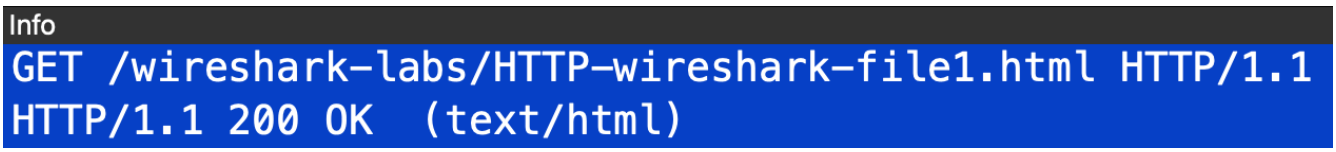
Student Information

Full Name : Mehmet Rüçhan Yavuzdemir
Id Number: 2522159

1 The Basic HTTP GET/response interaction

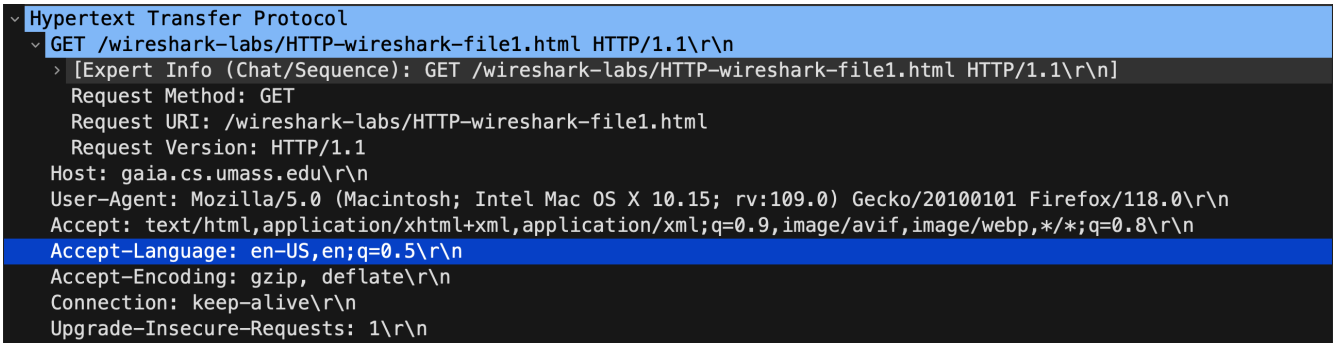
Answer 1

Both my browser, Firefox, and the server running HTTP/1.1. This is from the packet listing window, as shown below.



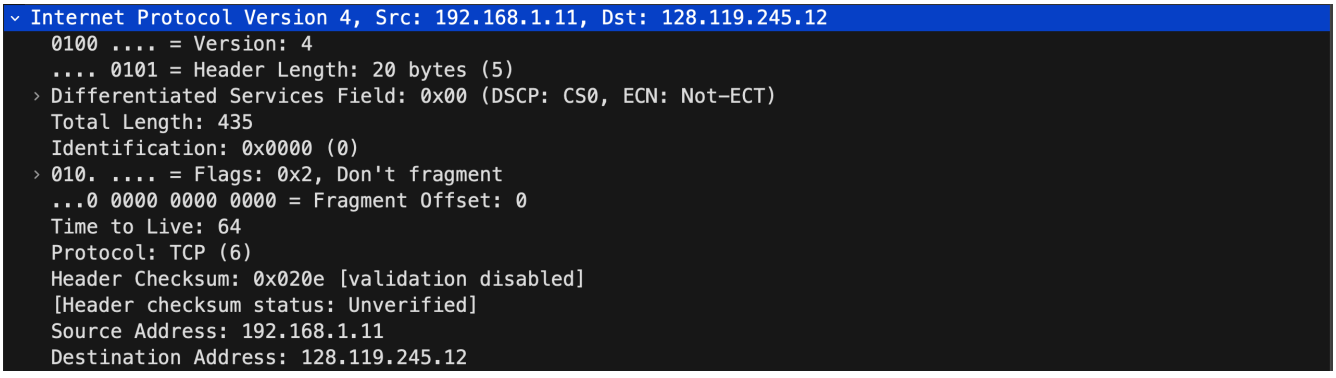
Answer 2

We should look at the HTTP GET request to see languages that our browser accepts. They are `en-US` and `en`.



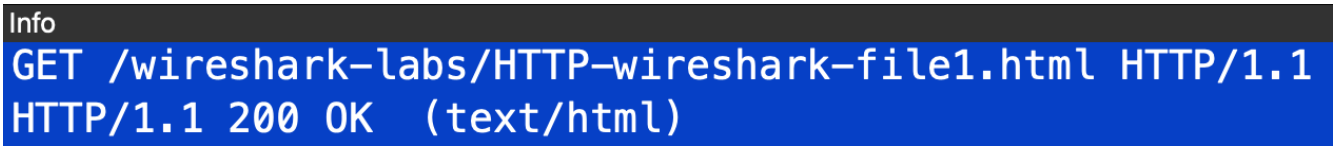
Answer 3

IP address information can be retrieved from the network layer. The IP address of my computer is `192.168.1.11` and the IP address of `gaia.cs.umass.edu` server is `128.119.245.12`.



