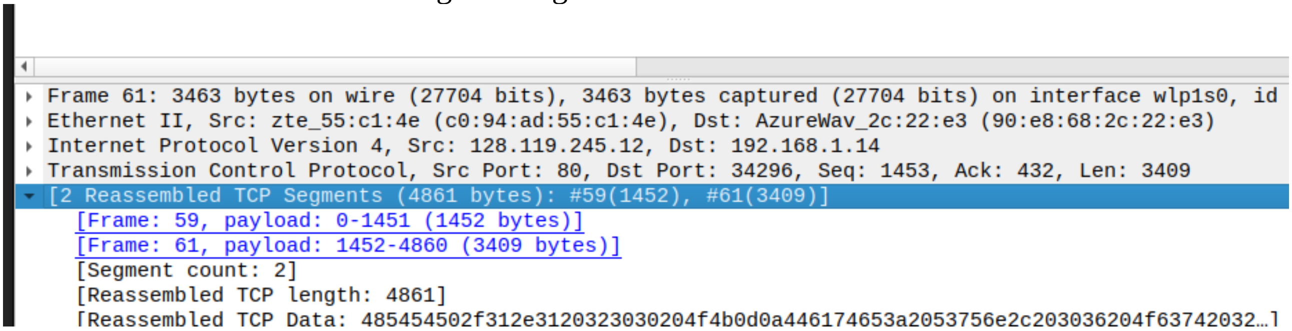


```
http
No.  Time                           Source          Destination      Protocol  Length Info
  48 2024-10-06 18:11:16,683773446 192.168.1.14    128.119.245.12   HTTP         485 GET /wiresh
  61 2024-10-06 18:11:16,948887659 128.119.245.12  192.168.1.14     HTTP        3463 HTTP/1.1 20

› Frame 61: 3463 bytes on wire (27704 bits), 3463 bytes captured (27704 bits) on interface wlp1s0, id 0
› Ethernet II, Src: zte_55:c1:4e (c0:94:ad:55:c1:4e), Dst: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3)
› Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.14
› Transmission Control Protocol, Src Port: 80, Dst Port: 34296, Seq: 1453, Ack: 432, Len: 3409
› [2 Reassembled TCP Segments (4861 bytes): #59(1452), #61(3409)]
▾ Hypertext Transfer Protocol
  › HTTP/1.1 200 OK\r\n
    Date: Sun, 06 Oct 2024 11:11:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
```

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

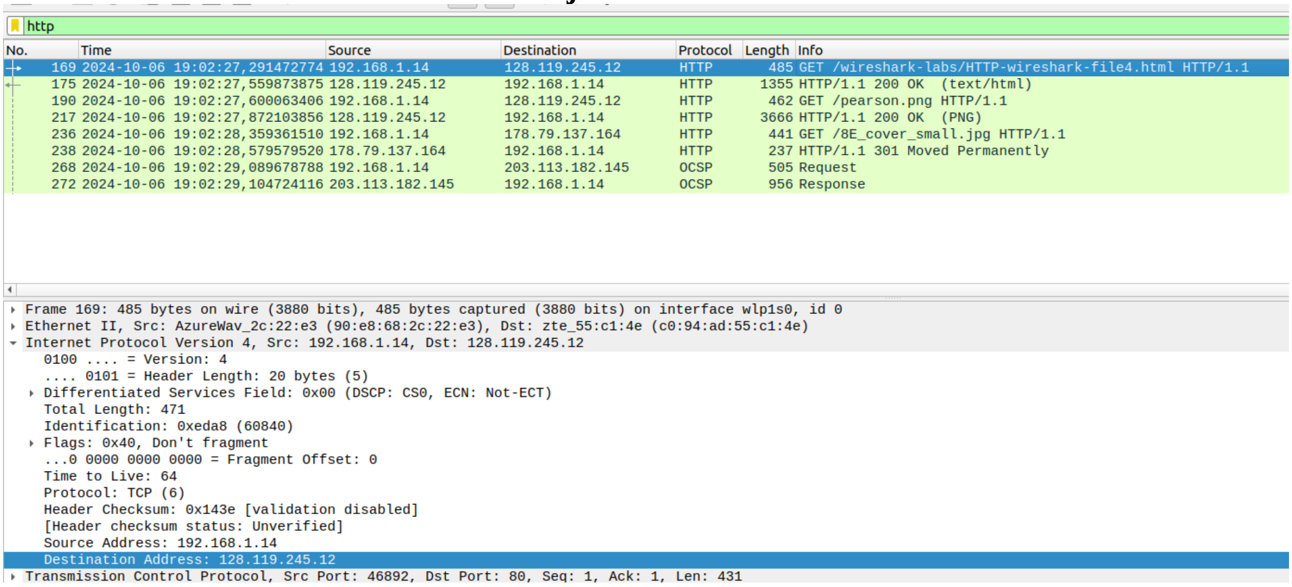
* Answer:

