Lab 1: Wireshark & Application Layer Protocols

(Based on Wireshark Labs from Kurose and Ross 6th Edition)

NAME: Caleb Woods

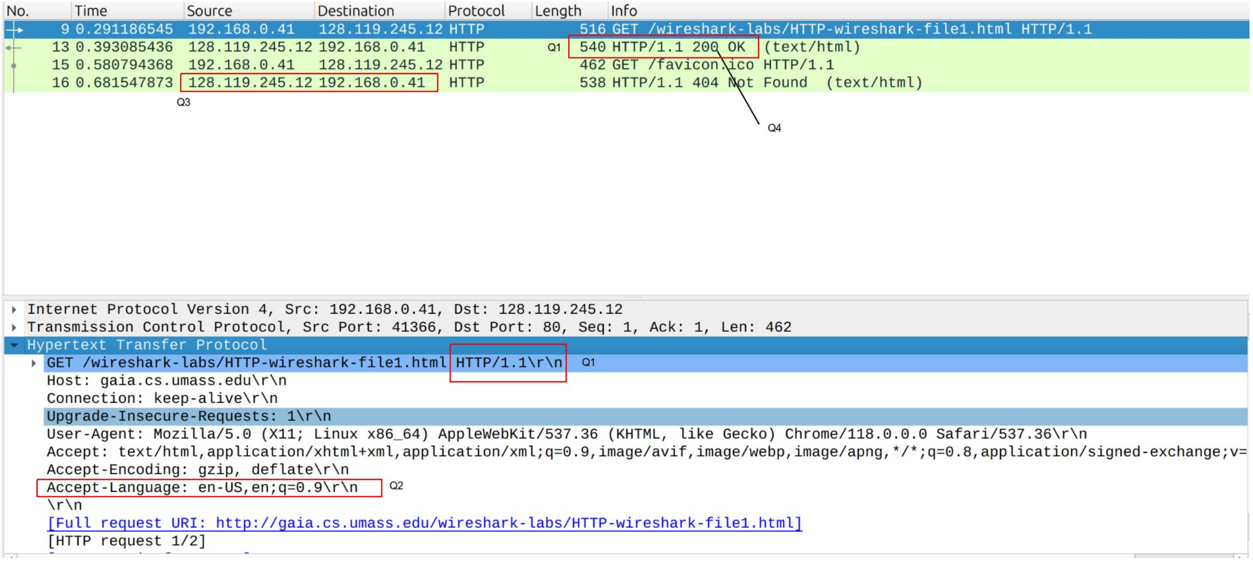
PART 1: HTTP (18 Points – 1 point per question)

1. The Basic HTTP GET/response interaction

By looking at the information in the HTTP GET and response messages, answer the following questions. You can paste the annotated screenshots directly in response to the questions.

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running? Local host HTTP 1.1, Server HTTP 1.1.
2. What languages (if any) does your browser indicate that it can accept to the server? En (English)
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server? Local Host IP address: 192.168.0.41, Server IP address: 128.119.245.12
4. What is the status code returned from the server to your browser? Status Code 200, Description: OK.
5. When was the HTML file that you are retrieving last modified at the server? Fri, 27 Oct 2023 05:59:02 GMT.
6. How many bytes of content are being returned to your browser?
For the HTTP file data return from Server the local host receives 128 Bytes as shown by the File Data header and value.

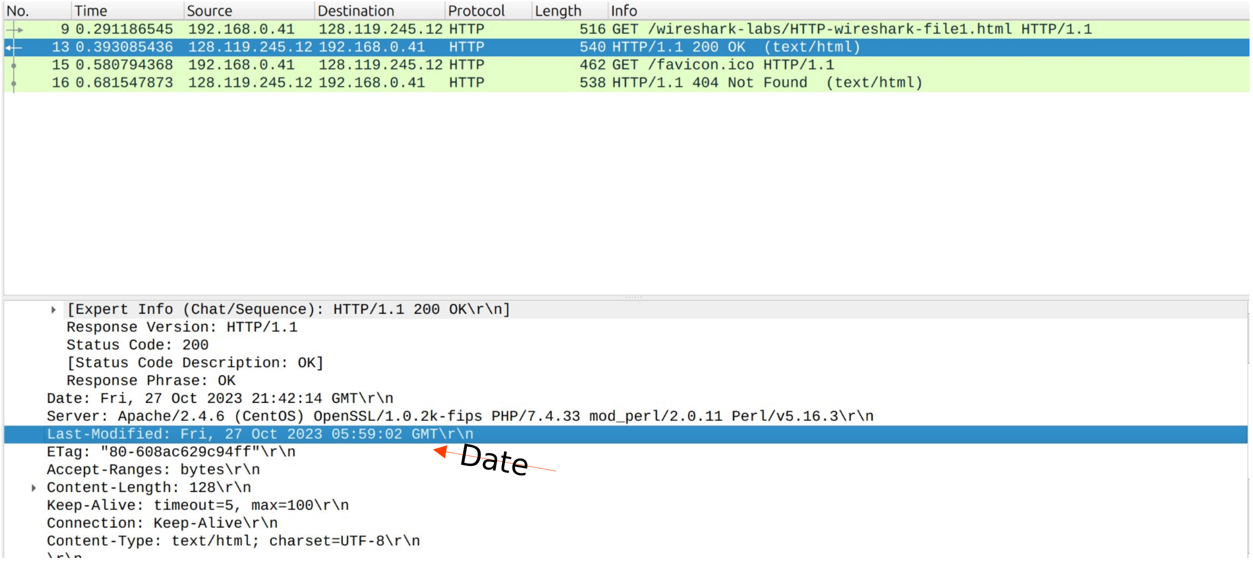
Screen shots
Q 1→4



```
No.  Time           Source          Destination     Protocol  Length  Info
   9 0.291186545    192.168.0.41    128.119.245.12  HTTP         516  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  13 0.393085436    128.119.245.12  192.168.0.41    HTTP         540  HTTP/1.1 200 OK  (text/html)
  15 0.580794368    192.168.0.41    128.119.245.12  HTTP         462  GET /favicon.ico HTTP/1.1
  16 0.681547873    128.119.245.12  192.168.0.41    HTTP         538  HTTP/1.1 404 Not Found  (text/html)
```

```
Internet Protocol Version 4, Src: 192.168.0.41, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 41366, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
  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 1/2]
```

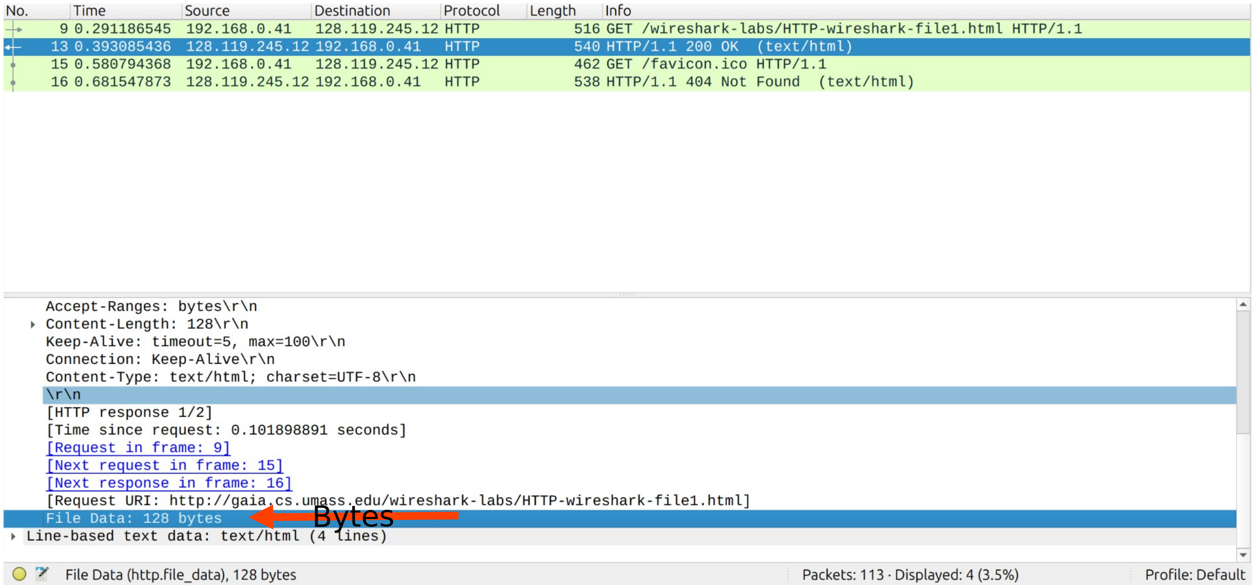
Q5



```
No.  Time         Source          Destination     Protocol  Length  Info
   9 0.291186545  192.168.0.41    128.119.245.12  HTTP         516  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  13 0.393085436  128.119.245.12  192.168.0.41    HTTP         540  HTTP/1.1 200 OK  (text/html)
  15 0.580794368  192.168.0.41    128.119.245.12  HTTP         462  GET /favicon.ico HTTP/1.1
  16 0.681547873  128.119.245.12  192.168.0.41    HTTP         538  HTTP/1.1 404 Not Found  (text/html)
```

```
    [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: Fri, 27 Oct 2023 21:42:14 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: Fri, 27 Oct 2023 05:59:02 GMT\r\n
  ETag: "80-608ac629c94ff"\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
```

