ECS 152A Programming 2

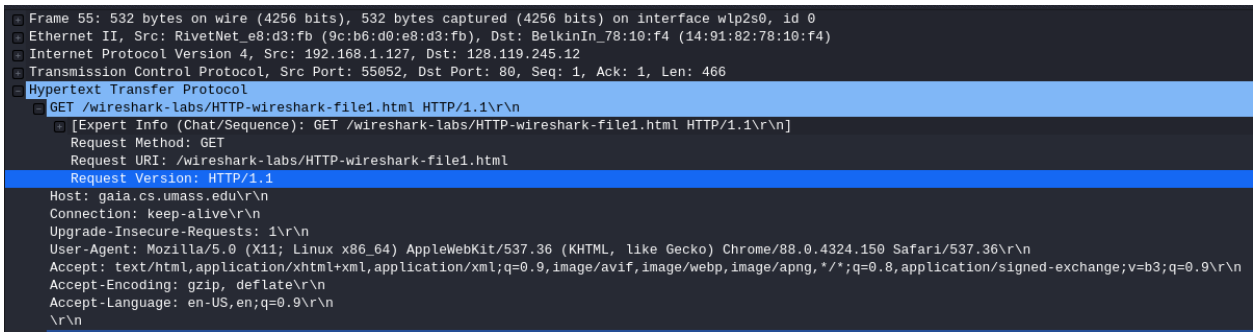
Daniel Phan	Noah Tarr
ID 914831996	ID 917286014
Section A04	Section A02

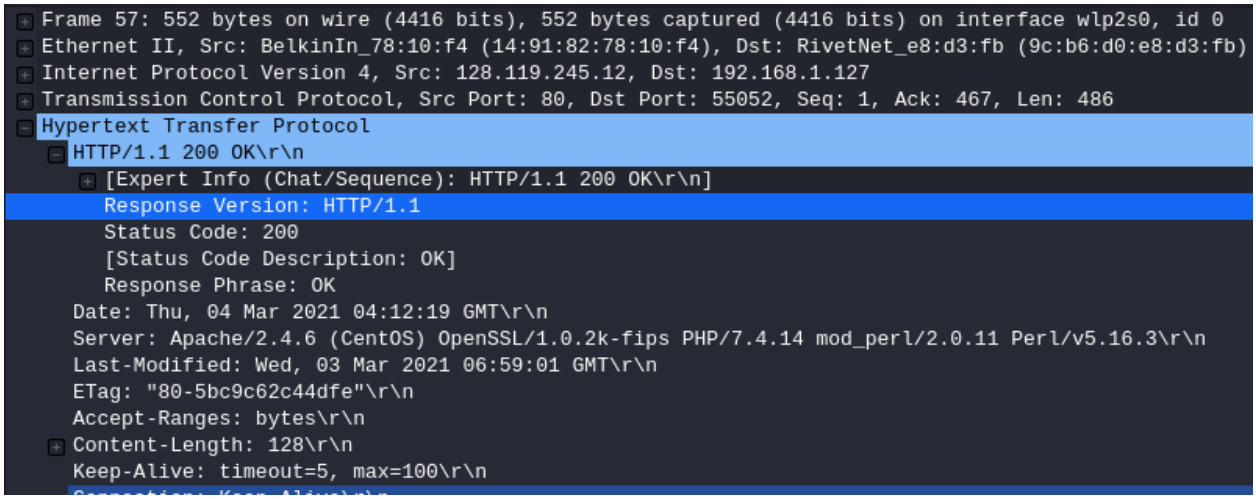
Due: 03/07/2021

1 HTTP Wireshark Lab

1.1 The Basic HTTP GET/Response Interaction

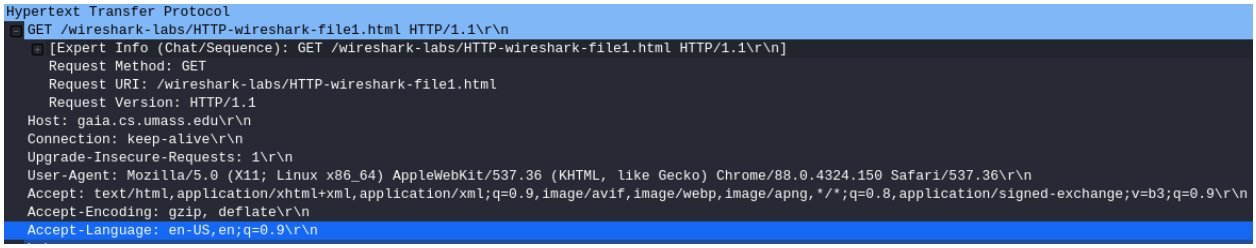
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