- There are 2 data-containing TCP segments were needed.



```
▸ Frame 61: 3463 bytes on wire (27704 bits), 3463 bytes captured (27704 bits) on interface wlp1s0, id
▸ Ethernet II, Src: zte_55:c1:4e (c0:94:ad:55:c1:4e), Dst: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.14
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 34296, Seq: 1453, Ack: 432, Len: 3409
▾ [2 Reassembled TCP Segments (4861 bytes): #59(1452), #61(3409)]
    [Frame: 59, payload: 0-1451 (1452 bytes)]
    [Frame: 61, payload: 1452-4860 (3409 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203036204f63742032…]
```

4. HTML Documents with Embedded Objects



```
http
```

```
No.   Time                          Source           Destination      Protocol Length Info
  169 2024-10-06 19:02:27,291472774 192.168.1.14     128.119.245.12   HTTP      485 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  175 2024-10-06 19:02:27,559873875 128.119.245.12   192.168.1.14     HTTP     1355 HTTP/1.1 200 OK  (text/html)
  190 2024-10-06 19:02:27,600063406 192.168.1.14     128.119.245.12   HTTP      462 GET /pearson.png HTTP/1.1
  217 2024-10-06 19:02:27,872103856 128.119.245.12   192.168.1.14     HTTP     3666 HTTP/1.1 200 OK  (PNG)
  236 2024-10-06 19:02:28,359361510 192.168.1.14     178.79.137.164   HTTP      441 GET /8E_cover_small.jpg HTTP/1.1
  238 2024-10-06 19:02:28,579579520 178.79.137.164   192.168.1.14     HTTP      237 HTTP/1.1 301 Moved Permanently
  268 2024-10-06 19:02:29,089678788 192.168.1.14     203.113.182.145  OCSP      505 Request
  272 2024-10-06 19:02:29,104724116 203.113.182.145  192.168.1.14     OCSP      956 Response
```

```
▸ Frame 169: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface wlp1s0, id 0
▸ Ethernet II, Src: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3), Dst: zte_55:c1:4e (c0:94:ad:55:c1:4e)
▾ Internet Protocol Version 4, Src: 192.168.1.14, 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: 471
    Identification: 0xeda8 (60840)
  ▸ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x143e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.14
    Destination Address: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 46892, Dst Port: 80, Seq: 1, Ack: 1, Len: 431
```

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

* Answer:

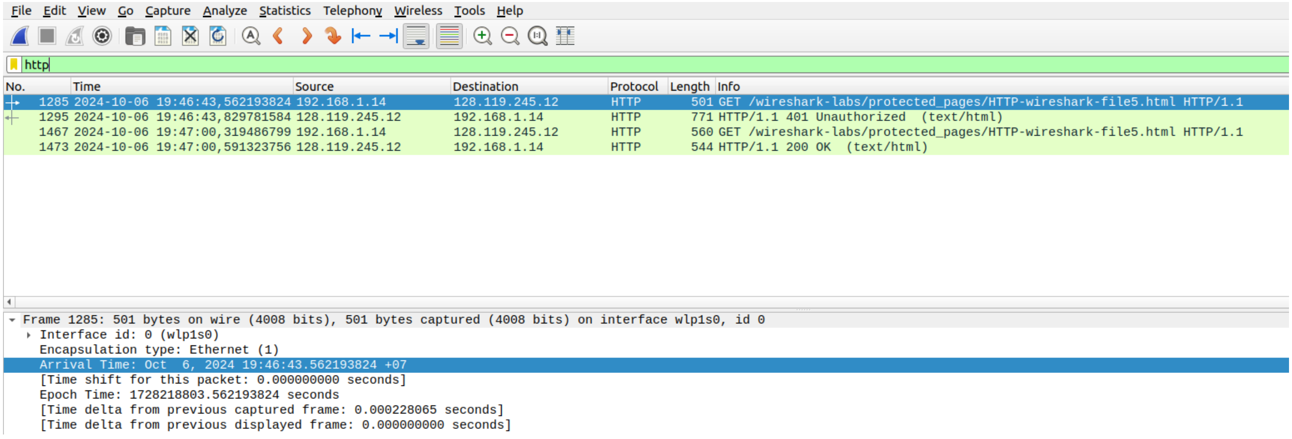
- There are three (3) HTTP GET request messages that my browser sent.
- Packet number 169 sent to address 128.119.245.12
- Packet number 190 sent to address 128.119.245.12
- Packet number 236 sent to address 178.79.137.164