Q6



```
No.  Time         Source          Destination     Protocol  Length  Info
   9 0.291186545  192.168.0.41    128.119.245.12  HTTP         516  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  13 0.393085436  128.119.245.12  192.168.0.41    HTTP         540  HTTP/1.1 200 OK  (text/html)
  15 0.580794368  192.168.0.41    128.119.245.12  HTTP         462  GET /favicon.ico HTTP/1.1
  16 0.681547873  128.119.245.12  192.168.0.41    HTTP         538  HTTP/1.1 404 Not Found  (text/html)
```

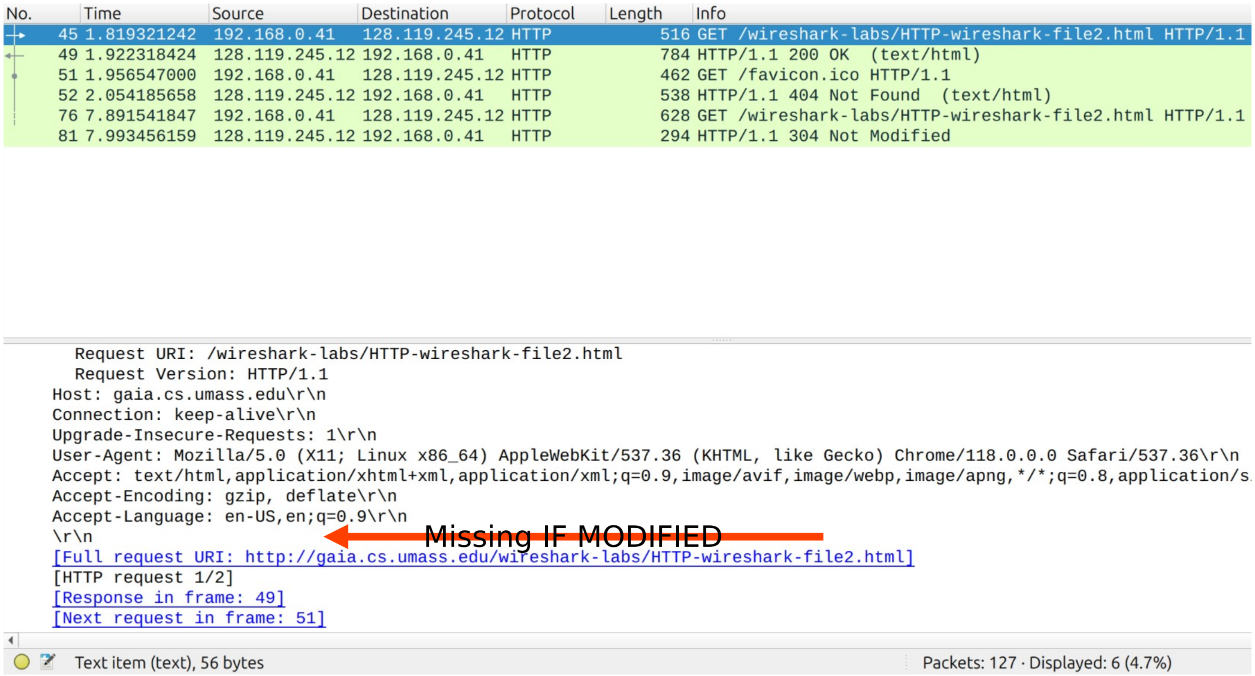
```
  Accept-Ranges: bytes\r\n
  Content-Length: 128\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.101898891 seconds]
  [Request in frame: 9]
  [Next request in frame: 15]
  [Next response in frame: 16]
  [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)
```

Bytes
File Data (http.file_data), 128 bytes
Packets: 113 · Displayed: 4 (3.5%)
Profile: Default

2. The HTTP CONDITIONAL GET/response interaction

Answer the following questions (and provide appropriate annotated screen-shots):

7. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET? No this does not appear in the first Get.



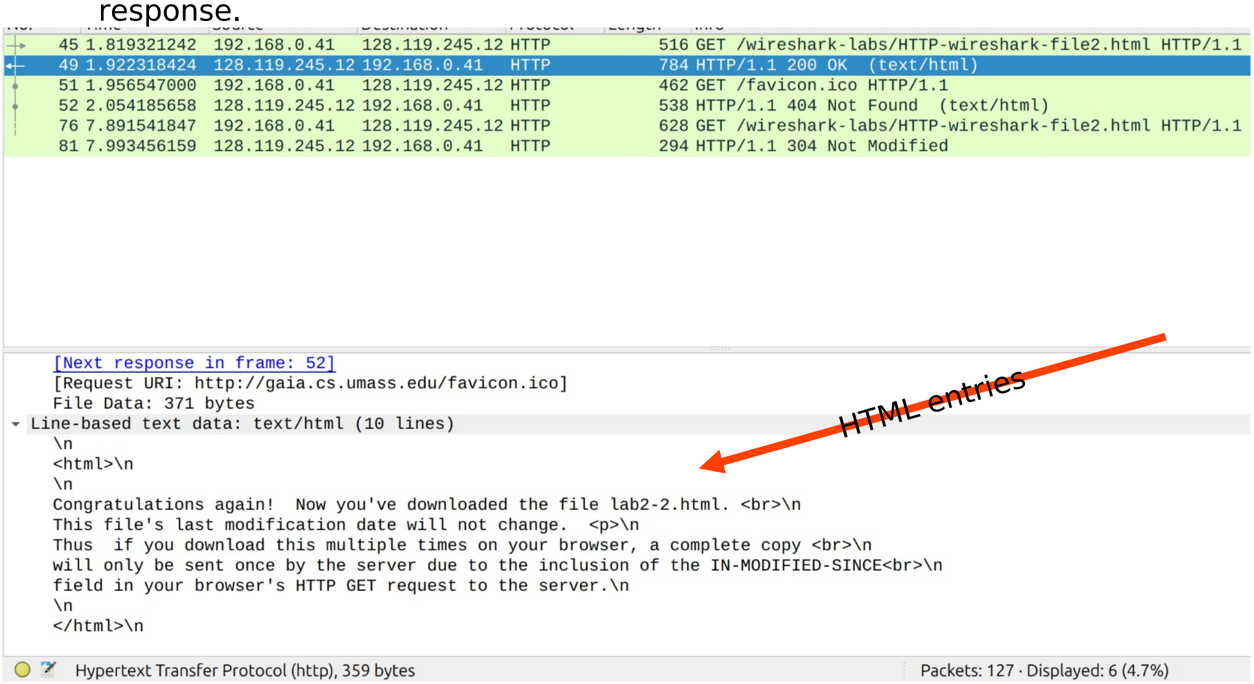
```
No.   Time          Source          Destination     Protocol  Length  Info
   45 1.819321242   192.168.0.41    128.119.245.12  HTTP       516 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   49 1.922318424   128.119.245.12  192.168.0.41    HTTP       784 HTTP/1.1 200 OK  (text/html)
   51 1.956547000   192.168.0.41    128.119.245.12  HTTP       462 GET /favicon.ico HTTP/1.1
   52 2.054185658   128.119.245.12  192.168.0.41    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
   76 7.891541847   192.168.0.41    128.119.245.12  HTTP       628 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   81 7.993456159   128.119.245.12  192.168.0.41    HTTP       294 HTTP/1.1 304 Not Modified
```

```
      Request URI: /wireshark-labs/HTTP-wireshark-file2.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/118.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
    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 1/2]
    [Response in frame: 49]
    [Next request in frame: 51]
```

Missing IF MODIFIED

```
Text item (text), 56 bytes                                    Packets: 127 · Displayed: 6 (4.7%)
```

8. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? Yes because I see the entries showing text or data we would expect from the web site page in the response.



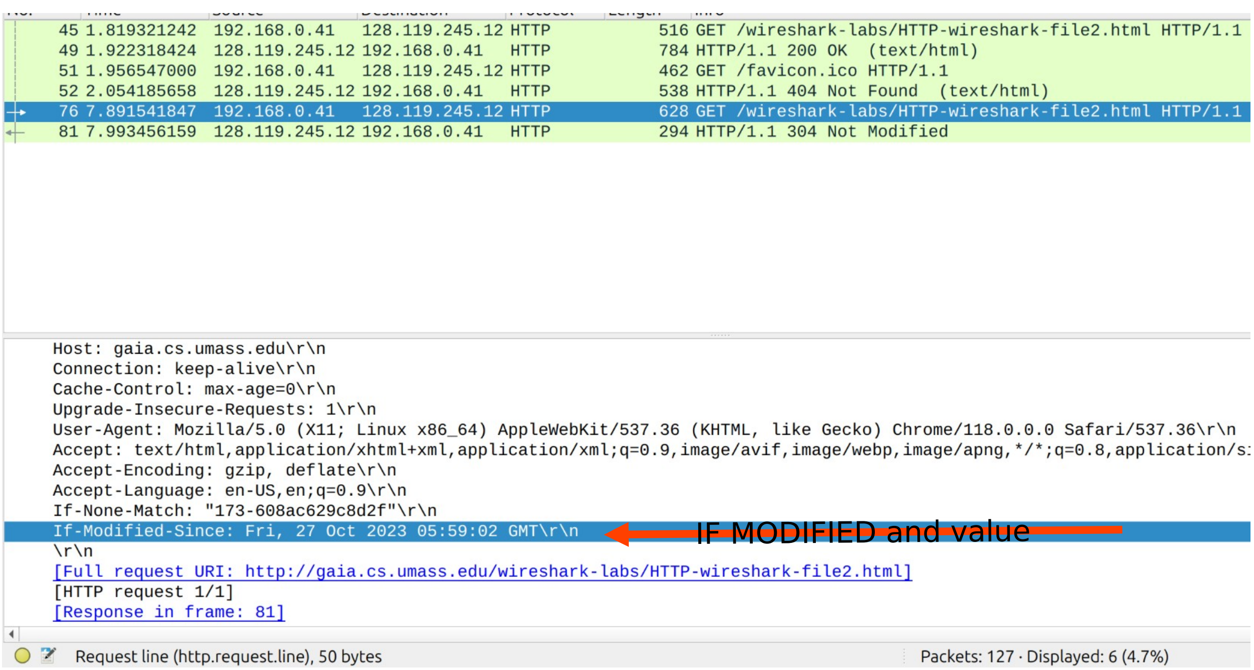
```
   45 1.819321242   192.168.0.41    128.119.245.12  HTTP       516 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   49 1.922318424   128.119.245.12  192.168.0.41    HTTP       784 HTTP/1.1 200 OK  (text/html)
   51 1.956547000   192.168.0.41    128.119.245.12  HTTP       462 GET /favicon.ico HTTP/1.1
   52 2.054185658   128.119.245.12  192.168.0.41    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
   76 7.891541847   192.168.0.41    128.119.245.12  HTTP       628 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   81 7.993456159   128.119.245.12  192.168.0.41    HTTP       294 HTTP/1.1 304 Not Modified
```

```
    [Next response in frame: 52]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    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
```