   - Both my browser and the server are running HTTP version 1.1.
   - 

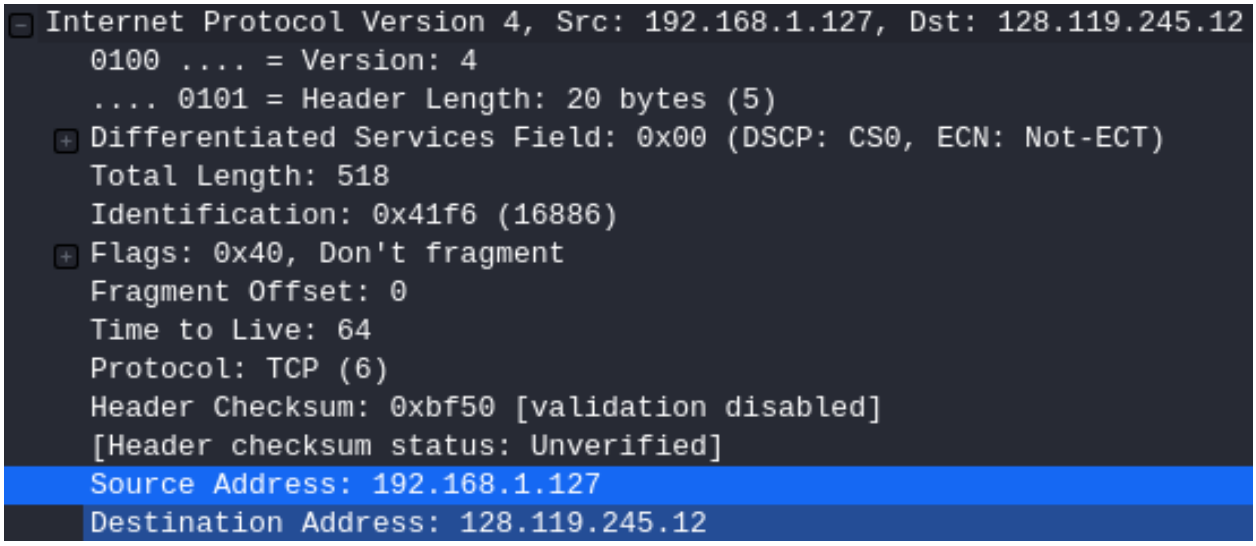
   - 

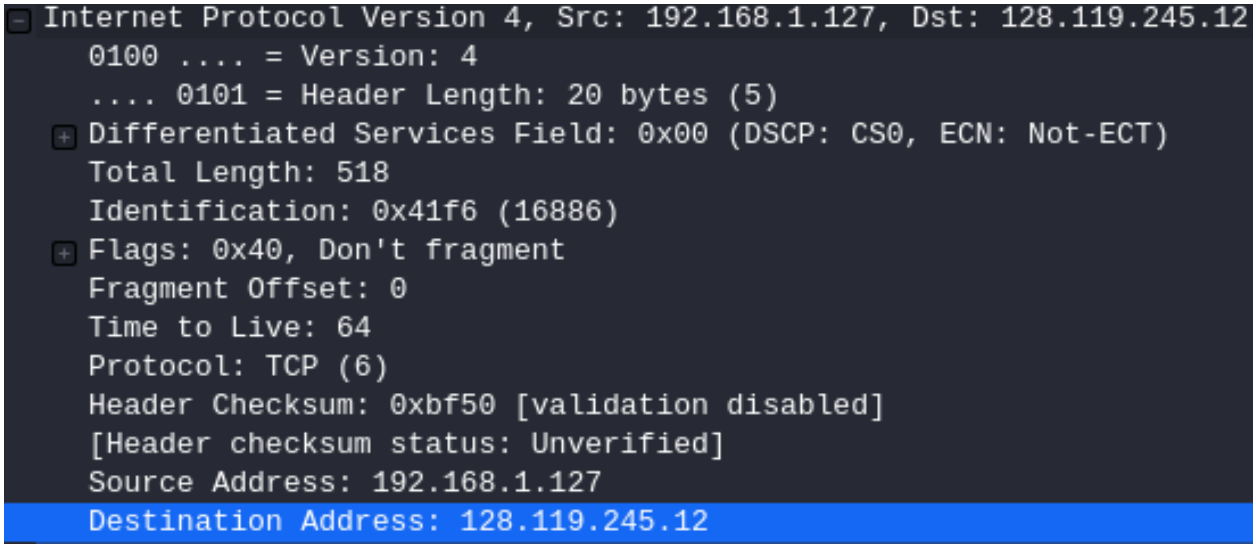
2. What languages (if any) does your browser indicate that it can accept to the server?

   - My browser indicates that it accepts US English.

- 

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

   - My IP address is 192.168.1.127, while the server's IP address is 128.119.245.12.
   - 

   - 

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

   - The server returned 200 for the HTML file and 404 for favico.ico.

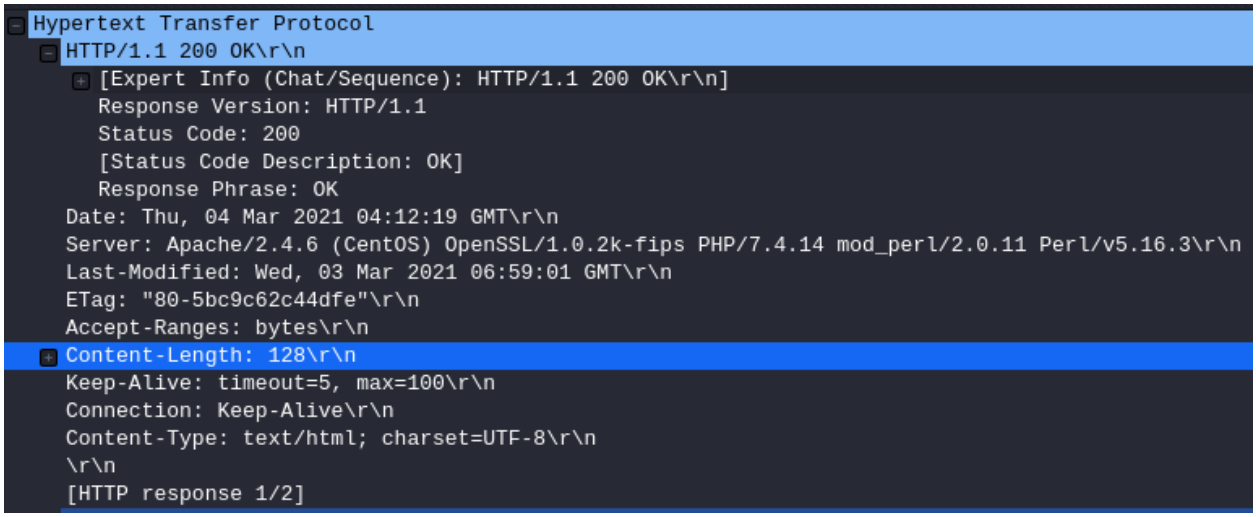
```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 04 Mar 2021 04:12:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 03 Mar 2021 06:59:01 GMT\r\n
    ETag: "80-5bc9c62c44dfe"\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
```

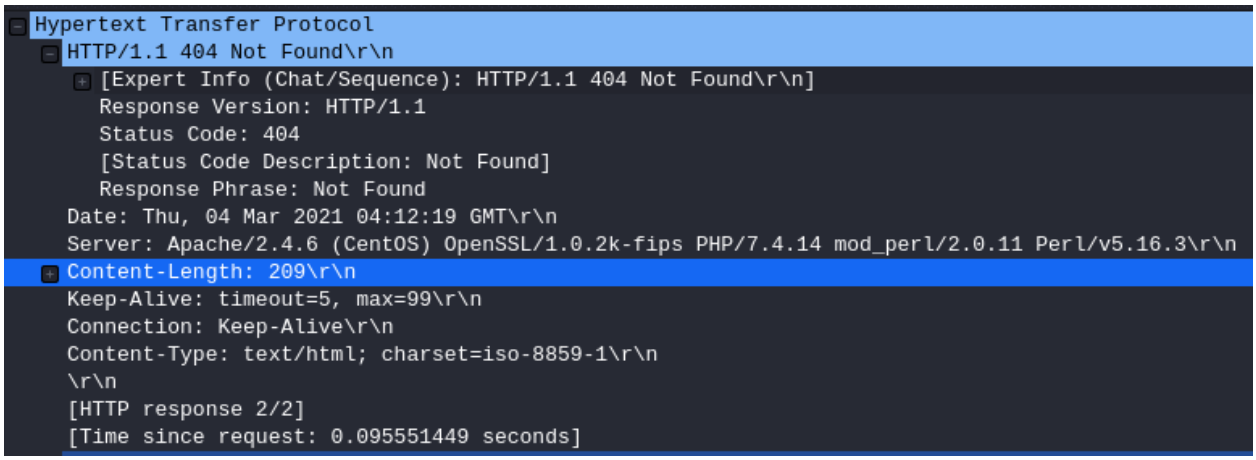
```
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
    Date: Thu, 04 Mar 2021 04:12:19 GMT\r\n
    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
  Content-Length: 209\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.095551449 seconds]
```

5. When was the HTML file that you are retrieving last modified at the server?
   - It was last modified on March 3, 2021, at 06:59:01 GMT.

```
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: Thu, 04 Mar 2021 04:12:19 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: Wed, 03 Mar 2021 06:59:01 GMT\r\n
    ETag: "80-5bc9c62c44dfe"\r\n
    Accept-Ranges: bytes\r\n
```

