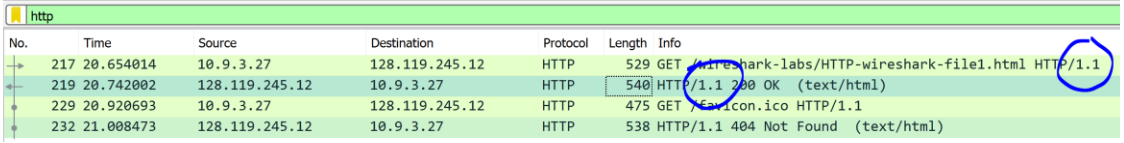
Gretel Rajamoney

4-22-2021

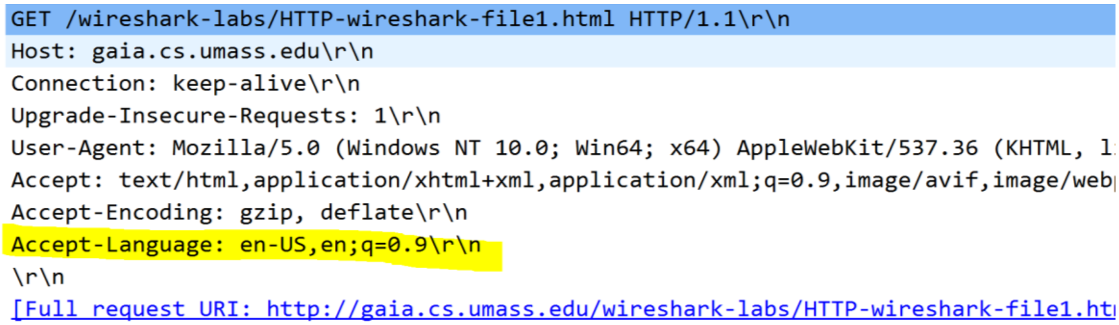
Wireshark Lab 2

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   My browser is running HTTP version 1.1, and my server is running HTTP version 1.1 as well.



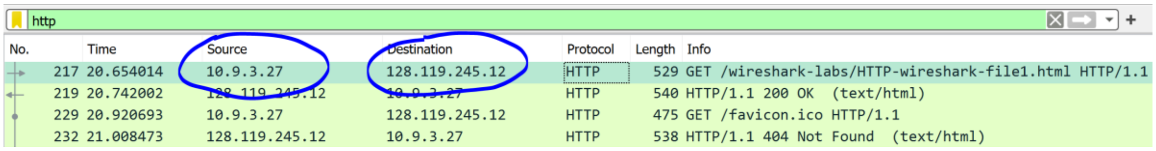
```
No.    Time        Source          Destination       Protocol  Length  Info
  217  20.654014   10.9.3.27       128.119.245.12    HTTP      529     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  219  20.742002   128.119.245.12  10.9.3.27         HTTP      540     HTTP/1.1 200 OK  (text/html)
  229  20.920693   10.9.3.27       128.119.245.12    HTTP      475     GET /favicon.ico HTTP/1.1
  232  21.008473   128.119.245.12  10.9.3.27         HTTP      538     HTTP/1.1 404 Not Found  (text/html)
```

2. What languages (if any) does your browser indicate that it can accept to the server?
   The language my browser indicates that it can accept is US-English.