HTML entries

```
Hypertext Transfer Protocol (http), 359 bytes                 Packets: 127 · Displayed: 6 (4.7%)
```

9. 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? Yes “IF-MODIFIED-SINCE:” does exist in the second GET. It shows: If-Modified-Since: Fri, 27 Oct 2023 05:59:02 GMT.



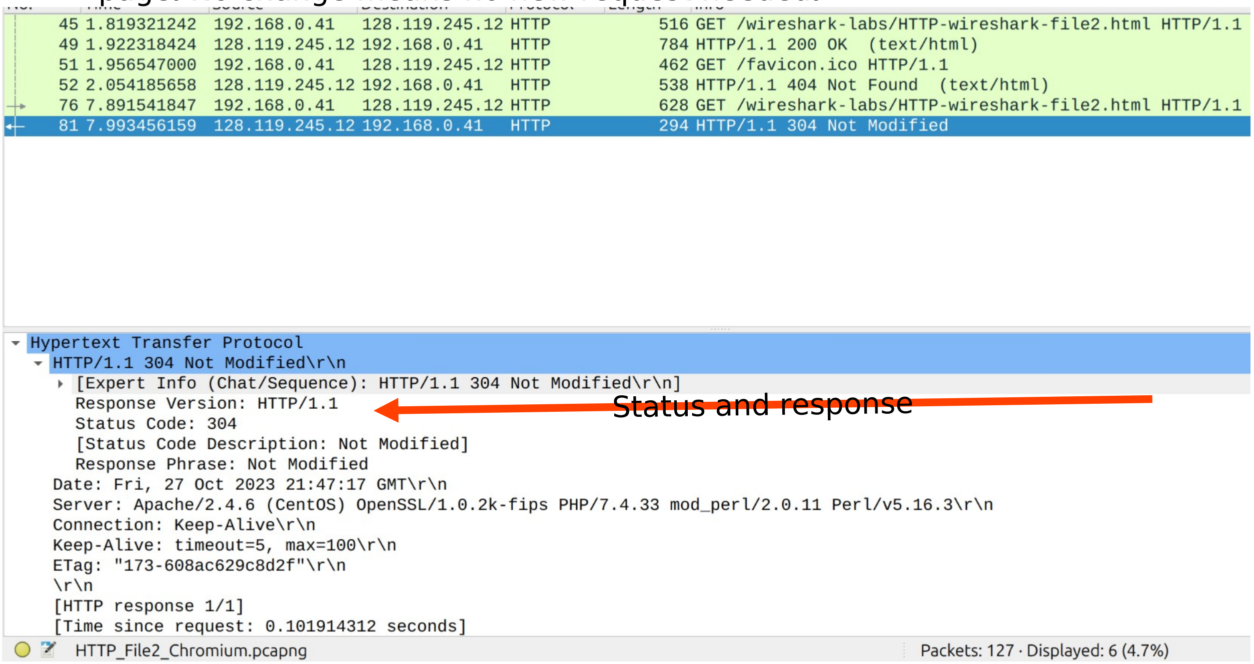
```
 45 1.819321242  192.168.0.41    128.119.245.12 HTTP    516 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 49 1.922318424  128.119.245.12 192.168.0.41    HTTP    784 HTTP/1.1 200 OK  (text/html)
 51 1.956547000  192.168.0.41    128.119.245.12 HTTP    462 GET /favicon.ico HTTP/1.1
 52 2.054185658  128.119.245.12 192.168.0.41    HTTP    538 HTTP/1.1 404 Not Found  (text/html)
 76 7.891541847  192.168.0.41    128.119.245.12 HTTP    628 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 81 7.993456159  128.119.245.12 192.168.0.41    HTTP    294 HTTP/1.1 304 Not Modified
```

```
    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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-608ac629c8d2f"\r\n
    If-Modified-Since: Fri, 27 Oct 2023 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 81]
```

IF MODIFIED and value

Request line (http.request.line), 50 bytes
Packets: 127 · Displayed: 6 (4.7%)

10. 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. The Status code value is 304, Not Modified. No it checked the cache and noticed that no change was made to the server side page. No change means no new request needed.



```
 45 1.819321242  192.168.0.41    128.119.245.12 HTTP    516 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 49 1.922318424  128.119.245.12 192.168.0.41    HTTP    784 HTTP/1.1 200 OK  (text/html)
 51 1.956547000  192.168.0.41    128.119.245.12 HTTP    462 GET /favicon.ico HTTP/1.1
 52 2.054185658  128.119.245.12 192.168.0.41    HTTP    538 HTTP/1.1 404 Not Found  (text/html)
 76 7.891541847  192.168.0.41    128.119.245.12 HTTP    628 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 81 7.993456159  128.119.245.12 192.168.0.41    HTTP    294 HTTP/1.1 304 Not Modified
```

```
▾ 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: Fri, 27 Oct 2023 21:47:17 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-608ac629c8d2f"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.101914312 seconds]
```

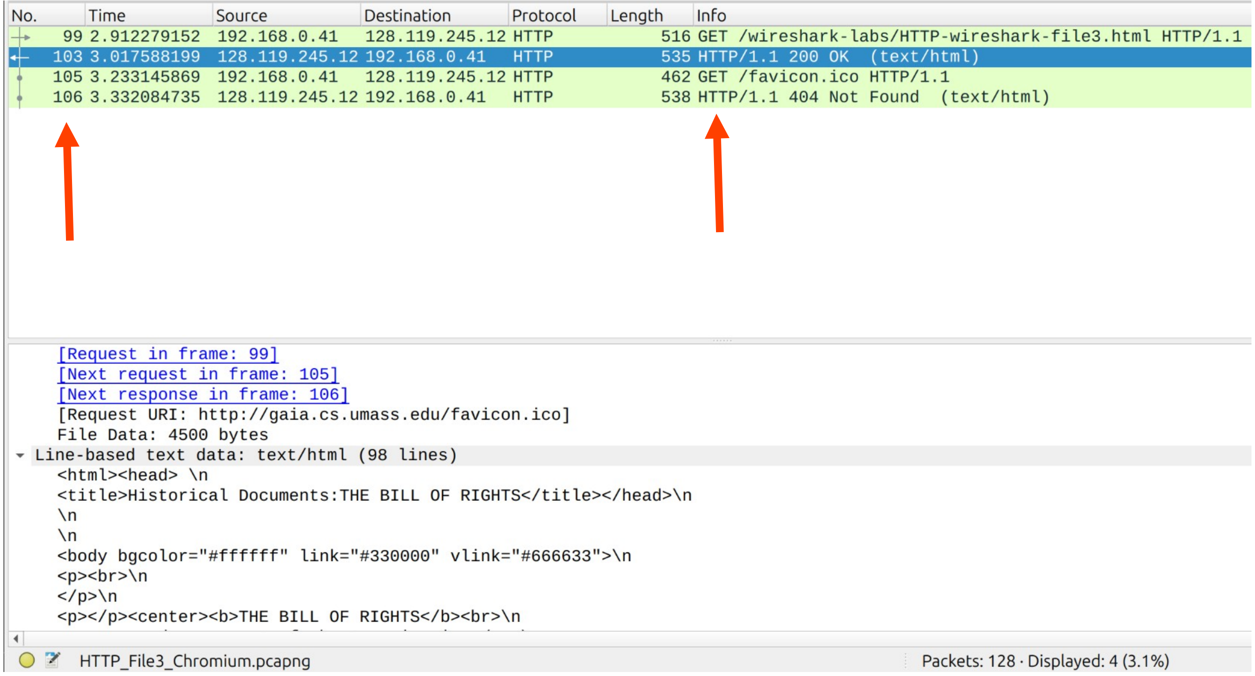
Status and response

HTTP_File2_Chromium.pcapng
Packets: 127 · Displayed: 6 (4.7%)

3. Retrieving Long Documents

Answer the following questions (and provide appropriate annotated screen shots):

11. How many HTTP GET request messages did your browser send? My Browser sent two GET requests. Which packet number in the trace contains the GET message for the Bill or Rights? Packet number 103 contains the Bill of Rights being sent to the local host.