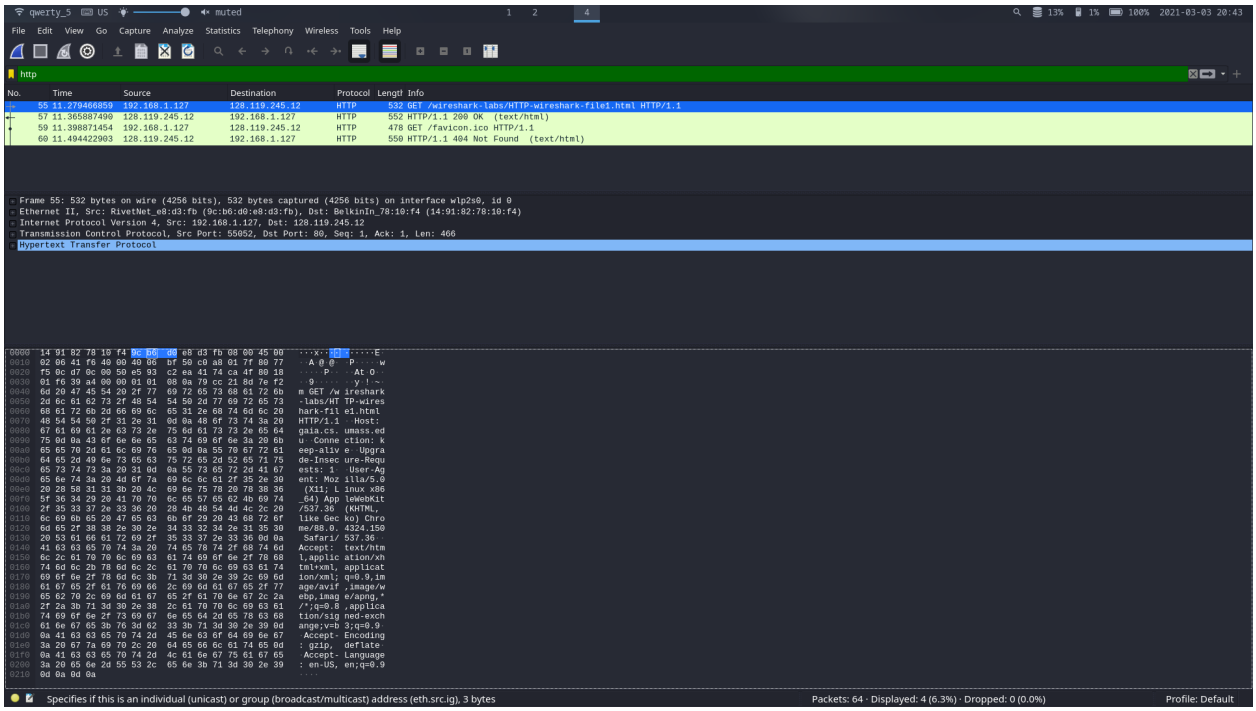
6. How many bytes of content are being returned to your browser?
   - There were 128 bytes for the HTML file, and 209 bytes for favico.ico.