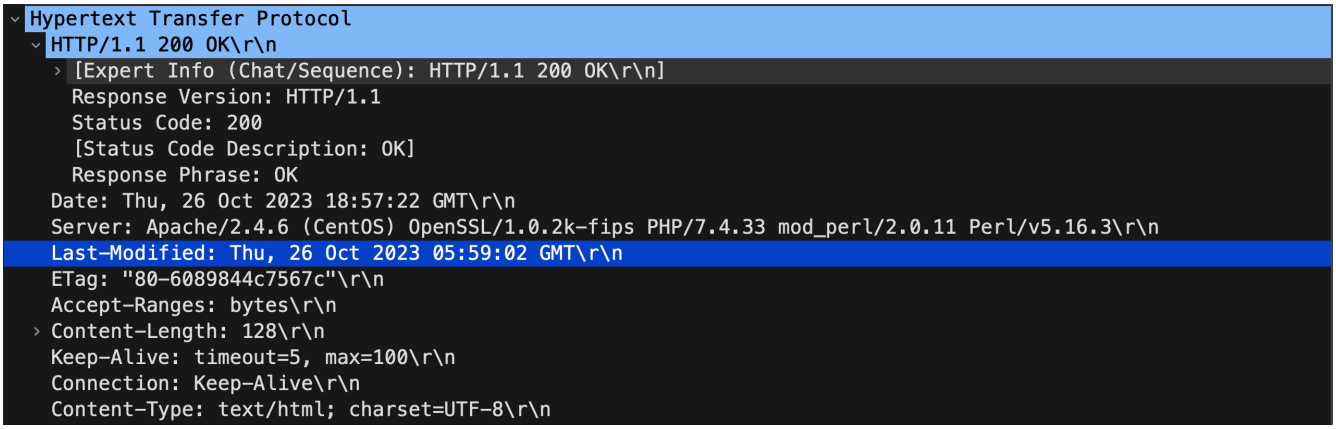
Answer 4

The status code returned from the server to my browser is `200 OK`.



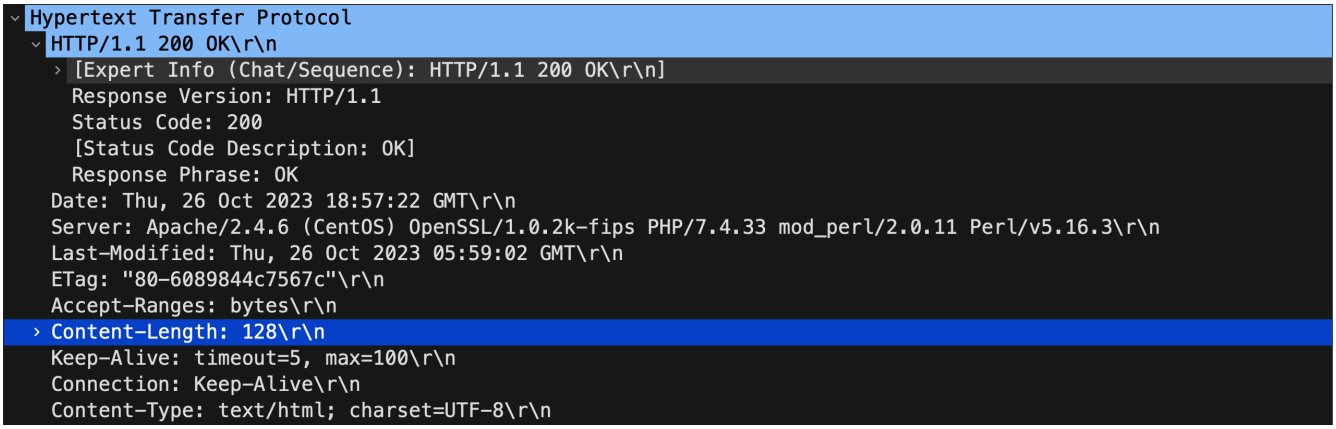
Answer 5

The retrieved HTML file is modified at the server on `Thu, 26 Oct 2023 05:59:02 GMT`, close to the time I sent the request.