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.

* Answer:

- According to the time field in the packet tracer. The first image “person.png” is requested at Oct 6, 2024 19:02:27.600063406 +07.
- The second image “8E_cover_small.jpg is requested at Oct 6, 2024 19:02:28.359361510 +07.
- Timestamps of their response also different and the first image are get before the second. Therefore my browser download the two images serially.

5 HTTP Authentication


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

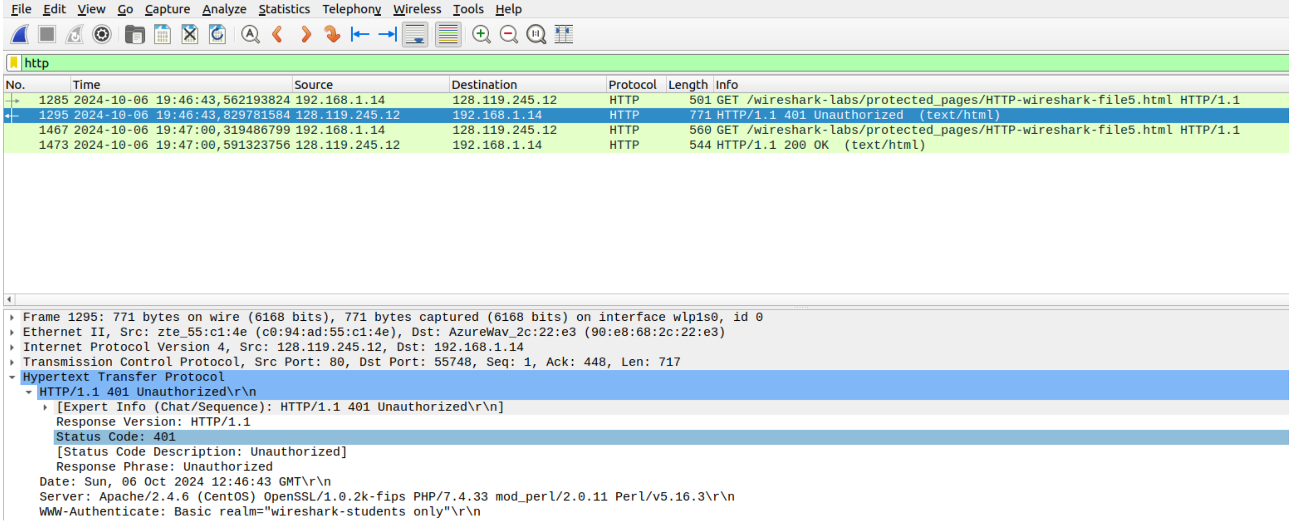
```
http
No.  Time                          Source          Destination     Protocol Length Info
1285 2024-10-06 19:46:43,562193824 192.168.1.14    128.119.245.12  HTTP     501 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1295 2024-10-06 19:46:43,829781584 128.119.245.12  192.168.1.14    HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
1467 2024-10-06 19:47:00,319486799 192.168.1.14    128.119.245.12  HTTP     560 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1473 2024-10-06 19:47:00,591323756 128.119.245.12  192.168.1.14    HTTP     544 HTTP/1.1 200 OK  (text/html)
```

```
Frame 1285: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface wlp1s0, id 0
  Interface id: 0 (wlp1s0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct  6, 2024 19:46:43.562193824 +07
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1728218803.562193824 seconds
  [Time delta from previous captured frame: 0.000228065 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
```

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.
- The Response Phrase is Unauthorized.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