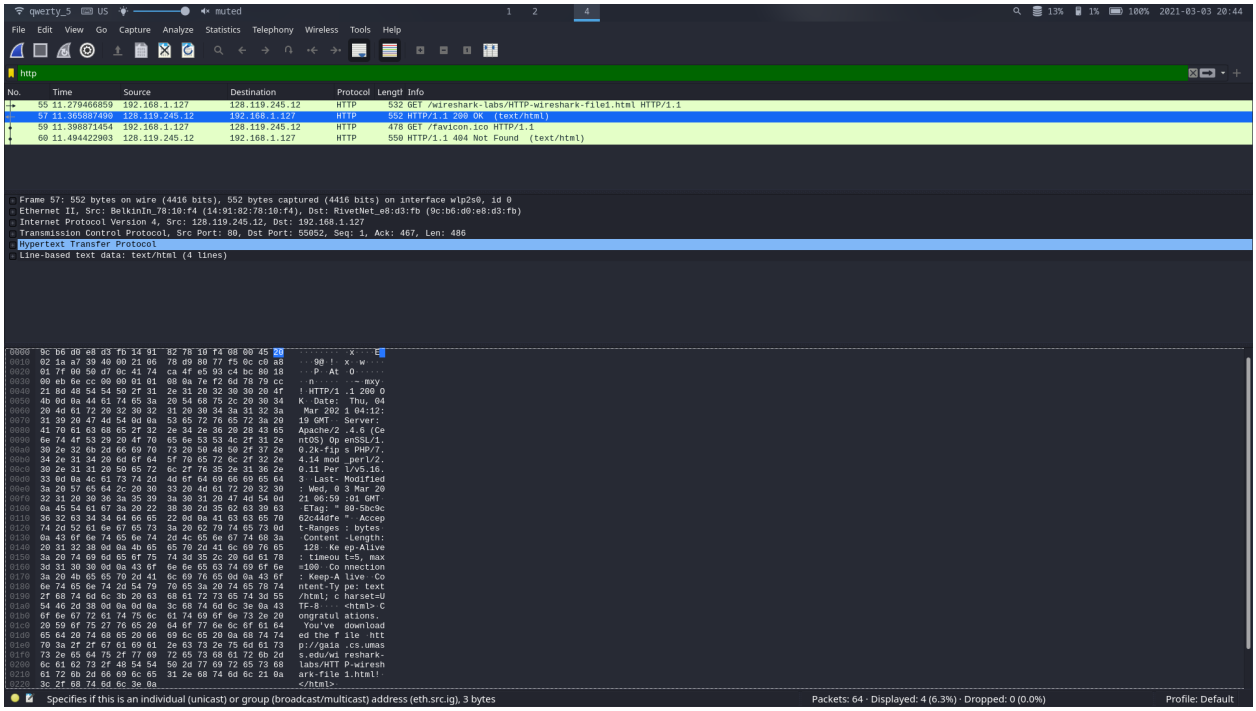
- 

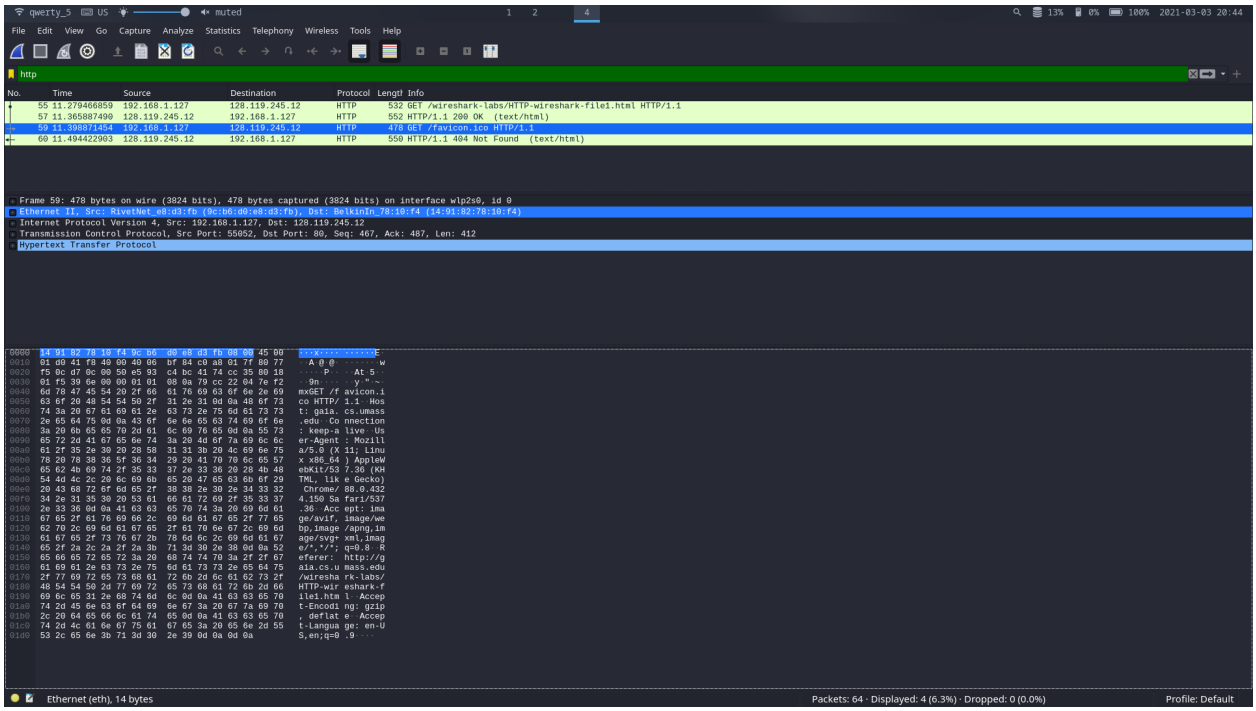
- 

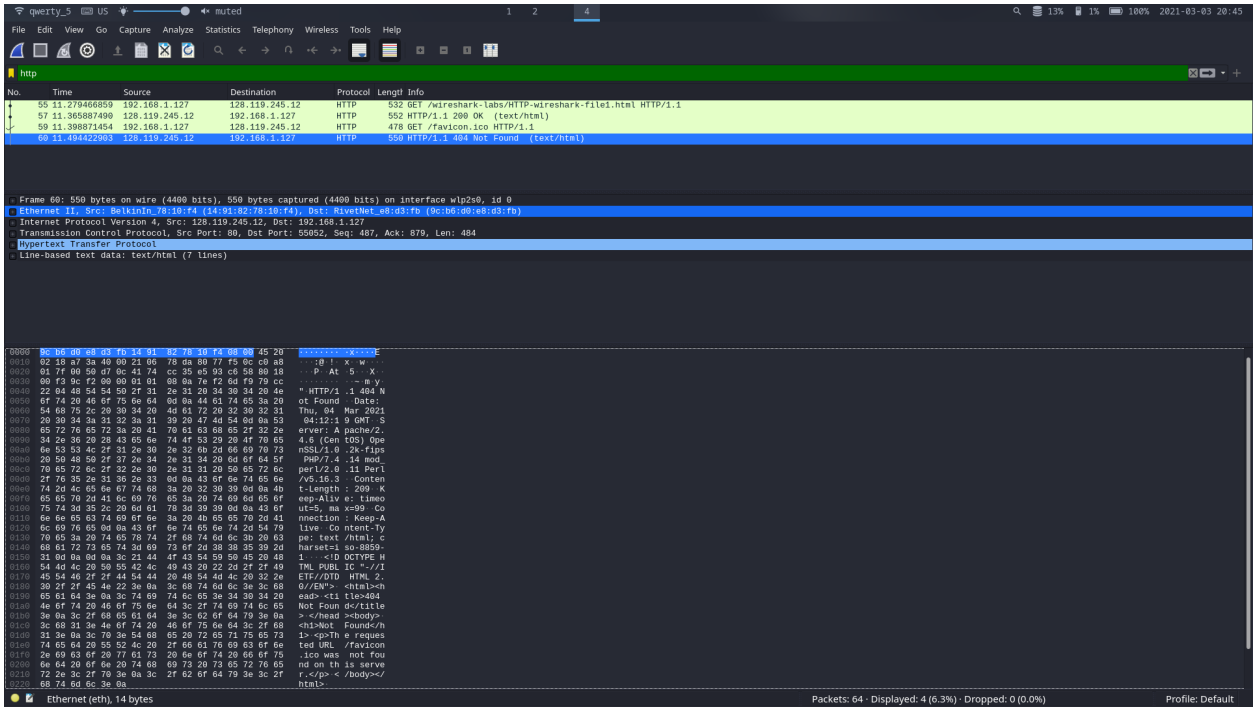
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

    - I do not see any headers that are not displayed.


qwerty_5 US muted 1 2 4 13% 1% 100% 2021-03-03 20:43
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
55 11.279466859 192.168.1.127 128.119.245.12 HTTP 532 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
57 11.365887490 128.119.245.12 192.168.1.127 HTTP 552 HTTP/1.1 200 OK (text/html)
59 11.398871454 192.168.1.127 128.119.245.12 HTTP 478 GET /favicon.ico HTTP/1.1
60 11.494422903 128.119.245.12 192.168.1.127 HTTP 550 HTTP/1.1 404 Not Found (text/html)
Frame 55: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface wlp2s0, id 0
Ethernet II, Src: RivetNet_e8:d3:fb (9c:b6:d0:e8:d3:fb), Dst: BelkinIn_78:10:f4 (14:91:82:78:10:f4)
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55052, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
Hypertext Transfer Protocol
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.src.ig), 3 bytes
Packets: 64 · Displayed: 4 (6.3%) · Dropped: 0 (0.0%)
Profile: Default


qwerty_5 US muted 1 2 4 13% 1% 100% 2021-03-03 20:44
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
55 11.279466859 192.168.1.127 128.119.245.12 HTTP 532 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
57 11.365887490 128.119.245.12 192.168.1.127 HTTP 552 HTTP/1.1 200 OK (text/html)
59 11.398871454 192.168.1.127 128.119.245.12 HTTP 478 GET /favicon.ico HTTP/1.1
60 11.494422903 128.119.245.12 192.168.1.127 HTTP 550 HTTP/1.1 404 Not Found (text/html)
Frame 57: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface wlp2s0, id 0
Ethernet II, Src: BelkinIn_78:10:f4 (14:91:82:78:10:f4), Dst: RivetNet_e8:d3:fb (9c:b6:d0:e8:d3:fb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
Transmission Control Protocol, Src Port: 80, Dst Port: 55052, Seq: 1, Ack: 467, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.src.ig), 3 bytes
Packets: 64 · Displayed: 4 (6.3%) · Dropped: 0 (0.0%)
Profile: Default