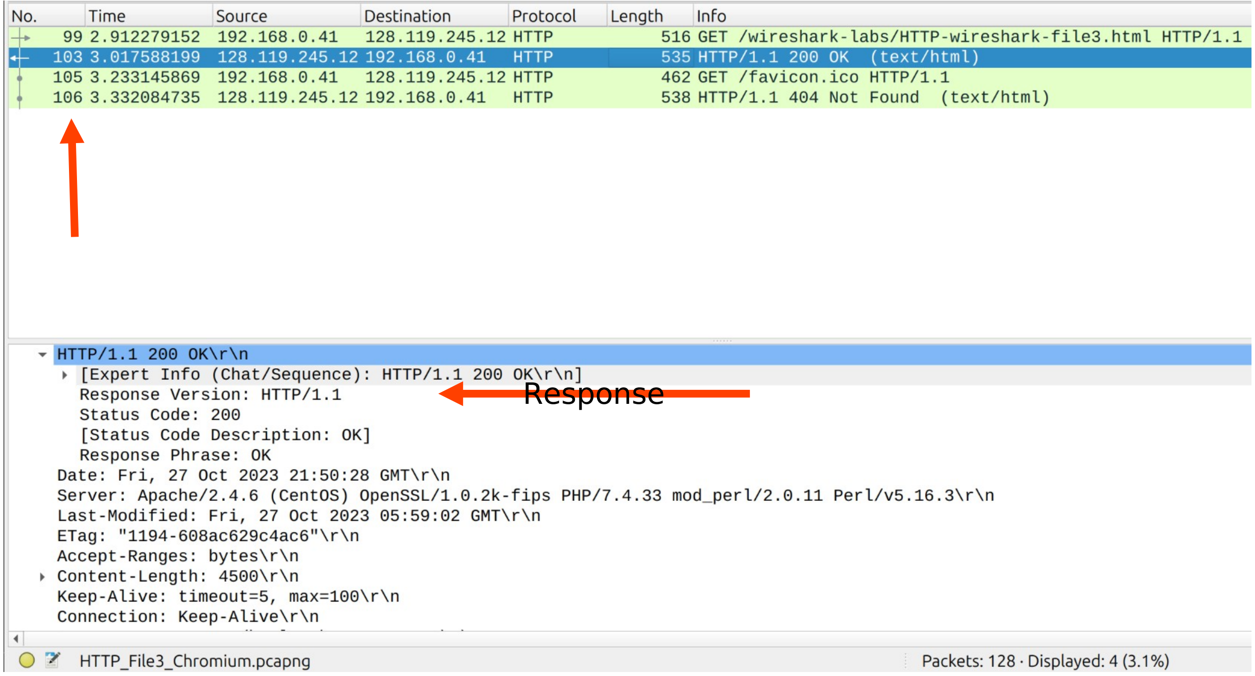


```
No.    Time         Source          Destination     Protocol  Length  Info
   99 2.912279152  192.168.0.41    128.119.245.12  HTTP         516  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  103 3.017588199  128.119.245.12  192.168.0.41    HTTP         535  HTTP/1.1 200 OK  (text/html)
  105 3.233145869  192.168.0.41    128.119.245.12  HTTP         462  GET /favicon.ico HTTP/1.1
  106 3.332084735  128.119.245.12  192.168.0.41    HTTP         538  HTTP/1.1 404 Not Found  (text/html)
```

```
    [Request in frame: 99]
    [Next request in frame: 105]
    [Next response in frame: 106]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 4500 bytes
▾ Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
```

HTTP_File3_Chromium.pcapng   Packets: 128 · Displayed: 4 (3.1%)

12. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? Again packet number 103 is the response to the Bill of Rights request. This response gives a status 200 with description OK.

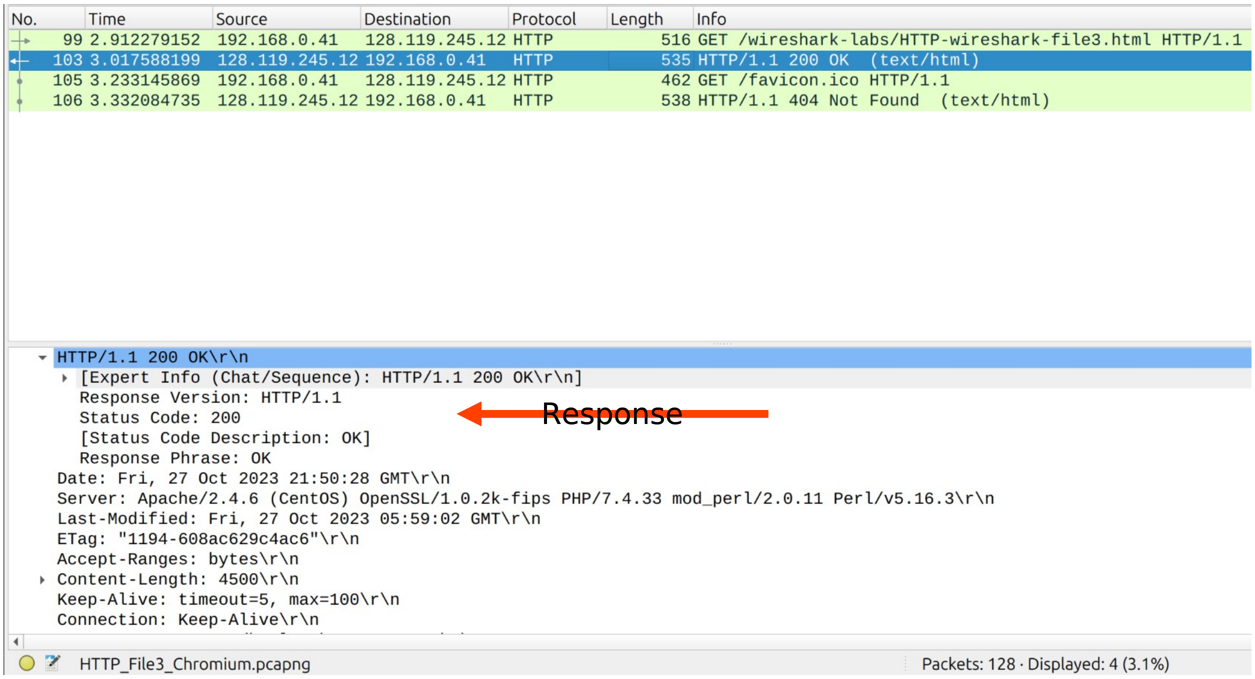


```
No.    Time         Source          Destination     Protocol  Length  Info
   99 2.912279152  192.168.0.41    128.119.245.12  HTTP         516  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  103 3.017588199  128.119.245.12  192.168.0.41    HTTP         535  HTTP/1.1 200 OK  (text/html)
  105 3.233145869  192.168.0.41    128.119.245.12  HTTP         462  GET /favicon.ico HTTP/1.1
  106 3.332084735  128.119.245.12  192.168.0.41    HTTP         538  HTTP/1.1 404 Not Found  (text/html)
```

```
  ▾ 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: Fri, 27 Oct 2023 21:50:28 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: Fri, 27 Oct 2023 05:59:02 GMT\r\n
    ETag: "1194-608ac629c4ac6"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
```

HTTP_File3_Chromium.pcapng   Packets: 128 · Displayed: 4 (3.1%)