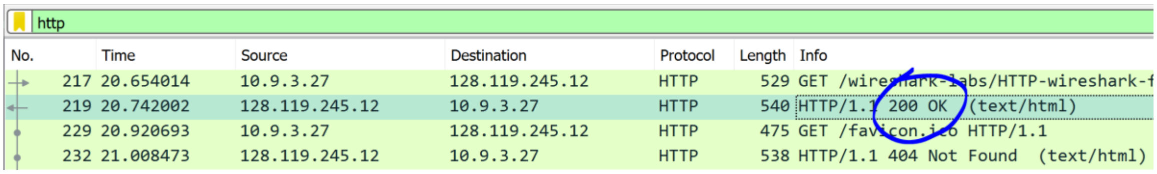
```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
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.ht
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   The IP address of my computer is 10.9.3.27 and the IP address of the gaia.cs.umass.edu server is 128.119.245.12



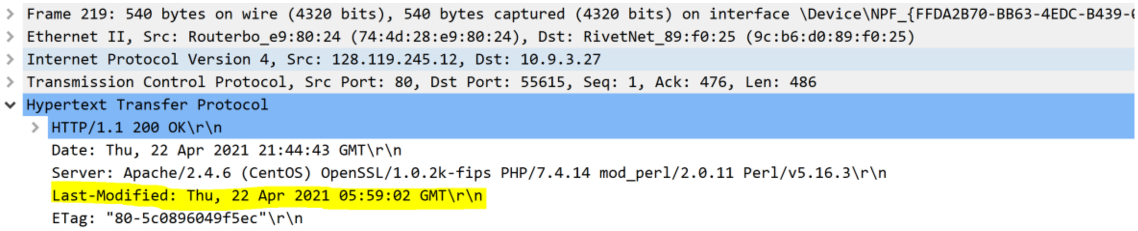
```
No.    Time        Source          Destination       Protocol  Length  Info
  217  20.654014   10.9.3.27       128.119.245.12    HTTP      529     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  219  20.742002   128.119.245.12  10.9.3.27         HTTP      540     HTTP/1.1 200 OK  (text/html)
  229  20.920693   10.9.3.27       128.119.245.12    HTTP      475     GET /favicon.ico HTTP/1.1
  232  21.008473   128.119.245.12  10.9.3.27         HTTP      538     HTTP/1.1 404 Not Found  (text/html)
```

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



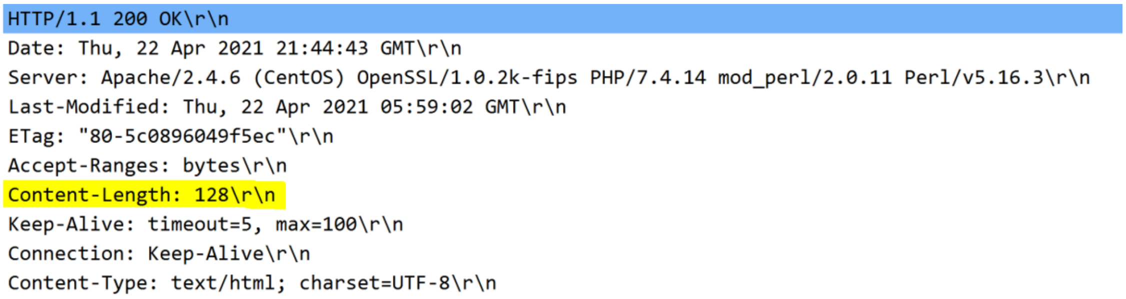
```
No.    Time        Source          Destination       Protocol  Length  Info
  217  20.654014   10.9.3.27       128.119.245.12    HTTP      529     GET /wireshark-labs/HTTP-wireshark-f
  219  20.742002   128.119.245.12  10.9.3.27         HTTP      540     HTTP/1.1 200 OK  (text/html)
  229  20.920693   10.9.3.27       128.119.245.12    HTTP      475     GET /favicon.ico HTTP/1.1
  232  21.008473   128.119.245.12  10.9.3.27         HTTP      538     HTTP/1.1 404 Not Found  (text/html)