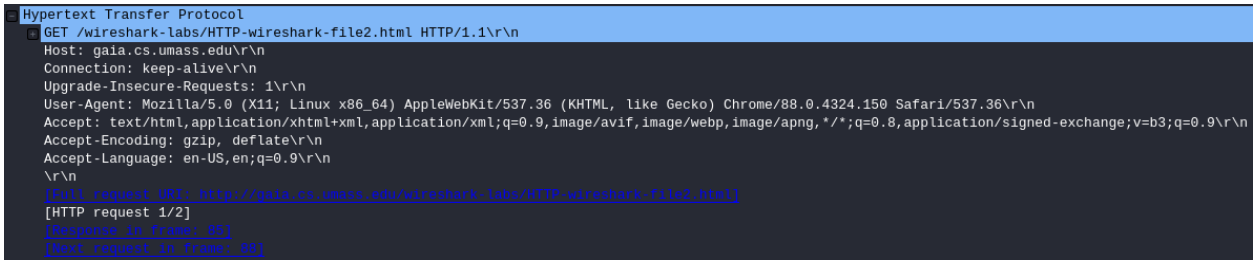


- 

1.2 The HTTP CONDITIONAL GET/response interaction

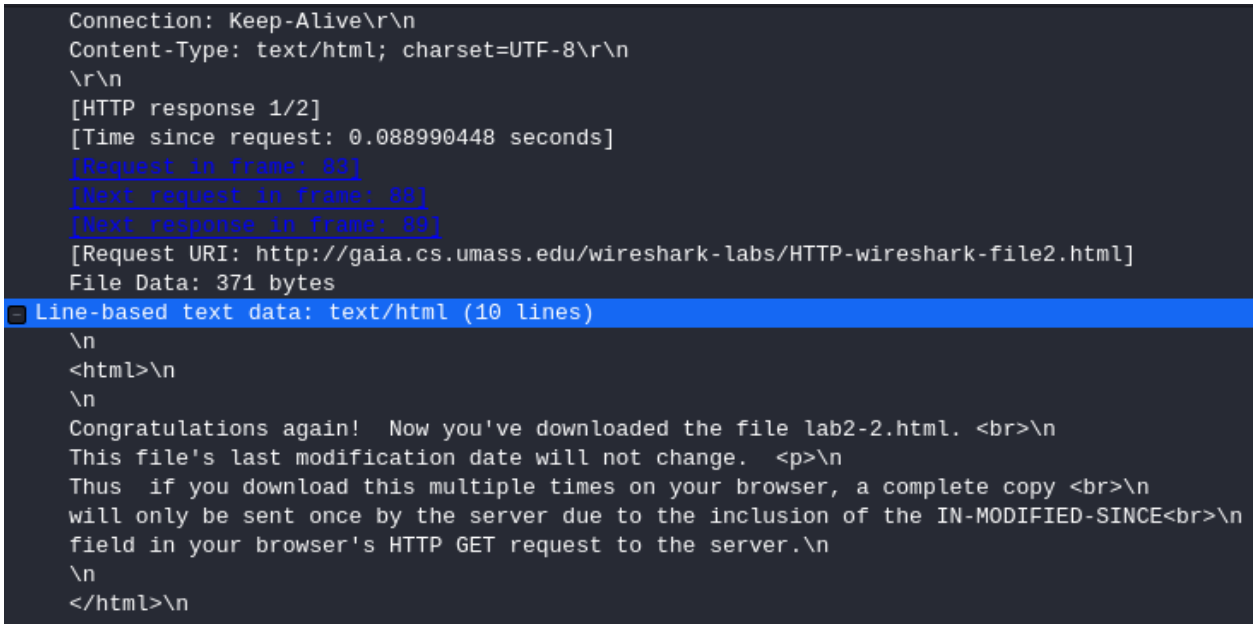
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

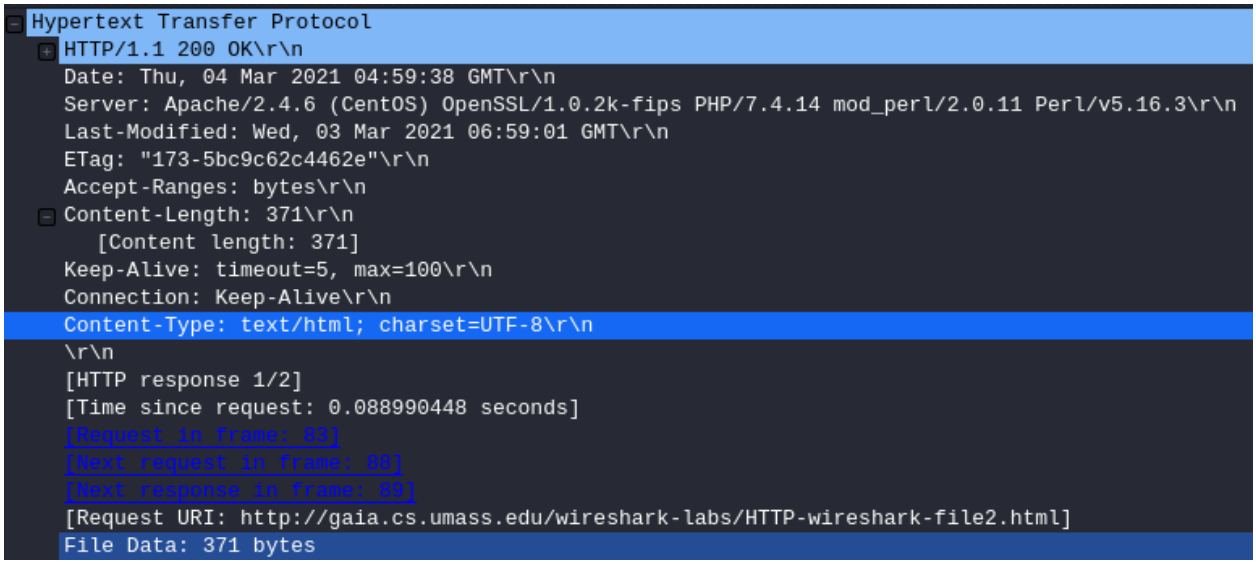
   - I do not see an "IF-MODIFIED-SINCE" line in the HTTP GET.

- 

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

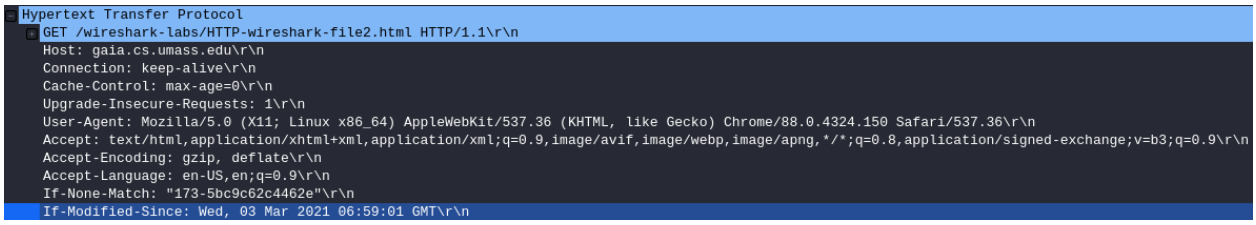
   - The server explicitly returned the contents. I can tell because the response contains the HTML file content, and content fields like "Content-Type" and "Content Length" are set.

   - 

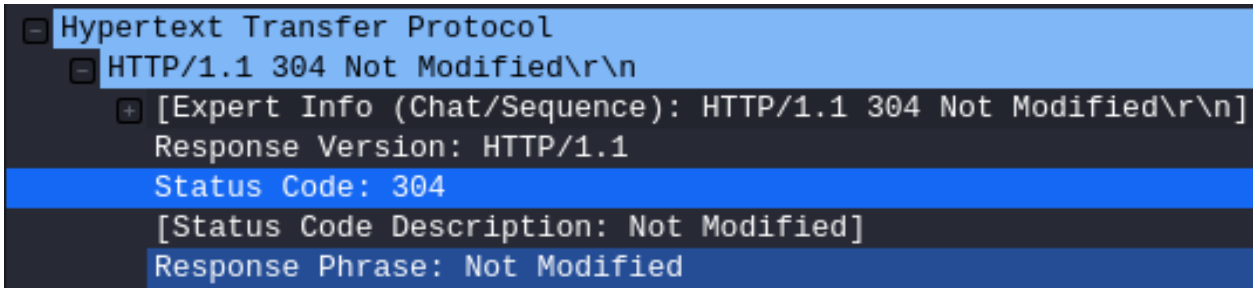
   - 

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?