13. What is the status code and phrase in the response? This response gives a status 200 with description OK.

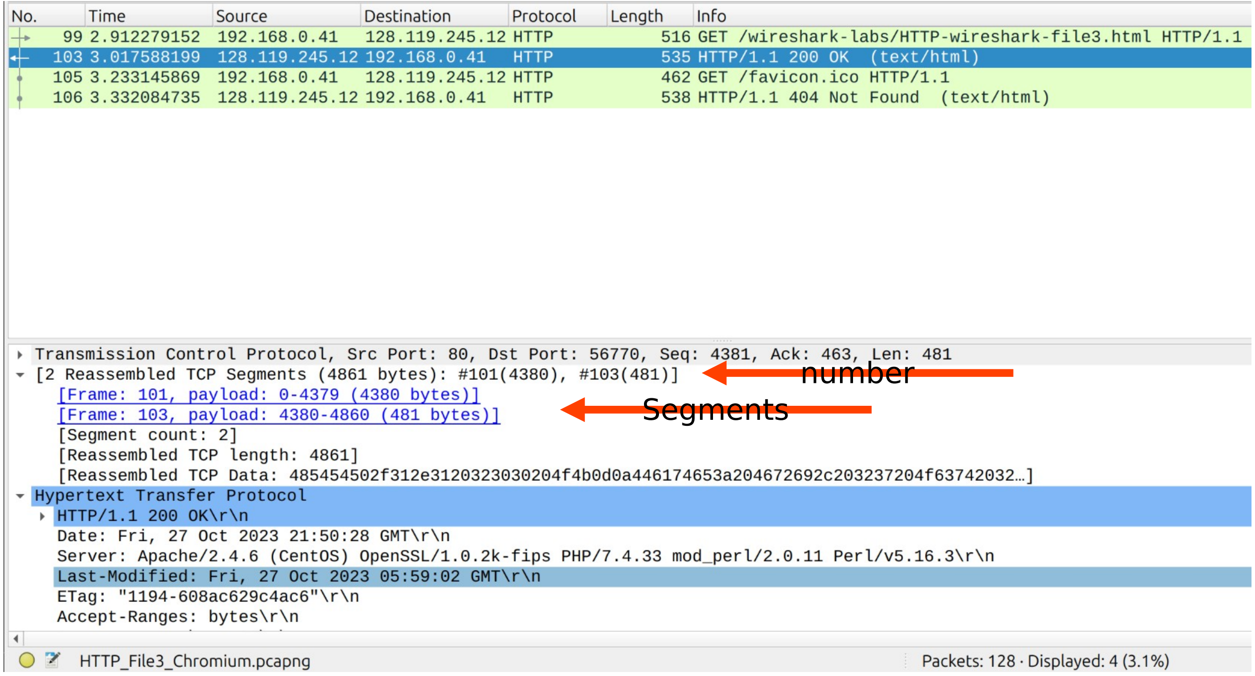


No.	Time	Source	Destination	Protocol	Length	Info
99	2.912279152	192.168.0.41	128.119.245.12	HTTP	516	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
103	3.017588199	128.119.245.12	192.168.0.41	HTTP	535	HTTP/1.1 200 OK (text/html)
105	3.233145869	192.168.0.41	128.119.245.12	HTTP	462	GET /favicon.ico HTTP/1.1
106	3.332084735	128.119.245.12	192.168.0.41	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
▾ 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: Fri, 27 Oct 2023 21:50:28 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: Fri, 27 Oct 2023 05:59:02 GMT\r\n
  ETag: "1194-608ac629c4ac6"\r\n
  Accept-Ranges: bytes\r\n
▸ Content-Length: 4500\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
```

Response
HTTP_File3_Chromium.pcapng
Packets: 128 · Displayed: 4 (3.1%)

14. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? It would seem that two TCP segments were transferred (in parallel?). One payload contained 4380 bytes and the second contained 481 bytes. Why would it split so unevenly if parallel processing? Maybe 4380 bytes is the segment data threshold.



No.	Time	Source	Destination	Protocol	Length	Info
99	2.912279152	192.168.0.41	128.119.245.12	HTTP	516	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
103	3.017588199	128.119.245.12	192.168.0.41	HTTP	535	HTTP/1.1 200 OK (text/html)
105	3.233145869	192.168.0.41	128.119.245.12	HTTP	462	GET /favicon.ico HTTP/1.1
106	3.332084735	128.119.245.12	192.168.0.41	HTTP	538	HTTP/1.1 404 Not Found (text/html)

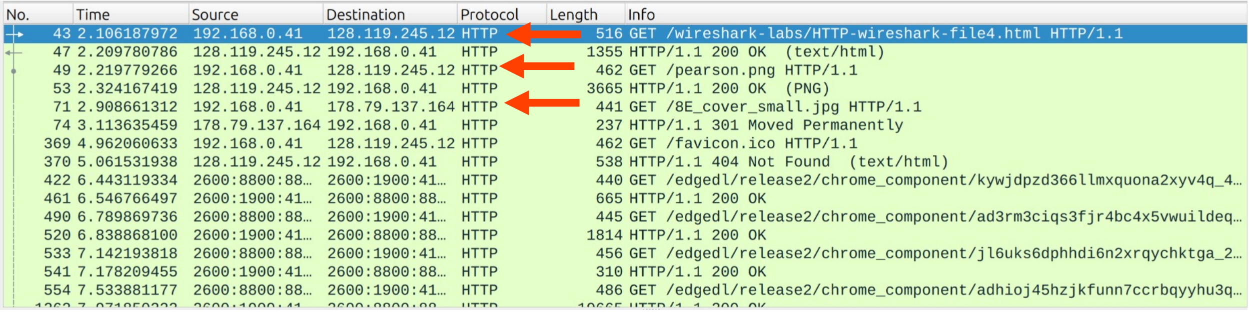
```
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 56770, Seq: 4381, Ack: 463, Len: 481
▾ [2 Reassembled TCP Segments (4861 bytes): #101(4380), #103(481)]
    [Frame: 101, payload: 0-4379 (4380 bytes)]
    [Frame: 103, payload: 4380-4860 (481 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203237204f63742032…]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Fri, 27 Oct 2023 21:50:28 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: Fri, 27 Oct 2023 05:59:02 GMT\r\n
    ETag: "1194-608ac629c4ac6"\r\n
    Accept-Ranges: bytes\r\n
```

number
Segments
HTTP_File3_Chromium.pcapng
Packets: 128 · Displayed: 4 (3.1%)

4. HTML Documents with Embedded Objects

Answer the following questions (and provide appropriate annotated screen shots)::

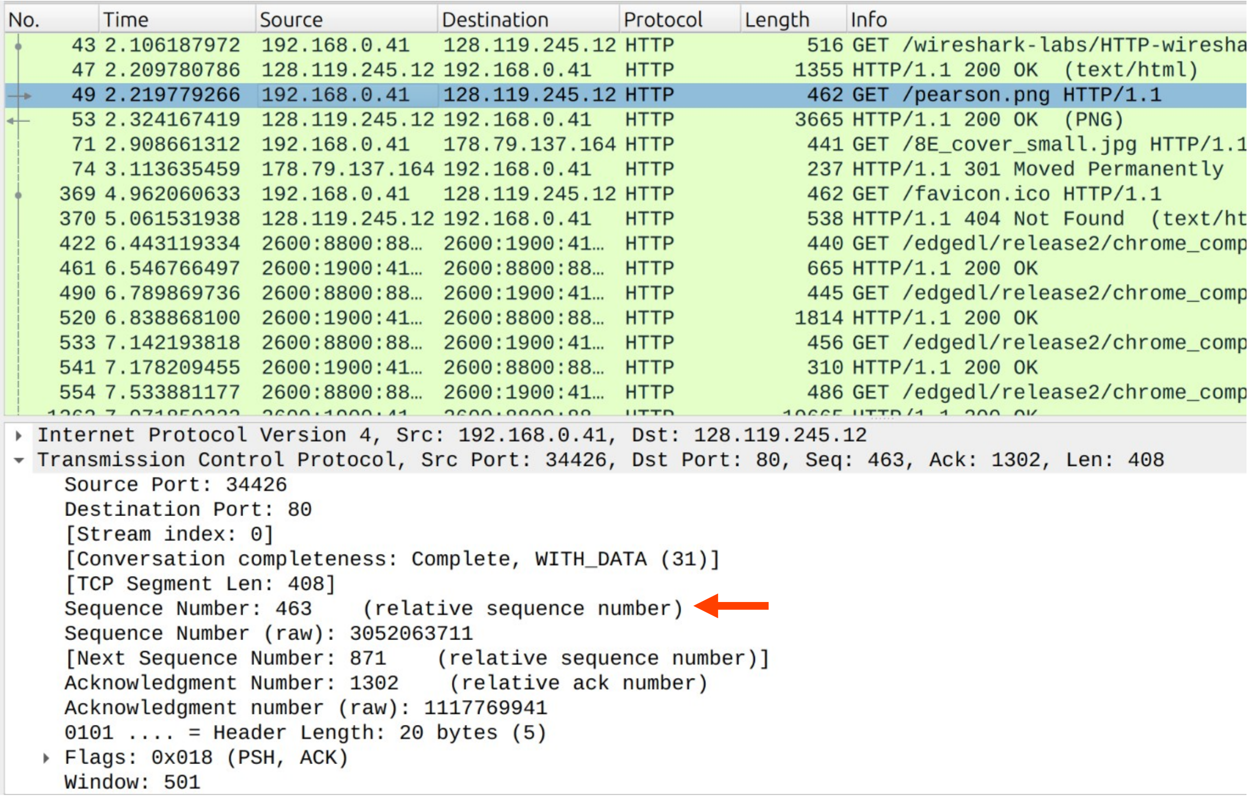
15. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent? I had many GET requests but only 5 Distinct GET requests with 3 being appropriate with this question. The destination IP addresses are for the 128.119.245.12 HTML form, 128.119.245.12 for the first .png, and 178.79.137.164 for the second .png. The rest are out of scope I believe.