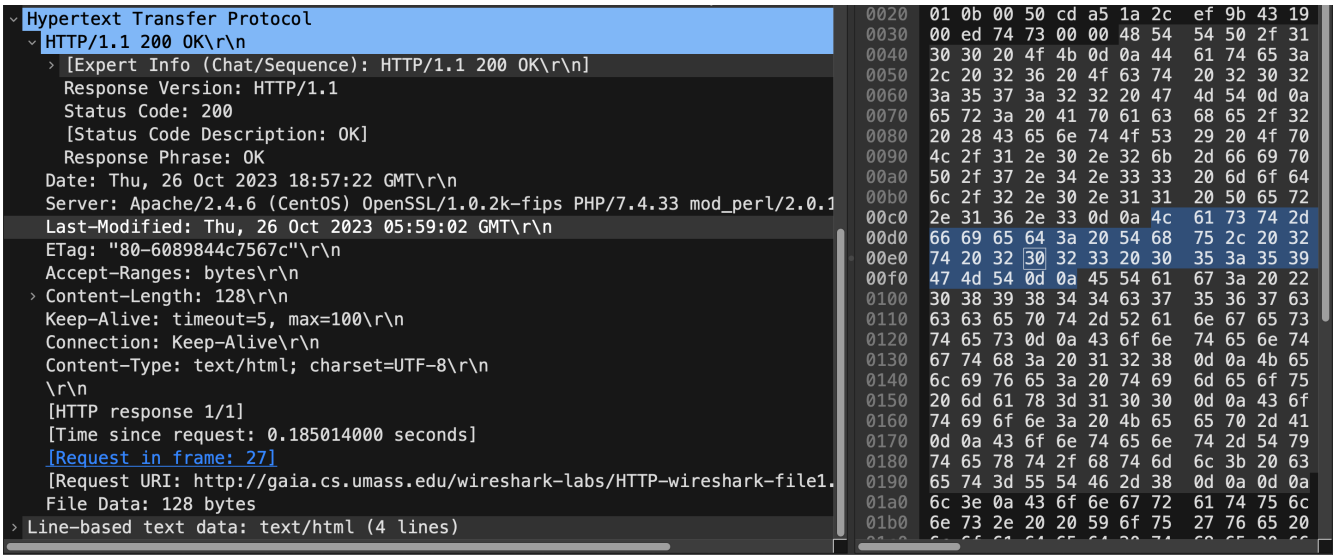
Answer 6

The content returned to my browser is 128 bytes, which is the `Content-Length`.



Answer 7

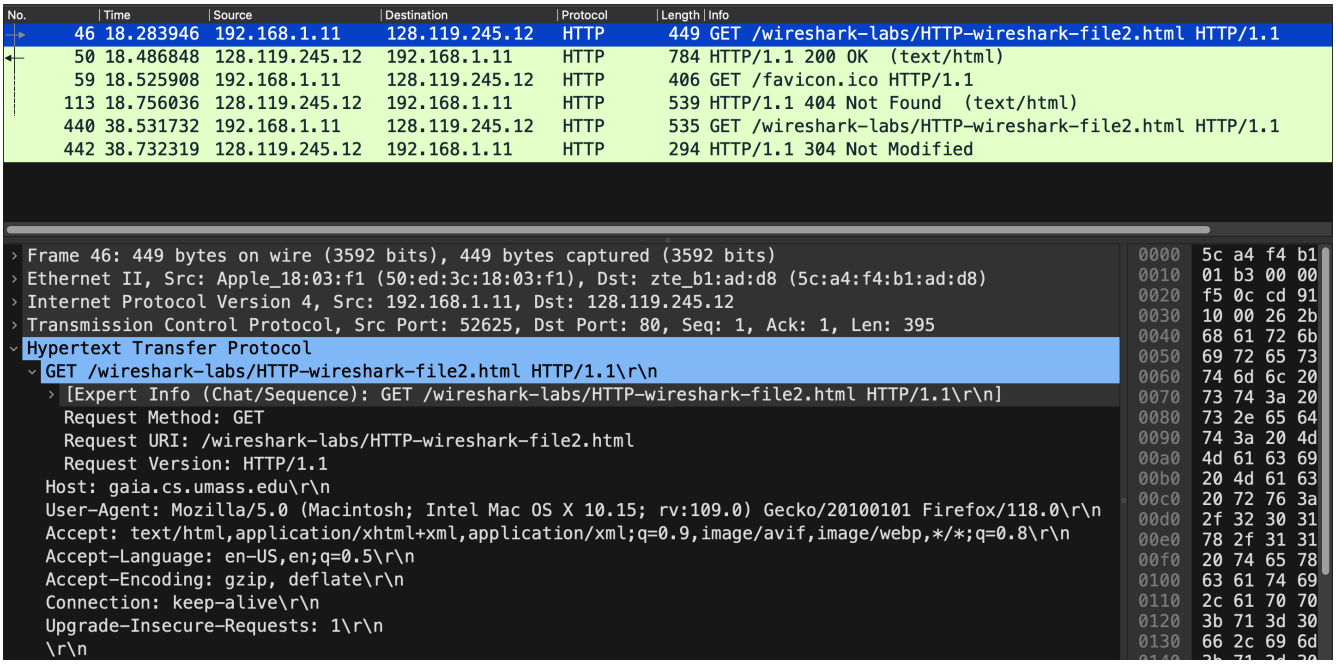
No, I do not see any single missing data. I examined the raw data, which is the actual bytes corresponding to the HTTP header and body information, and matched all the bytes with the corresponding headers. For example, I highlighted the raw data of the `Last-Modified` header information.