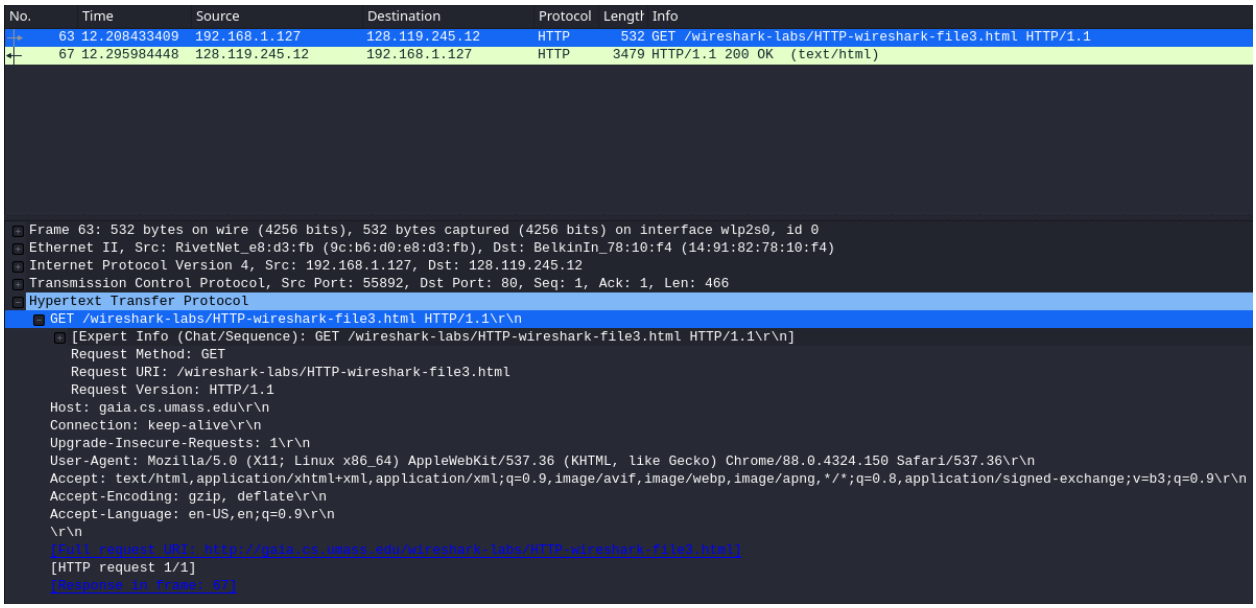
- There is an "If-Modified-Since" line, and it contains "Wed, 03 Mar 2021 06:59:01 GMT".
- 

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?

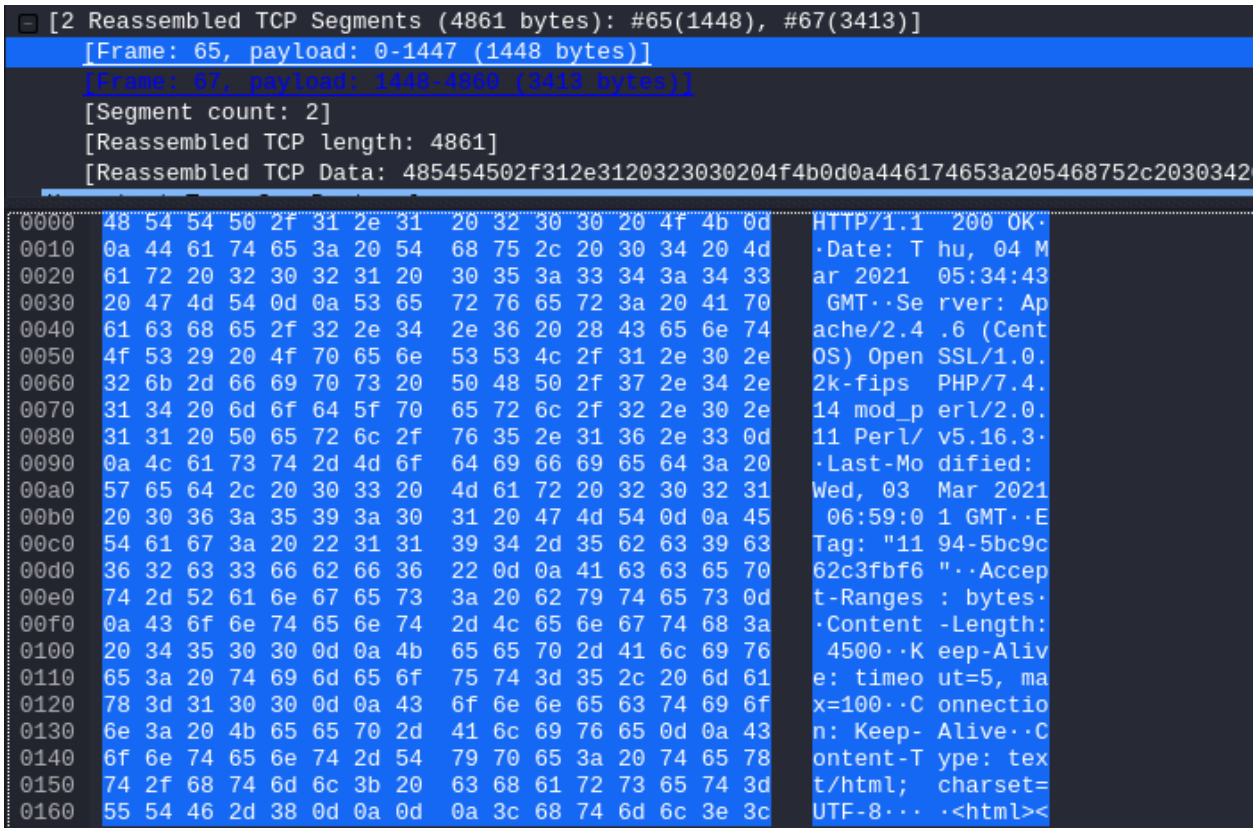
- The HTTP status code is 304 and the response phrase is "Not Modified". The server did not explicitly return the contents of the file, as none of the signs described in the response to question 9 appeared here.
- 

1.3 Retrieving Long Documents

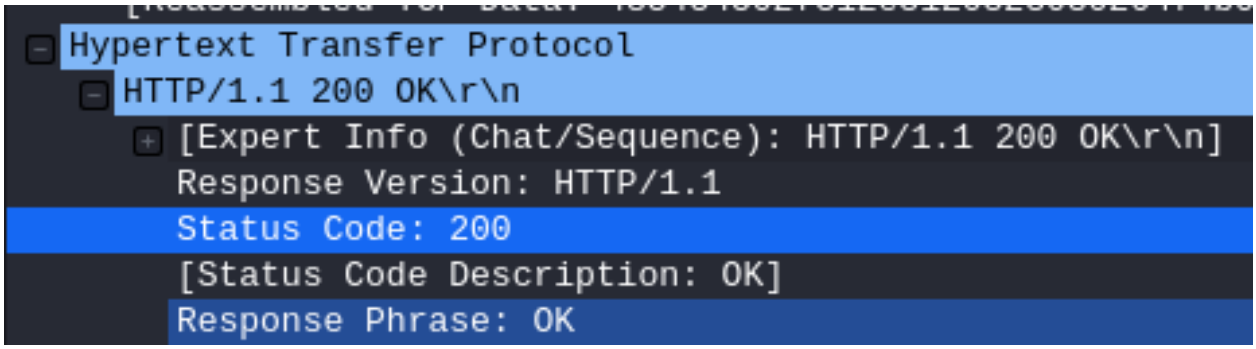
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

- My browser sent one HTTP GET request. The packet number was 63.
- 

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

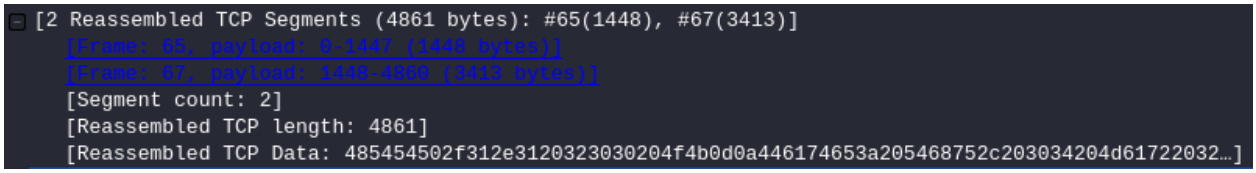
    - The packet number is 65. We see that the response was broken into 2 TCP segments. The raw data of the first segment, packet 65, is highlighted in blue, and we see the HTTP status code and phrase at the top of the raw data.
    - 

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

    - The status code is 200, and the phrase is "OK".
    - 

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

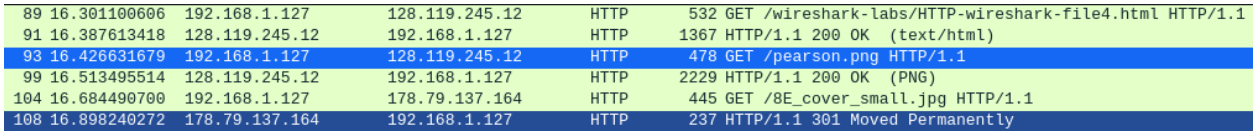
    - 2 data-containing TCP segments were needed.