```
No.  Time        Source          Destination     Protocol Length Info
 43 2.106187972 192.168.0.41    128.119.245.12 HTTP      516 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 47 2.209780786 128.119.245.12 192.168.0.41    HTTP     1355 HTTP/1.1 200 OK  (text/html)
 49 2.219779266 192.168.0.41    128.119.245.12 HTTP      462 GET /pearson.png HTTP/1.1
 53 2.324167419 128.119.245.12 192.168.0.41    HTTP     3665 HTTP/1.1 200 OK  (PNG)
 71 2.908661312 192.168.0.41    178.79.137.164 HTTP      441 GET /8E_cover_small.jpg HTTP/1.1
 74 3.113635459 178.79.137.164 192.168.0.41    HTTP      237 HTTP/1.1 301 Moved Permanently
369 4.962060633 192.168.0.41    128.119.245.12 HTTP      462 GET /favicon.ico HTTP/1.1
370 5.061531938 128.119.245.12 192.168.0.41    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
422 6.443119334 2600:8800:88… 2600:1900:41…   HTTP      440 GET /edgedl/release2/chrome_component/kywjdpzd366llmxquona2xyv4q_4…
461 6.546766497 2600:1900:41… 2600:8800:88…   HTTP      665 HTTP/1.1 200 OK
490 6.789869736 2600:8800:88… 2600:1900:41…   HTTP      445 GET /edgedl/release2/chrome_component/ad3rm3ciqs3fjr4bc4x5vwuildeq…
520 6.838868100 2600:1900:41… 2600:8800:88…   HTTP     1814 HTTP/1.1 200 OK
533 7.142193818 2600:8800:88… 2600:1900:41…   HTTP      456 GET /edgedl/release2/chrome_component/jl6uks6dphhdi6n2xrqychktga_2…
541 7.178209455 2600:1900:41… 2600:8800:88…   HTTP      310 HTTP/1.1 200 OK
554 7.533881177 2600:8800:88… 2600:1900:41…   HTTP      486 GET /edgedl/release2/chrome_component/adhioj45hzjkfunn7ccrbqyyhu3q…
```

16. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain. I think the browser made the request in a linear non parallel fashion. I say this because the Date header field shows 1 second difference in the return time. They are also in different packet numbers and the TCP sequence number is different.

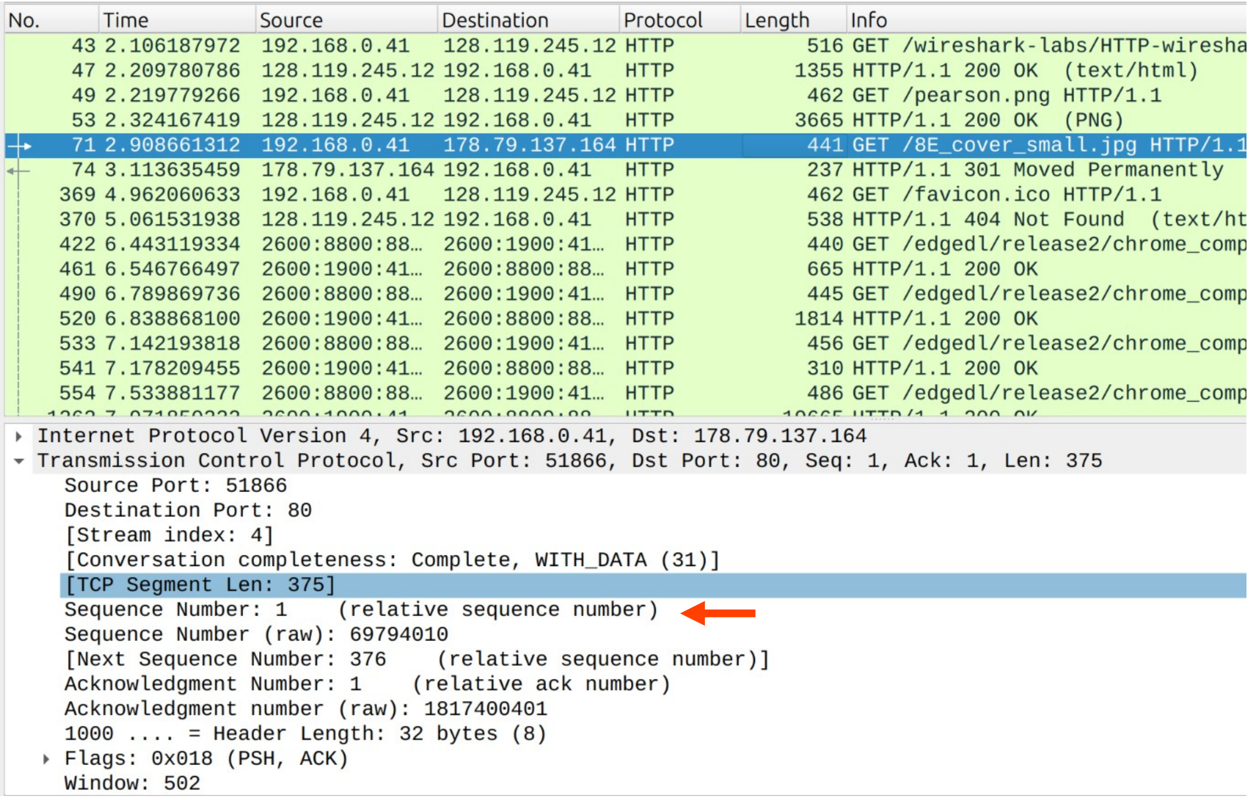
TCP for .png 1



```
No.  Time        Source          Destination     Protocol  Length Info
 43 2.106187972 192.168.0.41    128.119.245.12 HTTP         516 GET /wireshark-labs/HTTP-wiresha
 47 2.209780786 128.119.245.12 192.168.0.41    HTTP        1355 HTTP/1.1 200 OK  (text/html)
 49 2.219779266 192.168.0.41    128.119.245.12 HTTP         462 GET /pearson.png HTTP/1.1
 53 2.324167419 128.119.245.12 192.168.0.41    HTTP        3665 HTTP/1.1 200 OK  (PNG)
 71 2.908661312 192.168.0.41    178.79.137.164 HTTP         441 GET /8E_cover_small.jpg HTTP/1.1
 74 3.113635459 178.79.137.164 192.168.0.41    HTTP         237 HTTP/1.1 301 Moved Permanently
369 4.962060633 192.168.0.41    128.119.245.12 HTTP         462 GET /favicon.ico HTTP/1.1
370 5.061531938 128.119.245.12 192.168.0.41    HTTP         538 HTTP/1.1 404 Not Found  (text/ht
422 6.443119334 2600:8800:88…  2600:1900:41…   HTTP         440 GET /edgedl/release2/chrome_comp
461 6.546766497 2600:1900:41…  2600:8800:88…   HTTP         665 HTTP/1.1 200 OK
490 6.789869736 2600:8800:88…  2600:1900:41…   HTTP         445 GET /edgedl/release2/chrome_comp
520 6.838868100 2600:1900:41…  2600:8800:88…   HTTP        1814 HTTP/1.1 200 OK
533 7.142193818 2600:8800:88…  2600:1900:41…   HTTP         456 GET /edgedl/release2/chrome_comp
541 7.178209455 2600:1900:41…  2600:8800:88…   HTTP         310 HTTP/1.1 200 OK
554 7.533881177 2600:8800:88…  2600:1900:41…   HTTP         486 GET /edgedl/release2/chrome_comp
```

```
▸ Internet Protocol Version 4, Src: 192.168.0.41, Dst: 128.119.245.12
▾ Transmission Control Protocol, Src Port: 34426, Dst Port: 80, Seq: 463, Ack: 1302, Len: 408
    Source Port: 34426
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 408]
    Sequence Number: 463    (relative sequence number)
    Sequence Number (raw): 3052063711
    [Next Sequence Number: 871    (relative sequence number)]
    Acknowledgment Number: 1302    (relative ack number)
    Acknowledgment number (raw): 1117769941
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 501
```

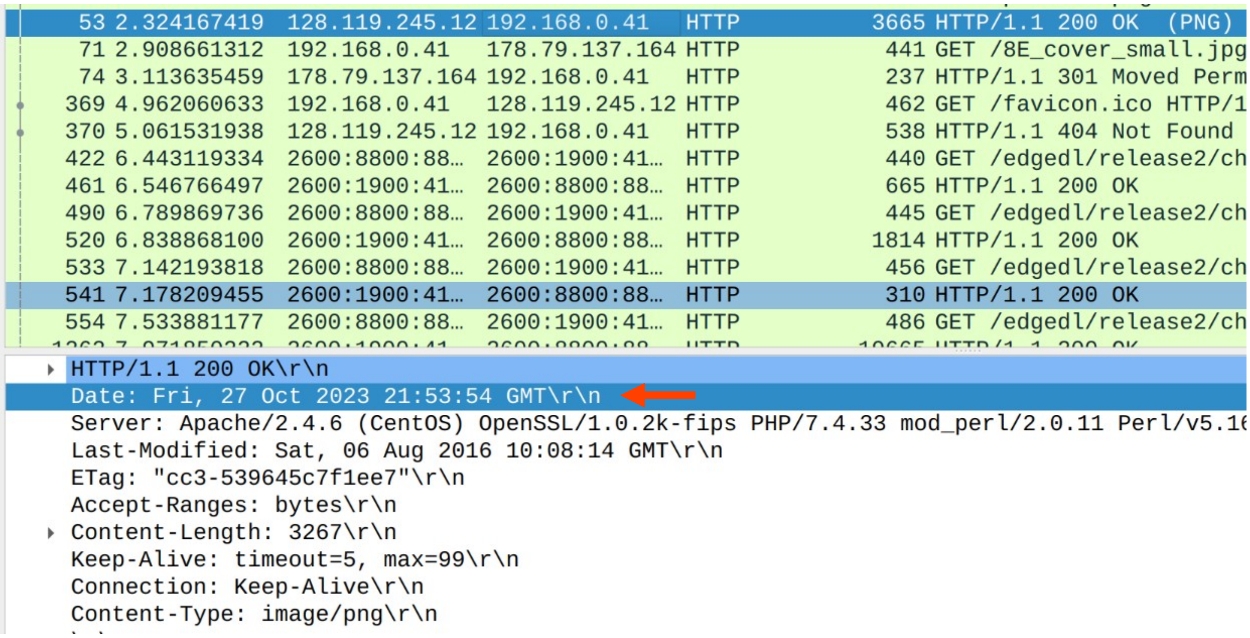
TCP for .png 2



```
No.     Time         Source          Destination     Protocol  Length Info
     43 2.106187972 192.168.0.41    128.119.245.12 HTTP           516 GET /wireshark-labs/HTTP-wiresha
     47 2.209780786 128.119.245.12 192.168.0.41    HTTP          1355 HTTP/1.1 200 OK  (text/html)
     49 2.219779266 192.168.0.41    128.119.245.12 HTTP           462 GET /pearson.png HTTP/1.1
     53 2.324167419 128.119.245.12 192.168.0.41    HTTP          3665 HTTP/1.1 200 OK  (PNG)
     71 2.908661312 192.168.0.41    178.79.137.164 HTTP           441 GET /8E_cover_small.jpg HTTP/1.1
     74 3.113635459 178.79.137.164 192.168.0.41    HTTP           237 HTTP/1.1 301 Moved Permanently
    369 4.962060633 192.168.0.41    128.119.245.12 HTTP           462 GET /favicon.ico HTTP/1.1
    370 5.061531938 128.119.245.12 192.168.0.41    HTTP           538 HTTP/1.1 404 Not Found  (text/ht
    422 6.443119334 2600:8800:88…   2600:1900:41…   HTTP           440 GET /edgedl/release2/chrome_comp
    461 6.546766497 2600:1900:41…   2600:8800:88…   HTTP           665 HTTP/1.1 200 OK
    490 6.789869736 2600:8800:88…   2600:1900:41…   HTTP           445 GET /edgedl/release2/chrome_comp
    520 6.838868100 2600:1900:41…   2600:8800:88…   HTTP          1814 HTTP/1.1 200 OK
    533 7.142193818 2600:8800:88…   2600:1900:41…   HTTP           456 GET /edgedl/release2/chrome_comp
    541 7.178209455 2600:1900:41…   2600:8800:88…   HTTP           310 HTTP/1.1 200 OK
    554 7.533881177 2600:8800:88…   2600:1900:41…   HTTP           486 GET /edgedl/release2/chrome_comp