```

5. When was the HTML file that you are retrieving last modified at the server?
   The HTML file that I am retrieving last modified at the server on Thursday, April 22 of 2021 and 05:59:02 GMT



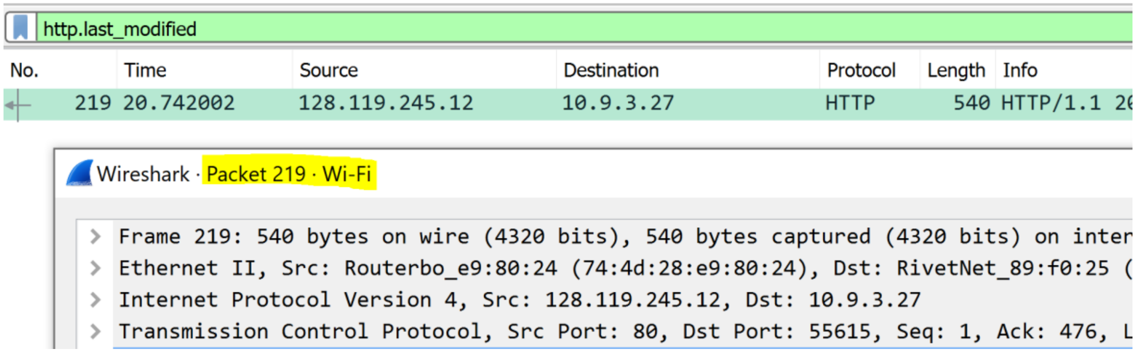
```
> Frame 219: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{FFDA2B70-BB63-4EDC-B439-
> Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Dst: RivetNet_89:f0:25 (9c:b6:d0:89:f0:25)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.9.3.27
> Transmission Control Protocol, Src Port: 80, Dst Port: 55615, Seq: 1, Ack: 476, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 22 Apr 2021 21:44:43 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 22 Apr 2021 05:59:02 GMT\r\n
    ETag: "80-5c0896049f5ec"\r\n
```

6. How many bytes of content are being returned to your browser?
   There are 128 bytes of content being returned to my browser.



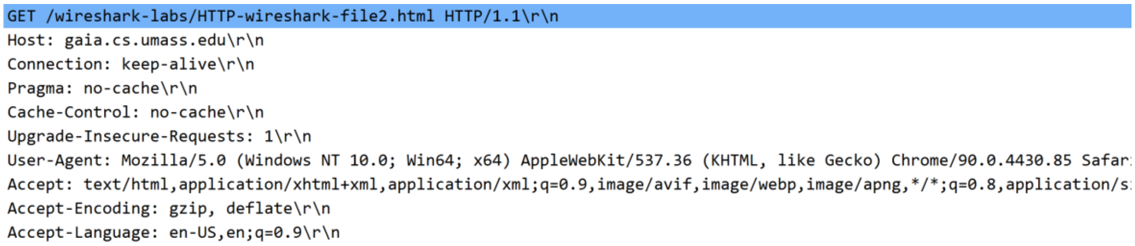
```
HTTP/1.1 200 OK\r\n
Date: Thu, 22 Apr 2021 21:44:43 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Thu, 22 Apr 2021 05:59:02 GMT\r\n
ETag: "80-5c0896049f5ec"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
```

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.
   Through inspecting the raw data in the packet content window, there are no headers within the data that are not displayed in the packet-listing window.



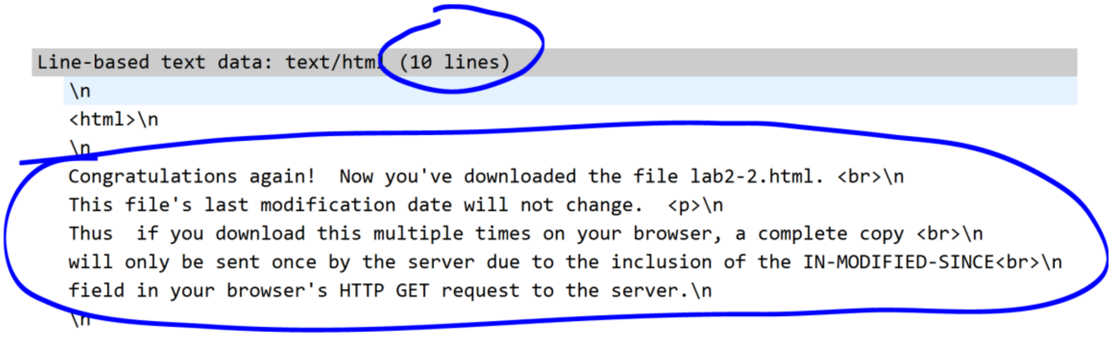
```
http.last_modified