2 The HTTP CONDITIONAL GET/response interaction

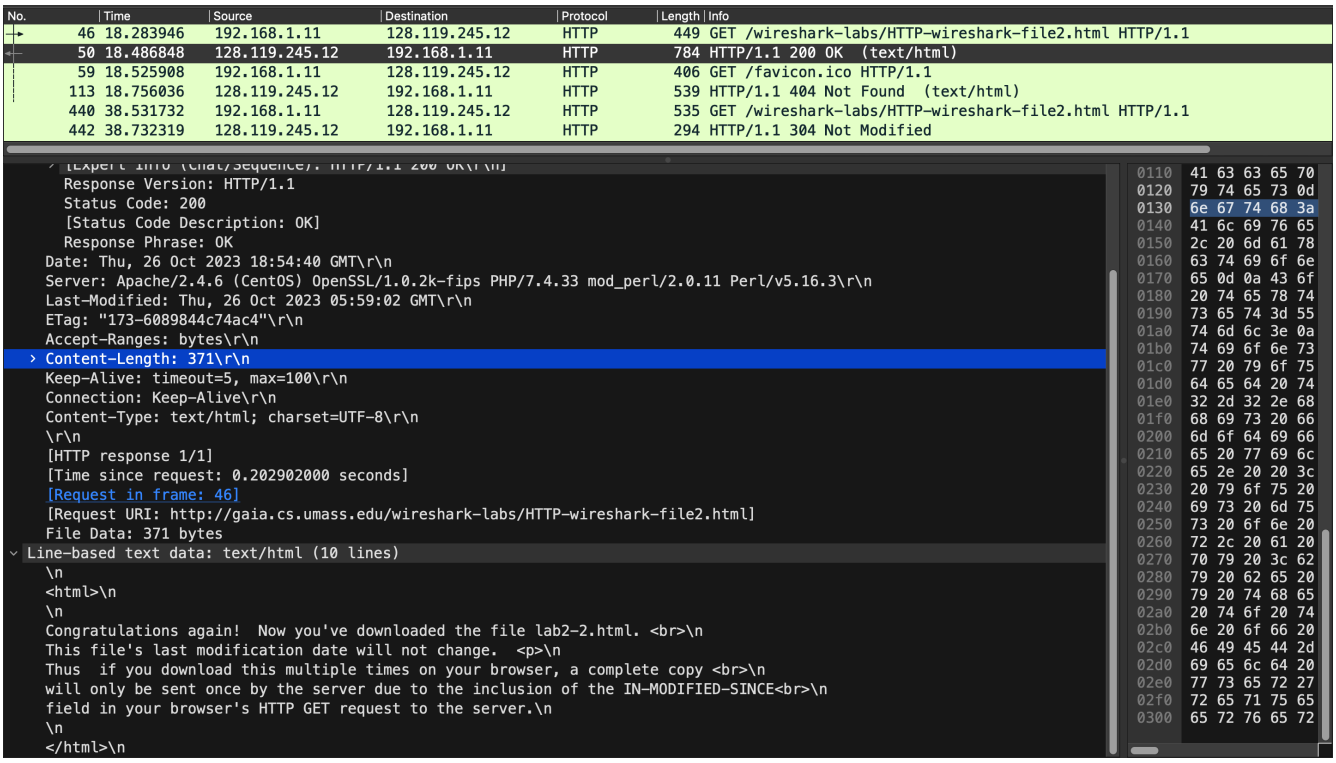
Answer 8

The HTTP GET request headers do not include `IF-MODIFIED-SINCE` header information since this is the first time sending the request. (The Google Chrome browser adds it the first time though, but my browser is Firefox)