▸ Internet Protocol Version 4, Src: 192.168.0.41, Dst: 178.79.137.164
▾ Transmission Control Protocol, Src Port: 51866, Dst Port: 80, Seq: 1, Ack: 1, Len: 375
    Source Port: 51866
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 375]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 69794010
    [Next Sequence Number: 376    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1817400401
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 502
```

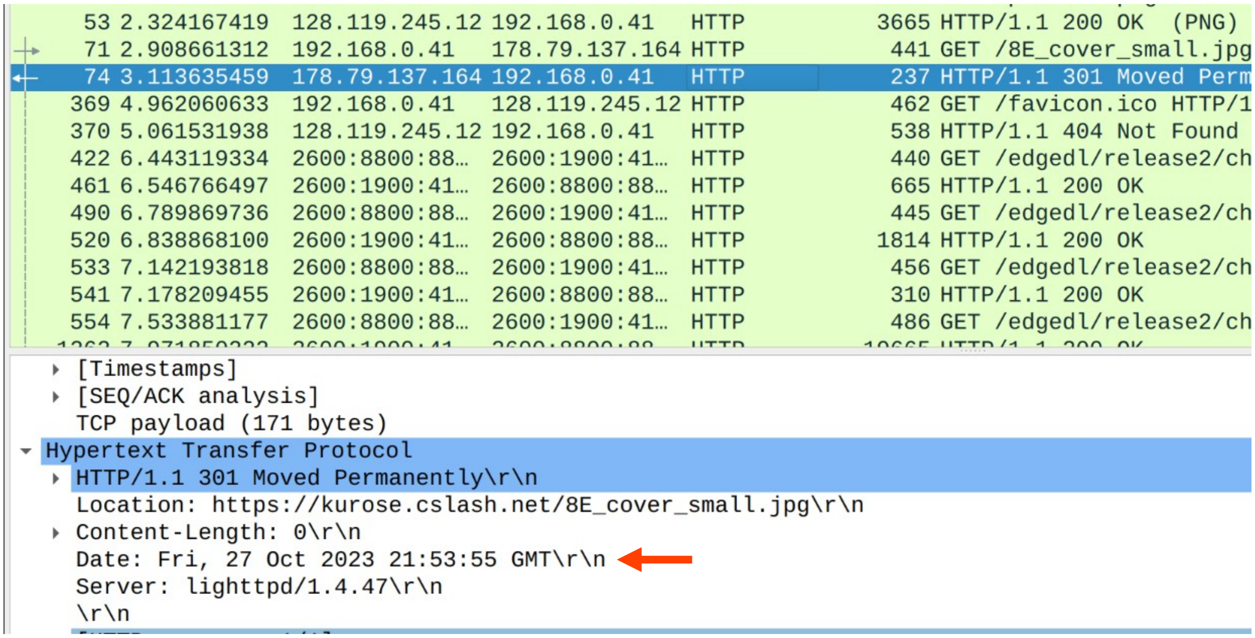
.png 1 response date



```
     53 2.324167419  128.119.245.12 192.168.0.41    HTTP          3665 HTTP/1.1 200 OK  (PNG)
     71 2.908661312  192.168.0.41    178.79.137.164 HTTP           441 GET /8E_cover_small.jpg
     74 3.113635459  178.79.137.164 192.168.0.41    HTTP           237 HTTP/1.1 301 Moved Perm
    369 4.962060633  192.168.0.41    128.119.245.12 HTTP           462 GET /favicon.ico HTTP/1
    370 5.061531938  128.119.245.12 192.168.0.41    HTTP           538 HTTP/1.1 404 Not Found
    422 6.443119334  2600:8800:88…   2600:1900:41…   HTTP           440 GET /edgedl/release2/ch
    461 6.546766497  2600:1900:41…   2600:8800:88…   HTTP           665 HTTP/1.1 200 OK
    490 6.789869736  2600:8800:88…   2600:1900:41…   HTTP           445 GET /edgedl/release2/ch
    520 6.838868100  2600:1900:41…   2600:8800:88…   HTTP          1814 HTTP/1.1 200 OK
    533 7.142193818  2600:8800:88…   2600:1900:41…   HTTP           456 GET /edgedl/release2/ch
    541 7.178209455  2600:1900:41…   2600:8800:88…   HTTP           310 HTTP/1.1 200 OK
    554 7.533881177  2600:8800:88…   2600:1900:41…   HTTP           486 GET /edgedl/release2/ch

  ▸ HTTP/1.1 200 OK\r\n
    Date: Fri, 27 Oct 2023 21:53:54 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
    Last-Modified: Sat, 06 Aug 2016 10:08:14 GMT\r\n
    ETag: "cc3-539645c7f1ee7"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 3267\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: image/png\r\n
```

.png 2 response date



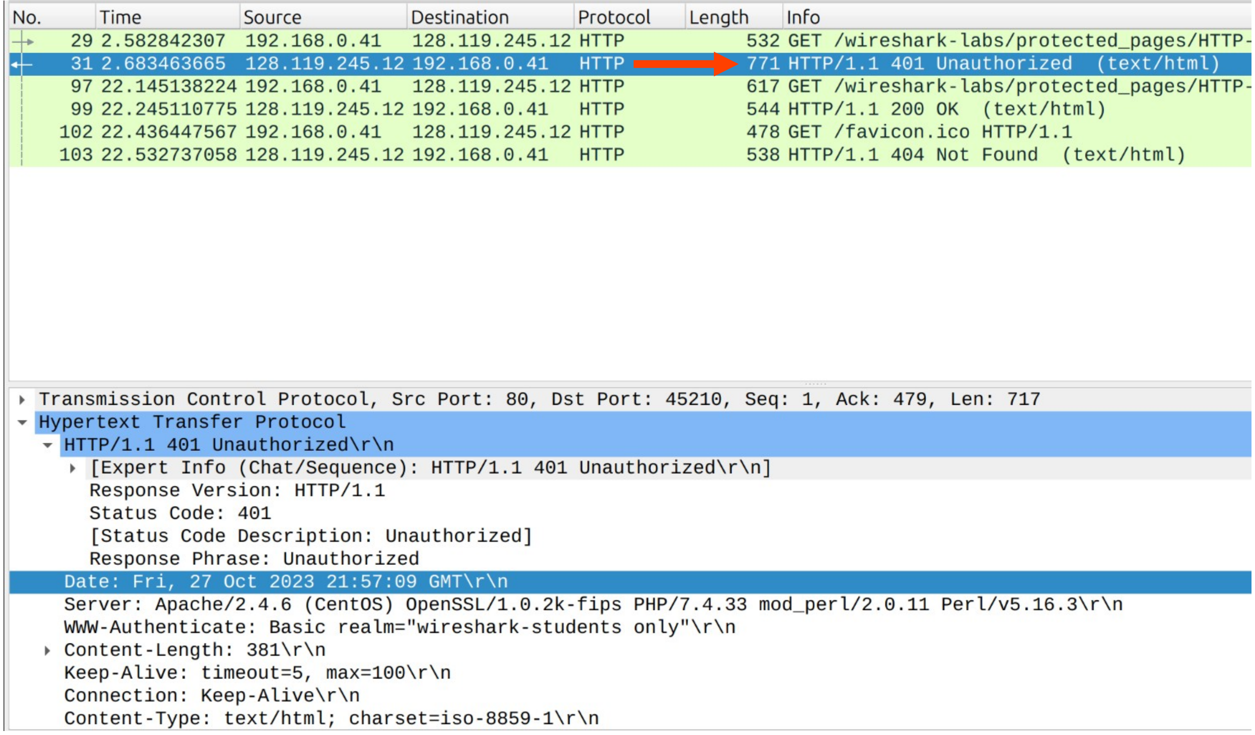
```
 53 2.324167419  128.119.245.12 192.168.0.41   HTTP  3665 HTTP/1.1 200 OK  (PNG)
 71 2.908661312  192.168.0.41   178.79.137.164 HTTP   441 GET /8E_cover_small.jpg
 74 3.113635459  178.79.137.164 192.168.0.41   HTTP   237 HTTP/1.1 301 Moved Perm
369 4.962060633  192.168.0.41   128.119.245.12 HTTP   462 GET /favicon.ico HTTP/1
370 5.061531938  128.119.245.12 192.168.0.41   HTTP   538 HTTP/1.1 404 Not Found
422 6.443119334  2600:8800:88…  2600:1900:41…  HTTP   440 GET /edgedl/release2/ch
461 6.546766497  2600:1900:41…  2600:8800:88…  HTTP   665 HTTP/1.1 200 OK
490 6.789869736  2600:8800:88…  2600:1900:41…  HTTP   445 GET /edgedl/release2/ch
520 6.838868100  2600:1900:41…  2600:8800:88…  HTTP  1814 HTTP/1.1 200 OK
533 7.142193818  2600:8800:88…  2600:1900:41…  HTTP   456 GET /edgedl/release2/ch
541 7.178209455  2600:1900:41…  2600:8800:88…  HTTP   310 HTTP/1.1 200 OK
554 7.533881177  2600:8800:88…  2600:1900:41…  HTTP   486 GET /edgedl/release2/ch
```