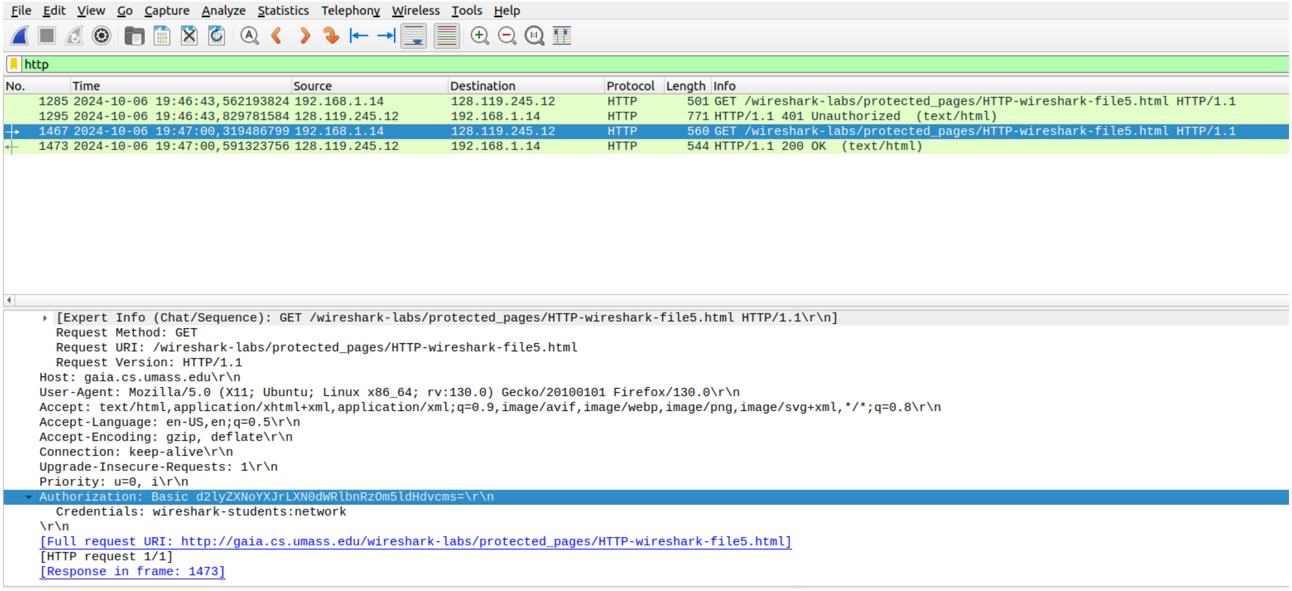
```
http
No.  Time                          Source          Destination     Protocol Length Info
1285 2024-10-06 19:46:43,562193824 192.168.1.14    128.119.245.12  HTTP     501 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1295 2024-10-06 19:46:43,829781584 128.119.245.12  192.168.1.14    HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
1467 2024-10-06 19:47:00,319486799 192.168.1.14    128.119.245.12  HTTP     560 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1473 2024-10-06 19:47:00,591323756 128.119.245.12  192.168.1.14    HTTP     544 HTTP/1.1 200 OK  (text/html)
```

```
Frame 1295: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface wlp1s0, id 0
Ethernet II, Src: zte_55:c1:4e (c0:94:ad:55:c1:4e), Dst: AzureWav_2c:22:e3 (90:e8:68:2c:22:e3)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.14
Transmission Control Protocol, Src Port: 80, Dst Port: 55748, Seq: 1, Ack: 448, Len: 717
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: Sun, 06 Oct 2024 12:46:43 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  WWW-Authenticate: Basic realm="wireshark-students only"\r\n
```

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

* Answer:

- Field "Authorization" is included in the second HTTP GET messages. This is included because we sent the server a username and password along with our request stating that we were authorized to receive the page.



http

```
No.   Time                          Source          Destination     Protocol Length Info
 1285 2024-10-06 19:46:43,562193824 192.168.1.14    128.119.245.12  HTTP       501 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 1295 2024-10-06 19:46:43,829781584 128.119.245.12  192.168.1.14    HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
 1467 2024-10-06 19:47:00,319486799 192.168.1.14    128.119.245.12  HTTP       560 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 1473 2024-10-06 19:47:00,591323756 128.119.245.12  192.168.1.14    HTTP       544 HTTP/1.1 200 OK  (text/html)
```

```
  [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
  Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Priority: u=0, i\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  Credentials: wireshark-students:network
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 1473]
```