No.     Time        Source            Destination    Protocol   Length  Info
    219 20.742002   128.119.245.12    10.9.3.27      HTTP          540  HTTP/1.1 2

Wireshark · Packet 219 · Wi-Fi

> Frame 219: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on inter
> Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Dst: RivetNet_89:f0:25 (
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.9.3.27
> Transmission Control Protocol, Src Port: 80, Dst Port: 55615, Seq: 1, Ack: 476, L
```

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?
   After inspecting the contents of the first HTTP GET request from my browser to the server, there is no IF-MODIFIED-SINCE line.

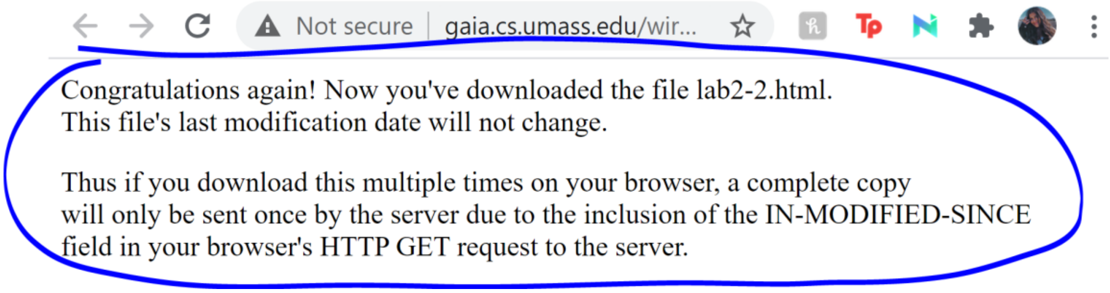