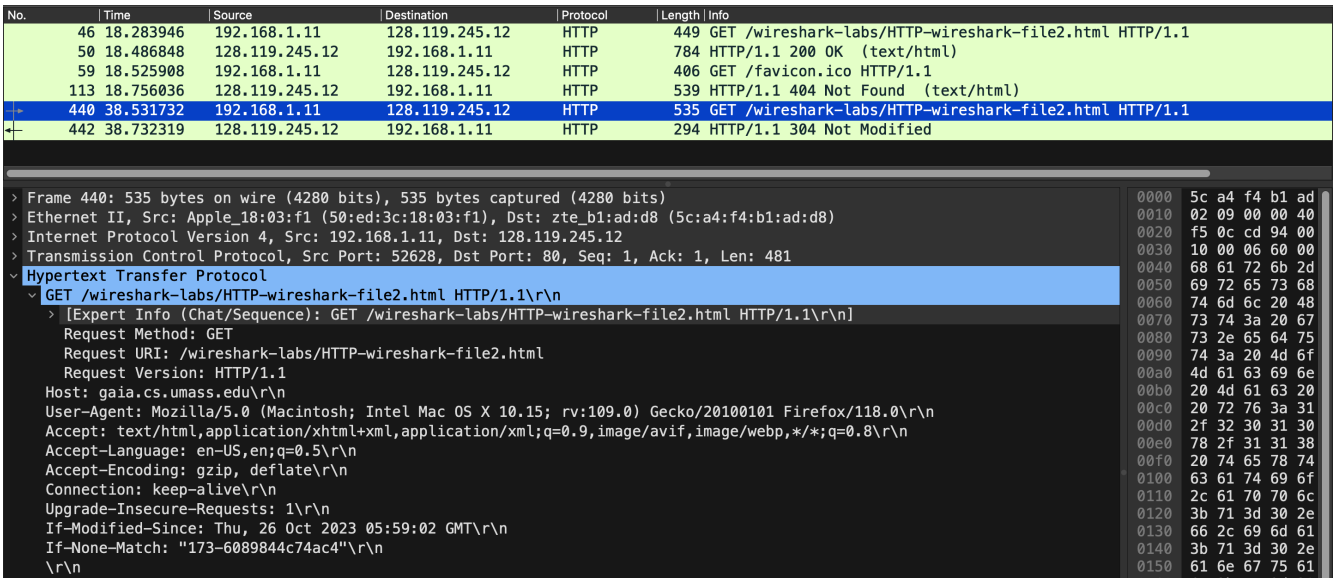
Answer 9

In the response, there are two pieces of evidence that show the server explicitly returned the contents of the file. First, `Content-Length` is 371 bytes, which means 371 bytes were sent. Second, we see `Line-based text data`, containing the corresponding HTML file. Hence, the server explicitly returned the contents of the file.



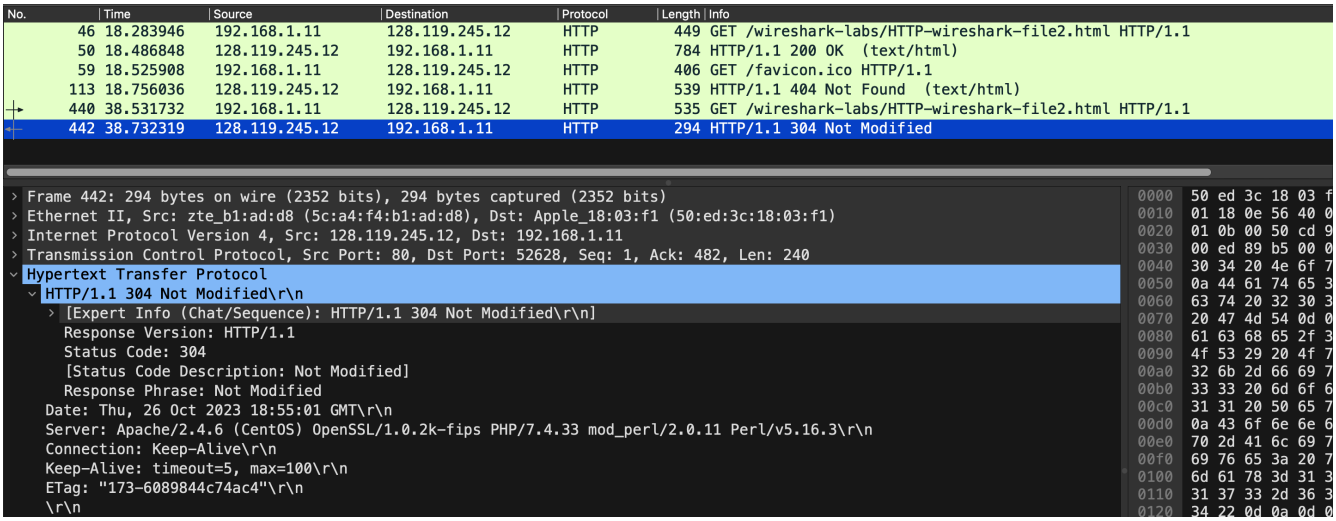
Answer 10

Yes, in the HTTP GET request, there is `If-Modified-Since` header information. It is a human-readable ASCII text containing the date and time, `Thu, 26 Oct 2023 05:59:02 GMT`.