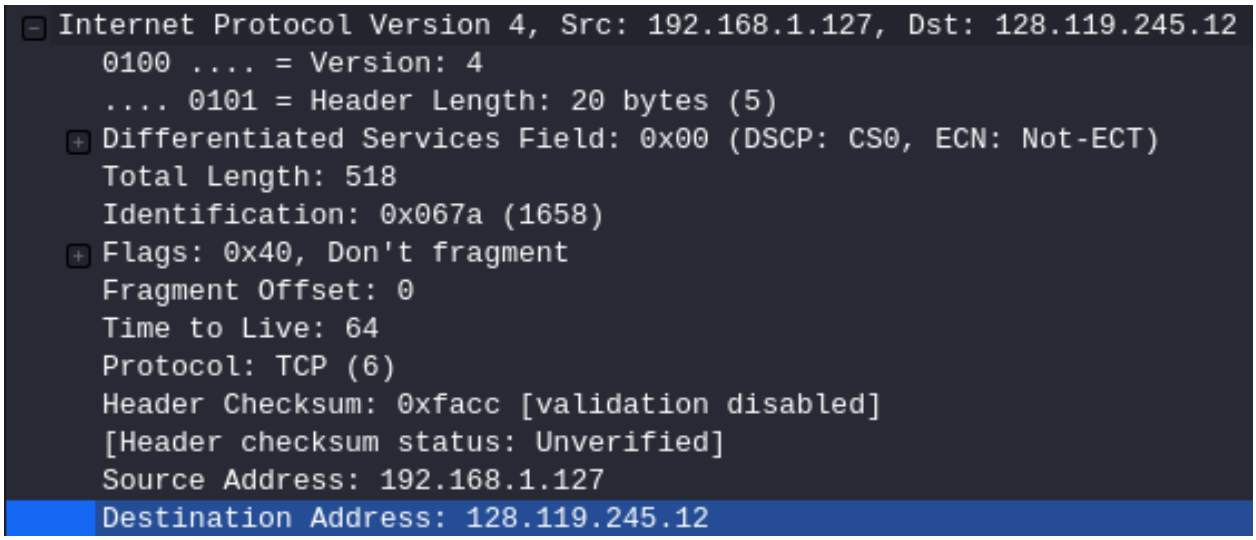
- 

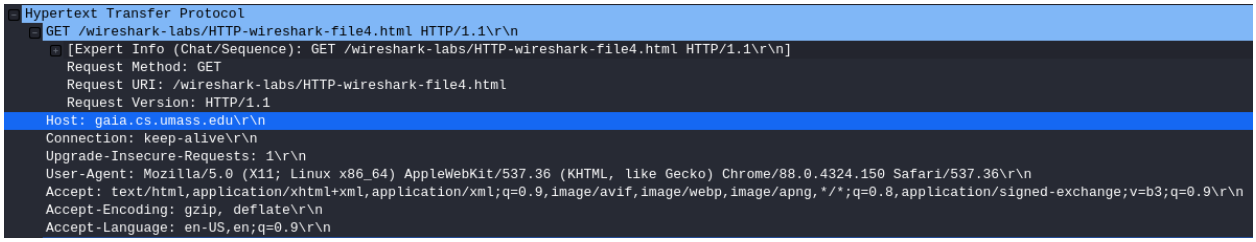
1.4 HTML Documents with Embedded Objects

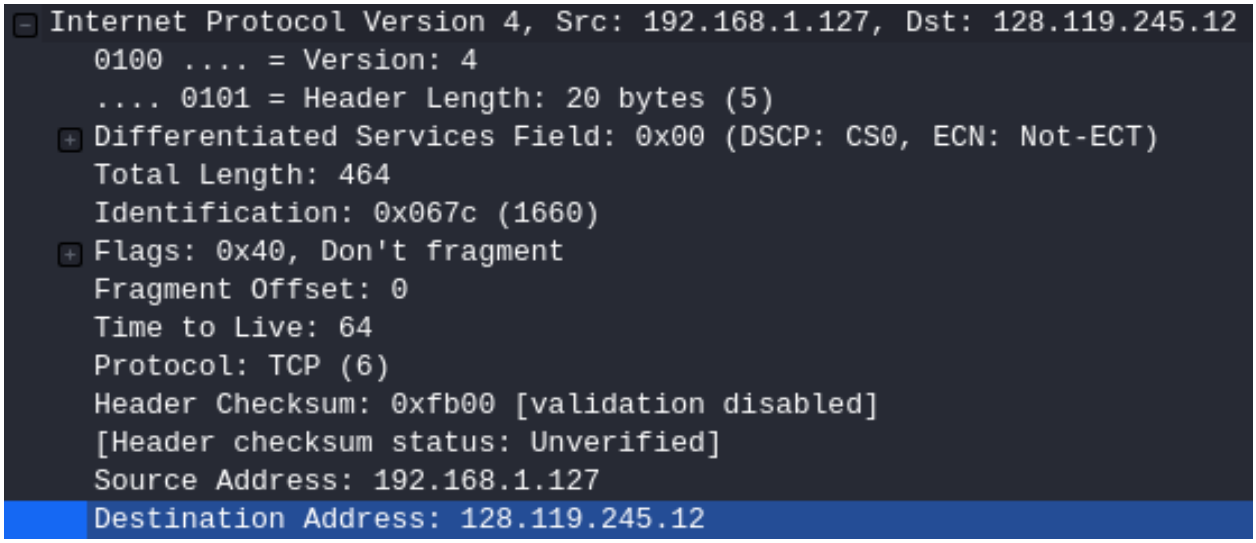
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

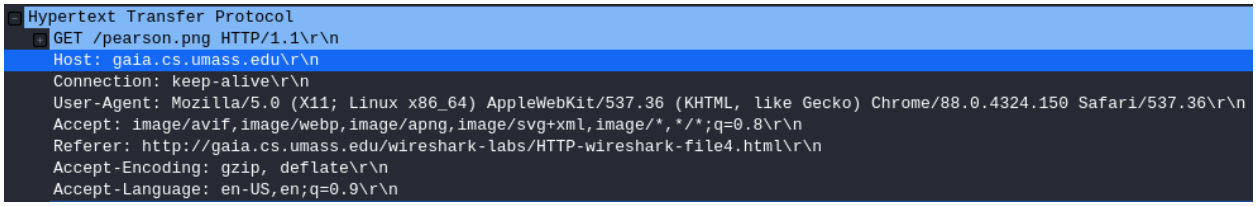
    - 3 HTTP GET requests were sent. The first two went to 128.119.245.12 (`gaia.cs.umass.edu`), while the third went to 178.79.137.164 (`kurose.cslash.net`).