```
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (171 bytes)
Hypertext Transfer Protocol
  HTTP/1.1 301 Moved Permanently\r\n
  Location: https://kurose.cslash.net/8E_cover_small.jpg\r\n
  Content-Length: 0\r\n
  Date: Fri, 27 Oct 2023 21:53:55 GMT\r\n
  Server: lighttpd/1.4.47\r\n
  \r\n
```

5. HTTP Authentication

Answer the following questions (and provide appropriate annotated screen shots):

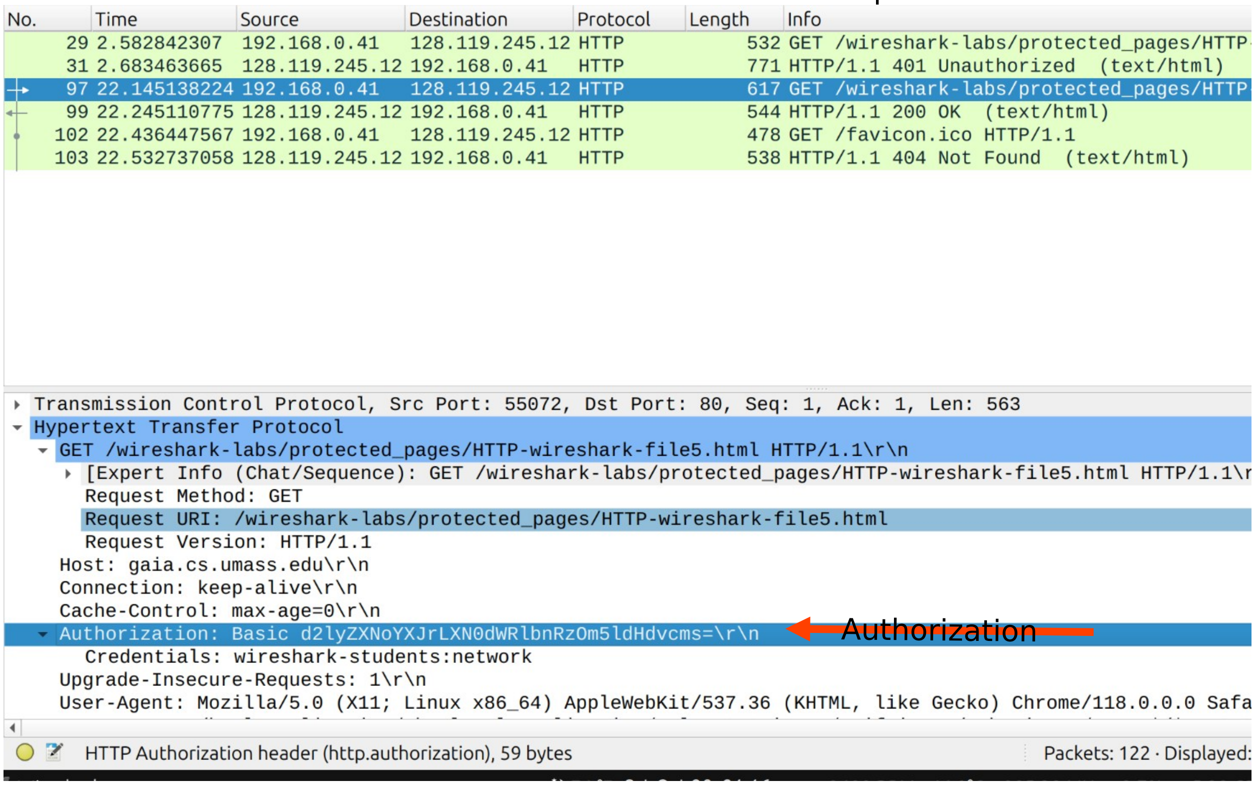
17. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? The server is asking for credentials before we can proceed forward. Status 401 Unauthorized.



```
No.  Time         Source         Destination    Protocol Length Info
 29 2.582842307  192.168.0.41   128.119.245.12 HTTP      532 GET /wireshark-labs/protected_pages/HTTP-
 31 2.683463665  128.119.245.12 192.168.0.41   HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
 97 22.145138224 192.168.0.41   128.119.245.12 HTTP      617 GET /wireshark-labs/protected_pages/HTTP-
 99 22.245110775 128.119.245.12 192.168.0.41   HTTP      544 HTTP/1.1 200 OK  (text/html)
102 22.436447567 192.168.0.41   128.119.245.12 HTTP      478 GET /favicon.ico HTTP/1.1
103 22.532737058 128.119.245.12 192.168.0.41   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
Transmission Control Protocol, Src Port: 80, Dst Port: 45210, Seq: 1, Ack: 479, 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: Fri, 27 Oct 2023 21:57:09 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
  Content-Length: 381\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=iso-8859-1\r\n
```

18. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? Now the GET includes a header field Authorization with a value in base64 as per the lab.



```
No.    Time         Source         Destination    Protocol   Length Info
    29 2.582842307  192.168.0.41   128.119.245.12 HTTP          532 GET /wireshark-labs/protected_pages/HTTP-
    31 2.683463665  128.119.245.12 192.168.0.41   HTTP          771 HTTP/1.1 401 Unauthorized  (text/html)
    97 22.145138224 192.168.0.41   128.119.245.12 HTTP          617 GET /wireshark-labs/protected_pages/HTTP-
    99 22.245110775 128.119.245.12 192.168.0.41   HTTP          544 HTTP/1.1 200 OK  (text/html)
   102 22.436447567 192.168.0.41   128.119.245.12 HTTP          478 GET /favicon.ico HTTP/1.1
   103 22.532737058 128.119.245.12 192.168.0.41   HTTP          538 HTTP/1.1 404 Not Found  (text/html)
```

```
▸ Transmission Control Protocol, Src Port: 55072, Dst Port: 80, Seq: 1, Ack: 1, Len: 563
▾ Hypertext Transfer Protocol
  ▾ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r
      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
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  ▾ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safa
```

Authorization
HTTP Authorization header (http.authorization), 59 bytes
Packets: 122 · Displayed:

PART 2: DNS (10 Points)

Wireshark Analysis of DNS.pcap

1. Download and open the **DNS.pcap** file posted on D2L with this assignment (make sure you’ve cleared your filters from the previous exercise).
2. Locate the DNS query and response messages. Are they sent over UDP or TCP? **(2 point)** User Datagram Protocol (UDP)
3. Open DNS packet number 9. What is this DNS query requesting? (**2 point**) The request is for the IP address for www.netbsd.org.
4. What does the DNS response provide? (**2 point**)
   The IP Address which is 204.152.190.12 for the host www.netbsd.org.
5. What is the query in packet number 11 asking for? (**2 point**)
   Type “AAAA” which is IPV6 address request for www.netbsd.org.
6. Look at packets 35 and 36. What happens here? (**2 point**)
   Packet 35 requests IPV4 address of GRIMM.utelsystems.local. Packet 36 responds saying I can find no such name to which an IP address is related.

PART 3: SMTP (10 Points)

Using Wireshark to analyze SMTP data.

To do the exercises you will need to download the ***SMTP.pcap*** file posted on D2L.

1. Open Wireshark.
2. Select File, Open on the menu bar. Select the SMTP Capture file (SMTP.pcap).
3. Locate the SMTP messages. Are they sent over UDP or TCP? **(2 point)**
   Transmission Control Protocol (TCP).
4. Observe the SMTP header in Packet **#18**. Find the information for every field of the header of this SMTP packet: **(2 point)**
   a. To: <teacher@starfish.eller.arizona.edu>
   b. From: "Student" <student@starfish.eller.arizona.edu>
   c. Date: Sat, 27 Nov 2010 18:00:52 -0700
   d. Subject: Class information
   e. MessageID#: <00a801cb8e97$b41ebbb0$1c5c3310$@eller.arizona.edu>
5. The first three frames are the three steps of the TCP startup. Frames 4 to 24, 26 contain the e-mail process and the e-mail message. Frames 25, 27-29 describe TCP shutdown. **(2 point)**
   a. What port number is used by the client? How do you know?
      The local host is using 192.168 designation for a local LAN. The local host is 192.168.1.100 and the source port is 55012 for this TCP segment activity.
   b. What port number is used on the server? How do you know?
      The server is a non local LAN number and its port is 25 for this TCP segment activity.
6. Locate packet 18 and click on it. Look inside the packet and expand the Internet Message Format tab (expand as many levels as needed). Answer the following questions from the email message **(2 point)**:
   a. What is the name of the person sending the email message?
      The name of the student is Pat Green.
   b. When was she born?
      Feb 10 1980.
   c. What is her SSN?

123-44-3211

d. Which part of the SMTP packed did you find this information in?
Under the Multipart Media Encapsulation (MIME) portion of the Internet Message Format.

e. In viewing this message, would you be concerned about email security? How could the security be improved?
Yes, this is concerning as we now know her sensitive information putting her in danger of having it used by someone else. This could be improved by making the data not readable by humans until it reaches its intended destination.

7. Locate frames 14 and 15. What is the purpose of these 2 frames? **(2 points)**

It would seem that packets 14 and 15 both carry portions needed for the MIME to be reconstructed in packet 18 later. Packet 14 carries the pure text conversation with the needed tags to build it later. Packet 15 carries the ASCII encoding that will tell the output how to make it look like it should. For example fonts, styles, margins, colors, etc for the text in packet 14.