```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Pragma: no-cache\r\n
Cache-Control: no-cache\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safar
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
```

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   Yes, the server explicitly returned the contents of the file, I can tell because it returns the following 10 lines as shown in the screenshot. The second screenshot provided below, shows what the browser displays.



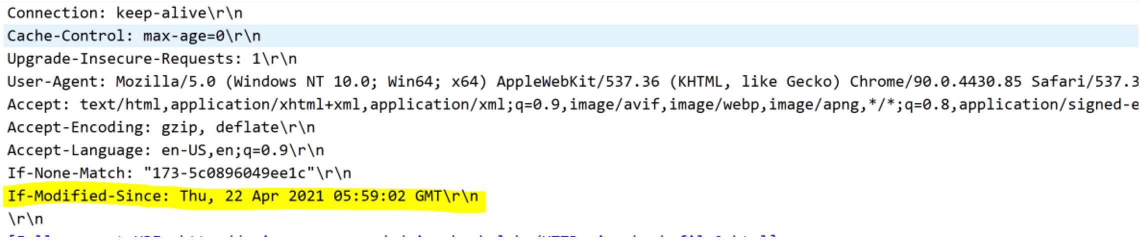
```
Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    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
```



Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

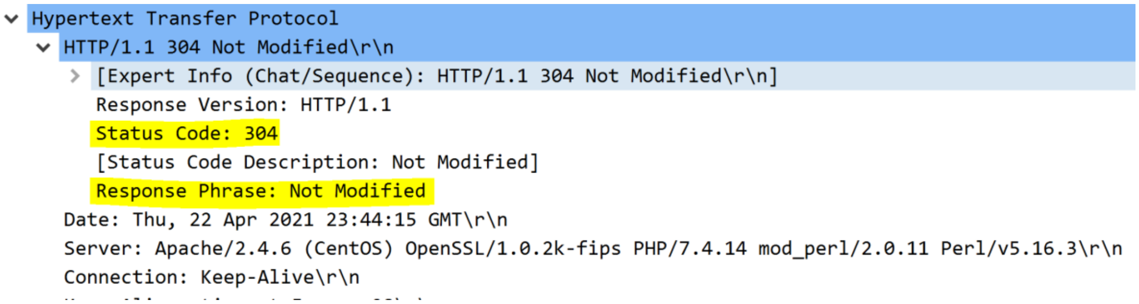
Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
field in your browser's HTTP GET request to the server.

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?
    After inspecting the contents of the second HTTP GET request from my browser to the server, the information that follows the IF-MODIFIED-SINCE header is Thu, 22 Apr 2021 05:59:02 GMT



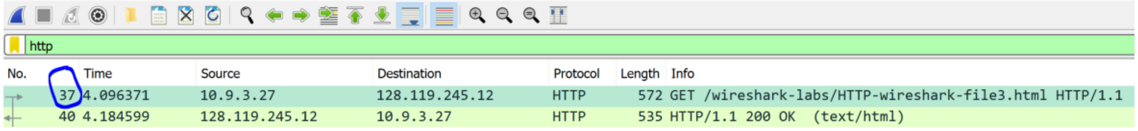
```
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5c0896049ee1c"\r\n
If-Modified-Since: Thu, 22 Apr 2021 05:59:02 GMT\r\n
\r\n
```

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.
    The HTTP status code is 304, and the phrase returned from the sever in response to this second HTTP GET is Not Modified. The server does not explicitly return the contents of the file because we cleared the browsers cache data, resulting in it being empty.



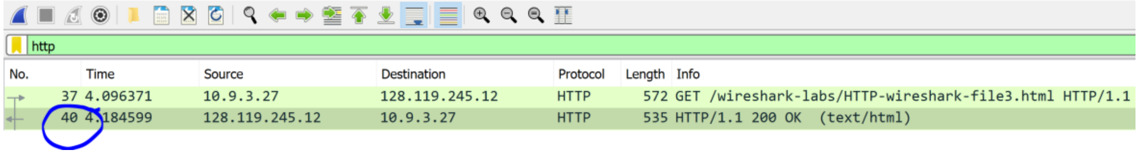
```
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Thu, 22 Apr 2021 23:44:15 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
```

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?
    My browser sends 1 HTTP GET request message. The packet number 37 contains the GET message for the Bill of Rights.



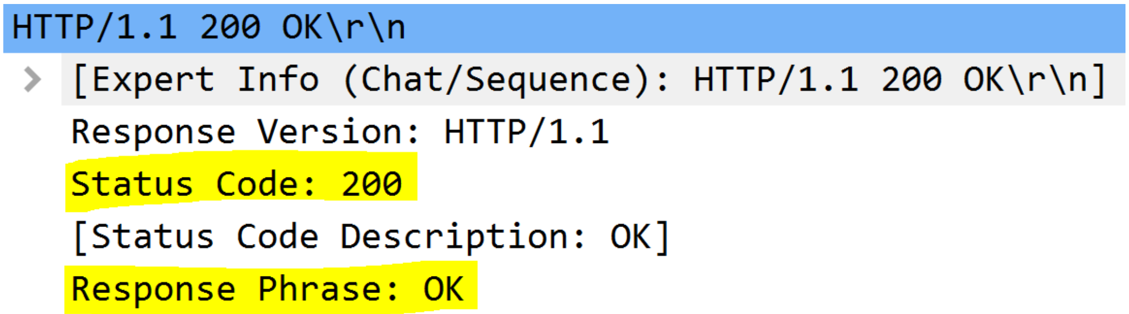
```
http
No.   Time        Source           Destination      Protocol  Length  Info
   37 4.096371    10.9.3.27        128.119.245.12   HTTP       572 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   40 4.184599    128.119.245.12   10.9.3.27        HTTP       535 HTTP/1.1 200 OK  (text/html)
```

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    The packet number associated with the response to the HTTP GET request is 40, the status code is 200, and response phrase is OK.



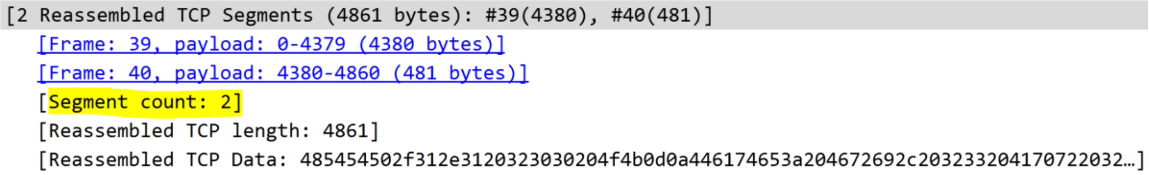
```
http
No.   Time        Source           Destination      Protocol  Length  Info
   37 4.096371    10.9.3.27        128.119.245.12   HTTP       572 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   40 4.184599    128.119.245.12   10.9.3.27        HTTP       535 HTTP/1.1 200 OK  (text/html)
```

14. What is the status code and phrase in the response?
    The status code and phrase in the response are 200 and OK.