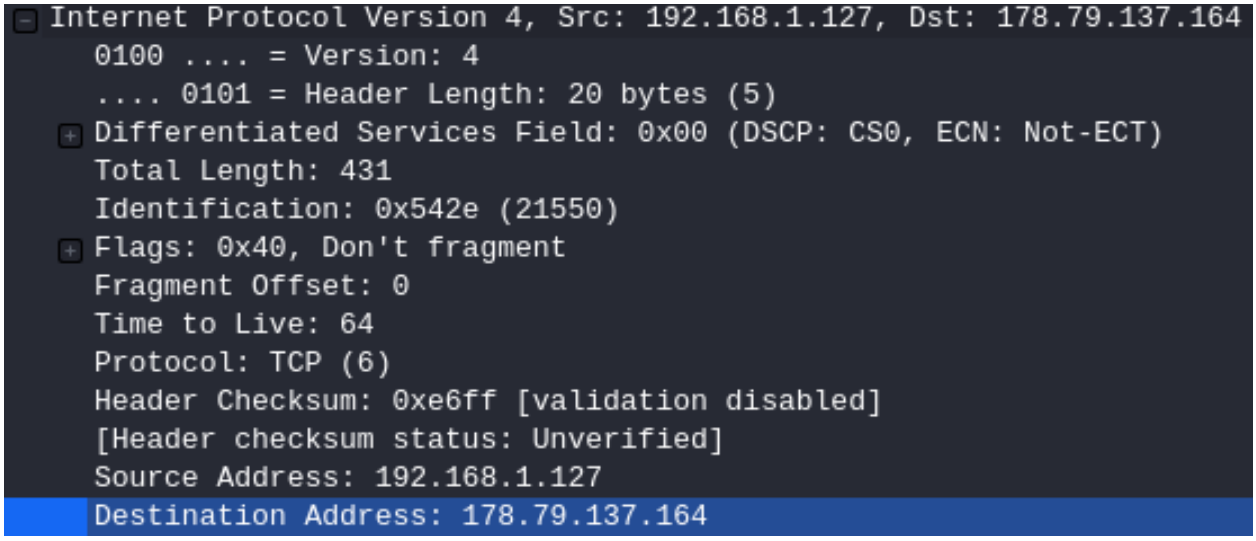
- 

- 

- 

- 

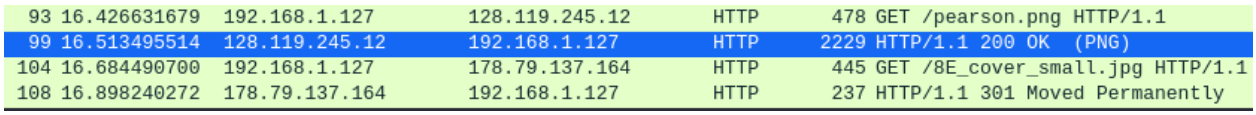
- 

- 

- 

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.

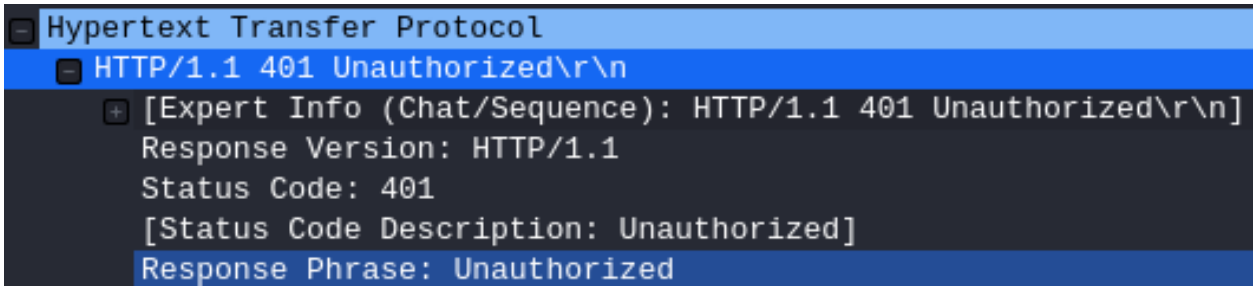
    - The images were downloaded serially. The last packet for `pearson.png` (packet 99) arrived before the GET request for `8E_cover_small.jpg` (packet 104) was sent.

- 

93	16.426631679	192.168.1.127	128.119.245.12	HTTP	478 GET /pearson.png HTTP/1.1
99	16.513495514	128.119.245.12	192.168.1.127	HTTP	2229 HTTP/1.1 200 OK (PNG)
104	16.684490700	192.168.1.127	178.79.137.164	HTTP	445 GET /8E_cover_small.jpg HTTP/1.1
108	16.898240272	178.79.137.164	192.168.1.127	HTTP	237 HTTP/1.1 301 Moved Permanently

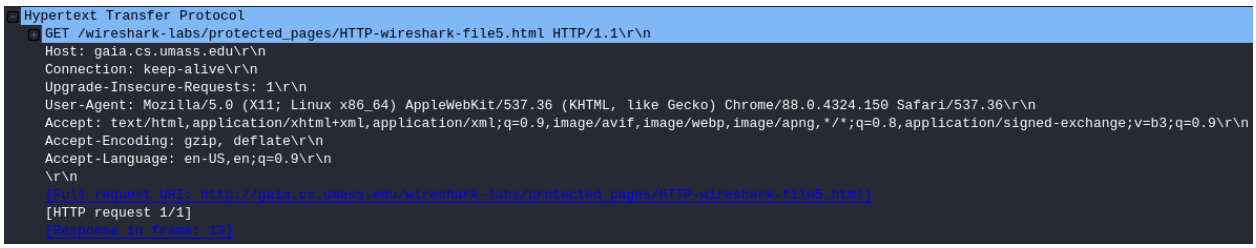
1.5 HTTP Authentication

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

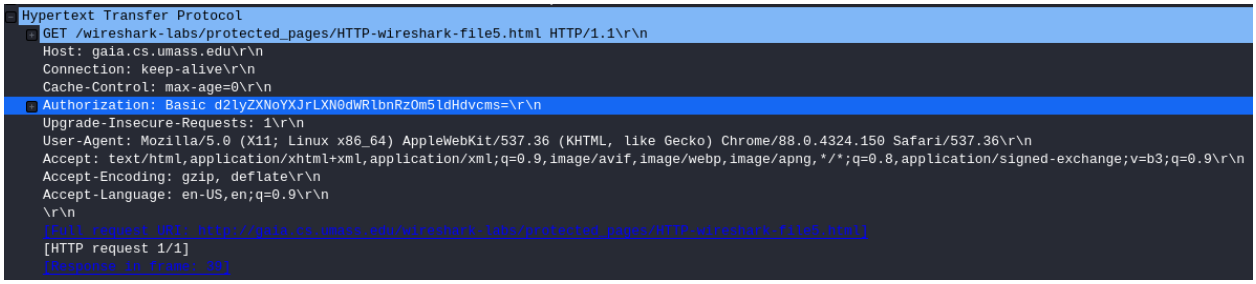
- The server responded with 401 and "Unauthorized".
- 

```
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
```

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

- The "Authorization" and "Cache-Control" fields are new.
- 

```
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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 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=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: 19]
```

- 

```
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
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 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=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: 28]
```