Answer 11

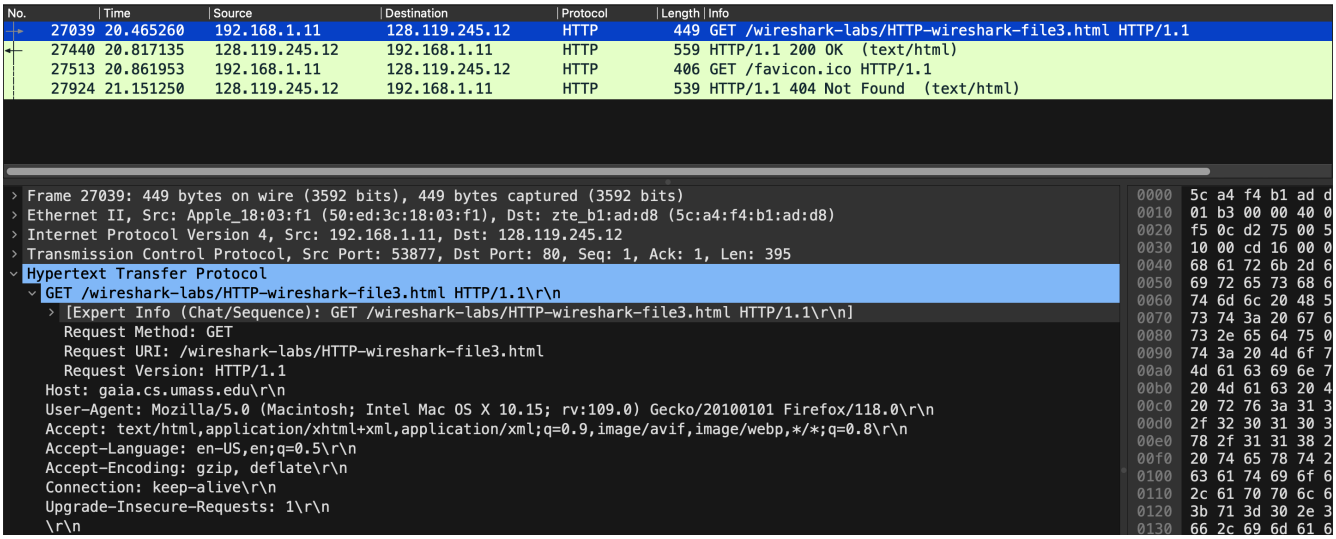
After sending the HTTP GET request a second time, the server returns `304 Not Modified`. Furthermore, it did not explicitly return the HTML file, because there is no `Content-Length` header information and `Line-based text data` appearing at the bottom of the screen.

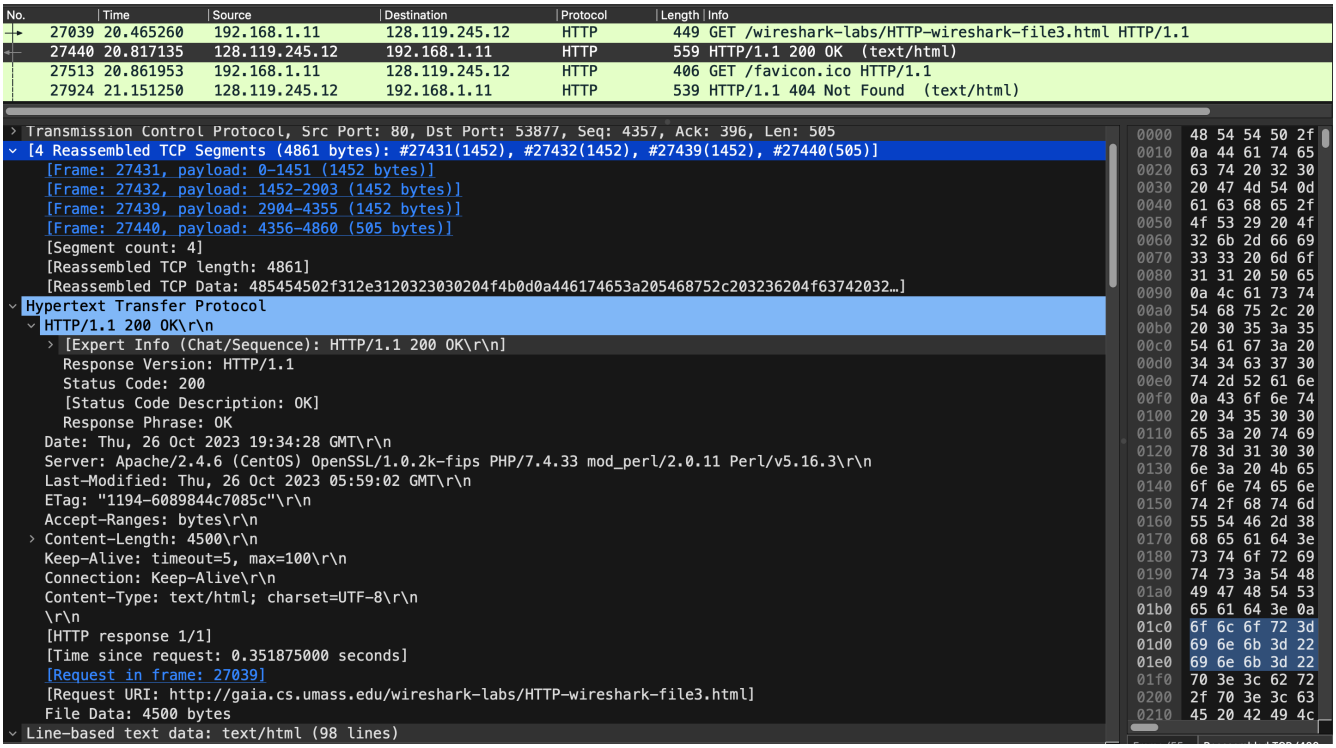


3 Retrieving Long Documents

Answer 12

My browser only sent one HTTP GET request with the packet number 27039. (actually, there is one more to favicon.ico, but in the lab manual, it is said that we can ignore it)





Answer 13

The packet with packet number 27440 contains the status code and the corresponding phrase associated with the response to the HTTP GET request.