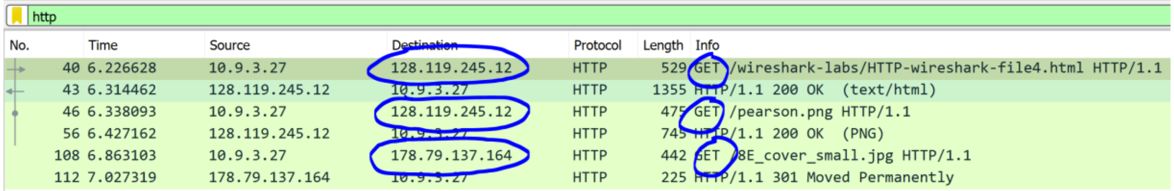
```
HTTP/1.1 200 OK\r\n
 > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
   Response Version: HTTP/1.1
   Status Code: 200
   [Status Code Description: OK]
   Response Phrase: OK
```

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
    There were 2 data-containing TCP segments needed to carry the single HTTP response and the text of the Bill of Rights.



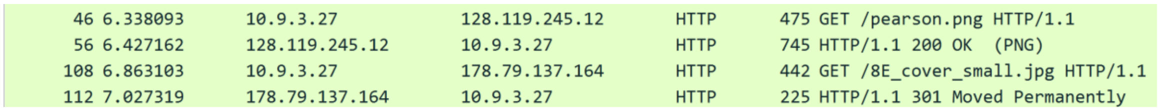
```
[2 Reassembled TCP Segments (4861 bytes): #39(4380), #40(481)]
    [Frame: 39, payload: 0-4379 (4380 bytes)]
    [Frame: 40, payload: 4380-4860 (481 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c20323320417072202032…]
```

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    My browser sent 3 HTTP GET request messages. The internet addresses that these GET requests were sent are 128.119.245.12, 128.119.245.12, and 178.79.137.164.



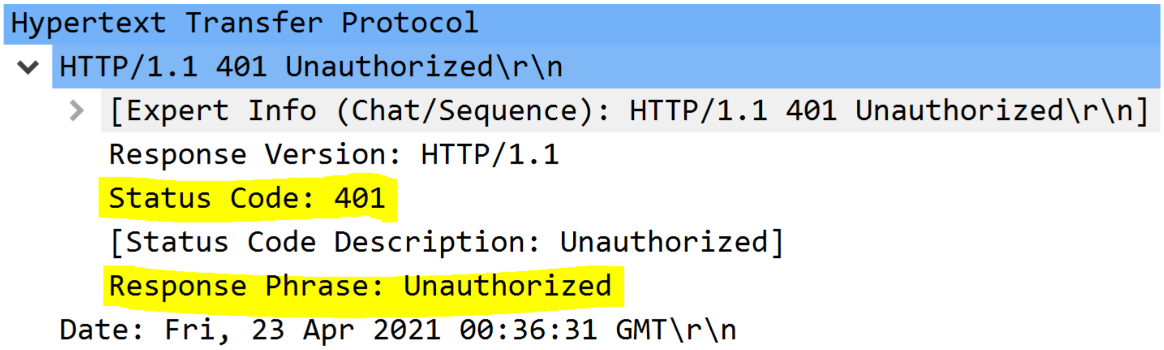
```
http
No.   Time        Source           Destination      Protocol  Length  Info
   40 6.226628    10.9.3.27        128.119.245.12   HTTP       529 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
   43 6.314462    128.119.245.12   10.9.3.27        HTTP      1355 HTTP/1.1 200 OK  (text/html)
   46 6.338093    10.9.3.27        128.119.245.12   HTTP       475 GET /pearson.png HTTP/1.1
   56 6.427162    128.119.245.12   10.9.3.27        HTTP       745 HTTP/1.1 200 OK  (PNG)
  108 6.863103    10.9.3.27        178.79.137.164   HTTP       442 GET /8E_cover_small.jpg HTTP/1.1
  112 7.027319    178.79.137.164   10.9.3.27        HTTP       225 HTTP/1.1 301 Moved Permanently
```

17. Can you tell whether your browser downloaded the two images serially, of whether they were downloaded from the two web sites in parallel? Explain.
    The two images were downloaded serially because as you can see in the screenshot below, the request for the first image was sent and then received prior to the request for the second image was sent. Due to this, the images were not downloaded from the two web sites in parallel.



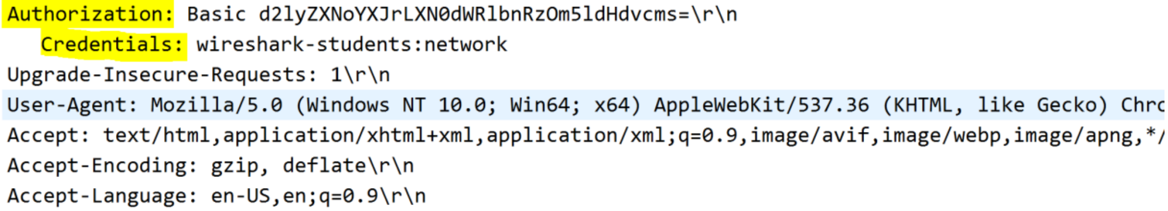
```
 46 6.338093    10.9.3.27       128.119.245.12   HTTP    475 GET /pearson.png HTTP/1.1
 56 6.427162    128.119.245.12  10.9.3.27        HTTP    745 HTTP/1.1 200 OK  (PNG)
108 6.863103    10.9.3.27       178.79.137.164   HTTP    442 GET /8E_cover_small.jpg HTTP/1.1
112 7.027319    178.79.137.164  10.9.3.27        HTTP    225 HTTP/1.1 301 Moved Permanently
```

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



```
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, 23 Apr 2021 00:36:31 GMT\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?
    When my browser sends the HTTP GET message for the second time, the new field included in the HTTP GET message is the Authorization and Credentials.



```
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) Chro
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
```