Answer 14

The status code and the phrase in the response were `200 OK`.

Answer 15

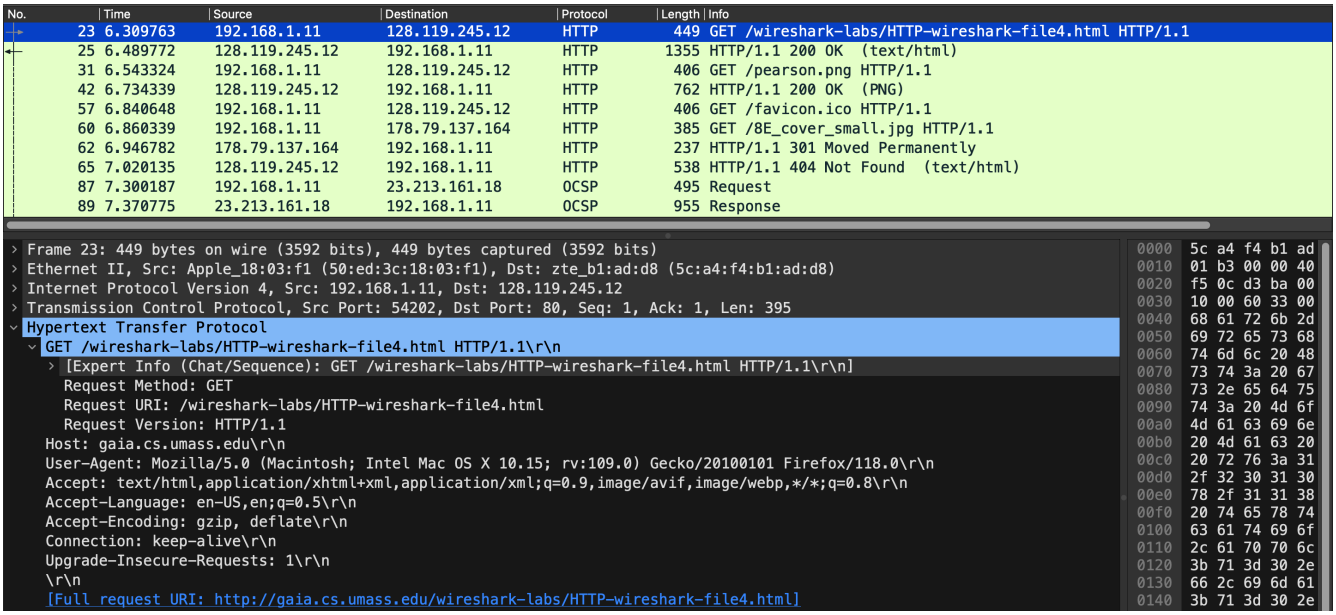
The text of the Bill of Rights did not fit into one TCP segment, hence **4** data-containing TCP segments were needed to carry this big HTTP response.

4 HTML Documents with Embedded Objects

Answer 16

If we again exclude the HTTP GET request to favicon.ico, there were **3** HTTP GET requests that my browser sent. These requests below were sent to these addresses respectively:

128.119.245.12 → `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html`
128.119.245.12 → `http://gaia.cs.umass.edu/pearson.png`
178.79.137.164 → `http://kurose.cslash.net/8E_cover_small.jpg`



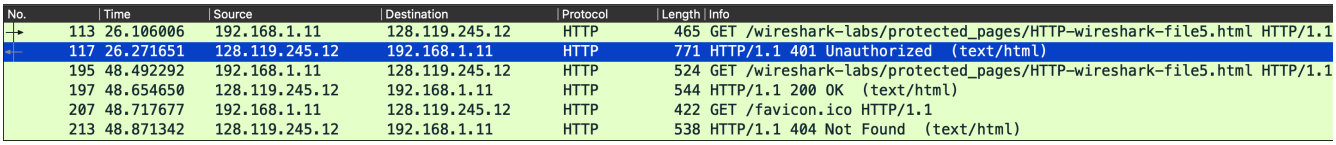
Answer 17

If we consider `Time` column in the packet-listing window, although I am not 100% sure if my browser downloaded these two images serially, it seems it downloaded serially because the second HTTP GET request for `8E_cover_small.jpg` was sent after the HTTP response for `pearson.png` arrived. On the other hand, even though we excluded favicon.ico HTTP requests and responses, it is also possible that the browser used parallel downloading in some cases because packet 62 including the HTTP response is not the response to packet 57 including the HTTP request. However, I am convinced that the browser downloaded the two images serially, as explained above.

5 HTTP Authentication

Answer 18

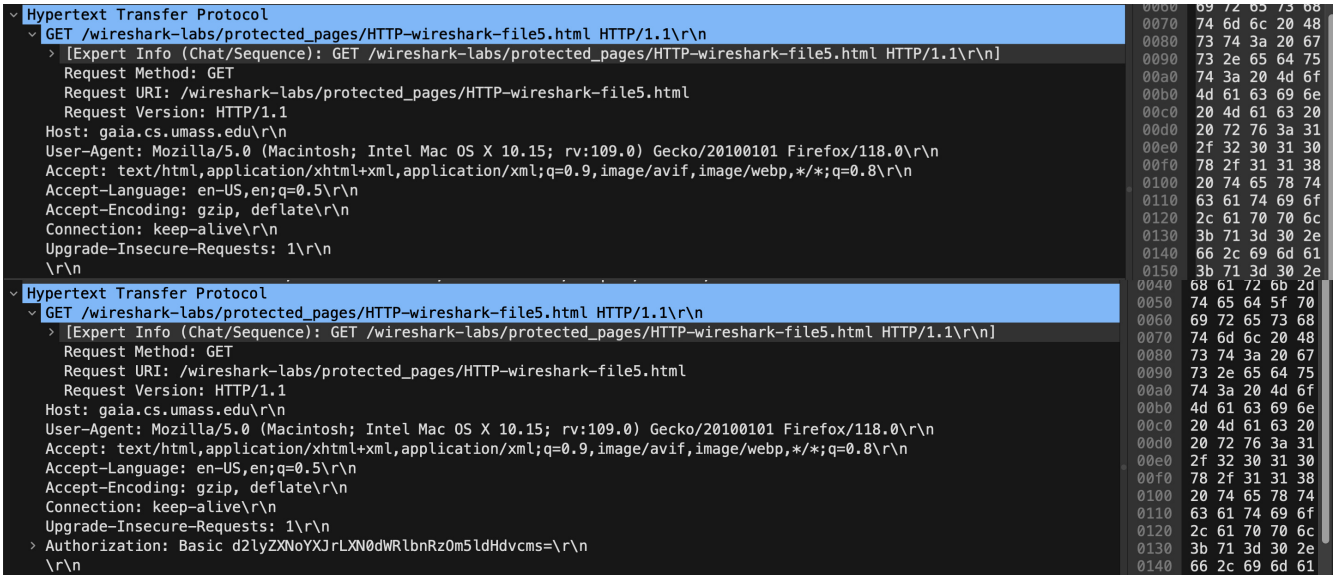
The server returns the status code and phrase `401 Unauthorized` to the initial HTTP GET request sent by the browser.



No.	Time	Source	Destination	Protocol	Length	Info
113	26.106006	192.168.1.11	128.119.245.12	HTTP	465	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
117	26.271651	128.119.245.12	192.168.1.11	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
195	48.492292	192.168.1.11	128.119.245.12	HTTP	524	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
197	48.654650	128.119.245.12	192.168.1.11	HTTP	544	HTTP/1.1 200 OK (text/html)
207	48.717677	192.168.1.11	128.119.245.12	HTTP	422	GET /favicon.ico HTTP/1.1
213	48.871342	128.119.245.12	192.168.1.11	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Answer 19

I merged two images so that you can see the difference very clearly. In the second HTTP GET request, `Authorization: Basic` header information was added as a new field.



```
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\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 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
  \r\n
```

```
0070  74 6d 6c 20 48
0080  73 74 3a 20 67
0090  73 2e 65 64 75
00a0  74 3a 20 4d 6f
00b0  4d 61 63 69 6e
00c0  20 4d 61 63 20
00d0  20 72 76 3a 31
00e0  2f 32 30 31 30
00f0  78 2f 31 31 38
0100  20 74 65 78 74
0110  63 61 74 69 6f
0120  2c 61 70 70 6c
0130  3b 71 3d 30 2e
0140  66 2c 69 6d 61
0150  3b 71 3d 30 2e
```

```
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\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 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
> Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  \r\n
```

```
0040  68 61 72 6b 2d
0050  74 65 64 5f 70
0060  69 72 65 73 68
0070  74 6d 6c 20 48
0080  73 74 3a 20 67
0090  73 2e 65 64 75
00a0  74 3a 20 4d 6f
00b0  4d 61 63 69 6e
00c0  20 4d 61 63 20
00d0  20 72 76 3a 31
00e0  2f 32 30 31 30
00f0  78 2f 31 31 38
0100  20 74 65 78 74
0110  63 61 74 69 6f
0120  2c 61 70 70 6c
0130  3b 71 3d 30 2e
0140  66 2c 69 6d 61
```