Wireshark Lab: HTTP v6.1

Vandré Leal Cândido

August 20, 2017

1 The Basic HTTP GET/response interaction

Figure 1: Request (Section 1)

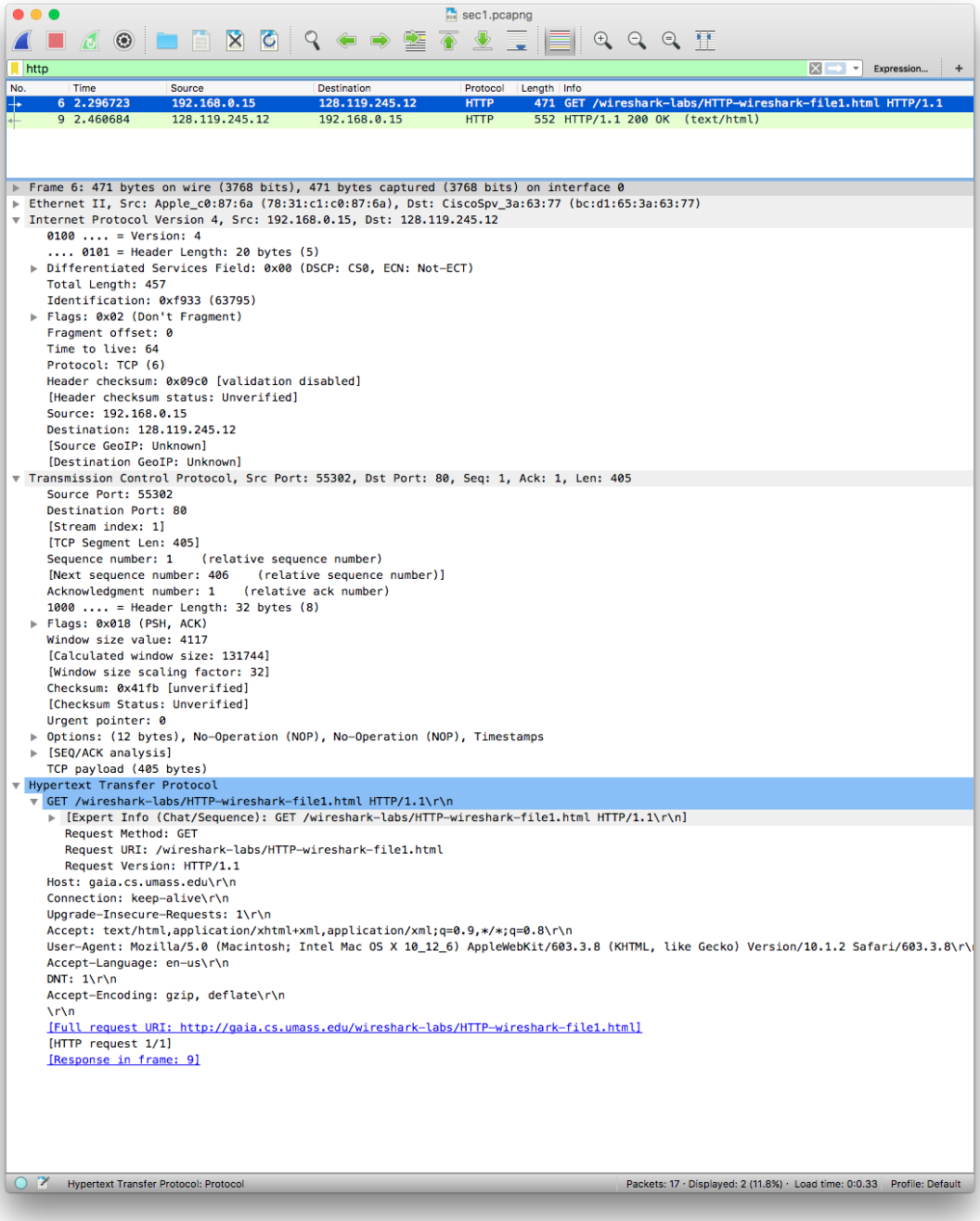
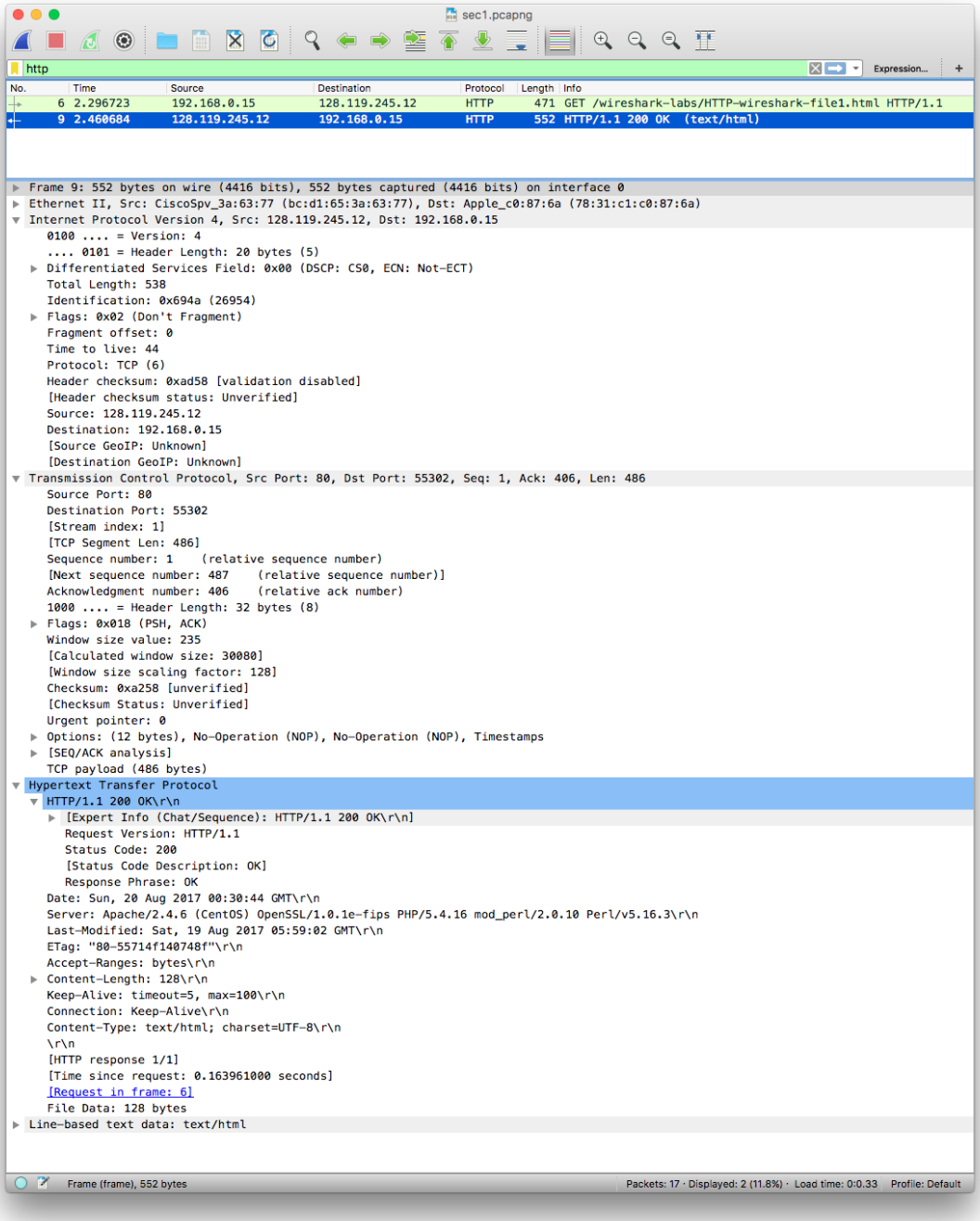


Figure 2: Response (Section 1)



- *Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?*

  Both browser and server use HTTP version 1.1.

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

  Only US English. [Accept-Language: en-us]

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

  Local IP address: 192.168.0.15 / gaia.cs.umass.edu: 128.119.245.12.

- *What is the status code returned from the server to your browser?*

  The status code returned is 200 [OK].

- *When was the HTML file that you are retrieving last modified at the server?*

  The HTML file was Last-Modified: Sat, 19 Aug 2017 05:59:02 GMT.

- *How many bytes of content are being returned to your browser?*

  128 bytes of content are being returned. [Content-Length: 128]

- *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.*

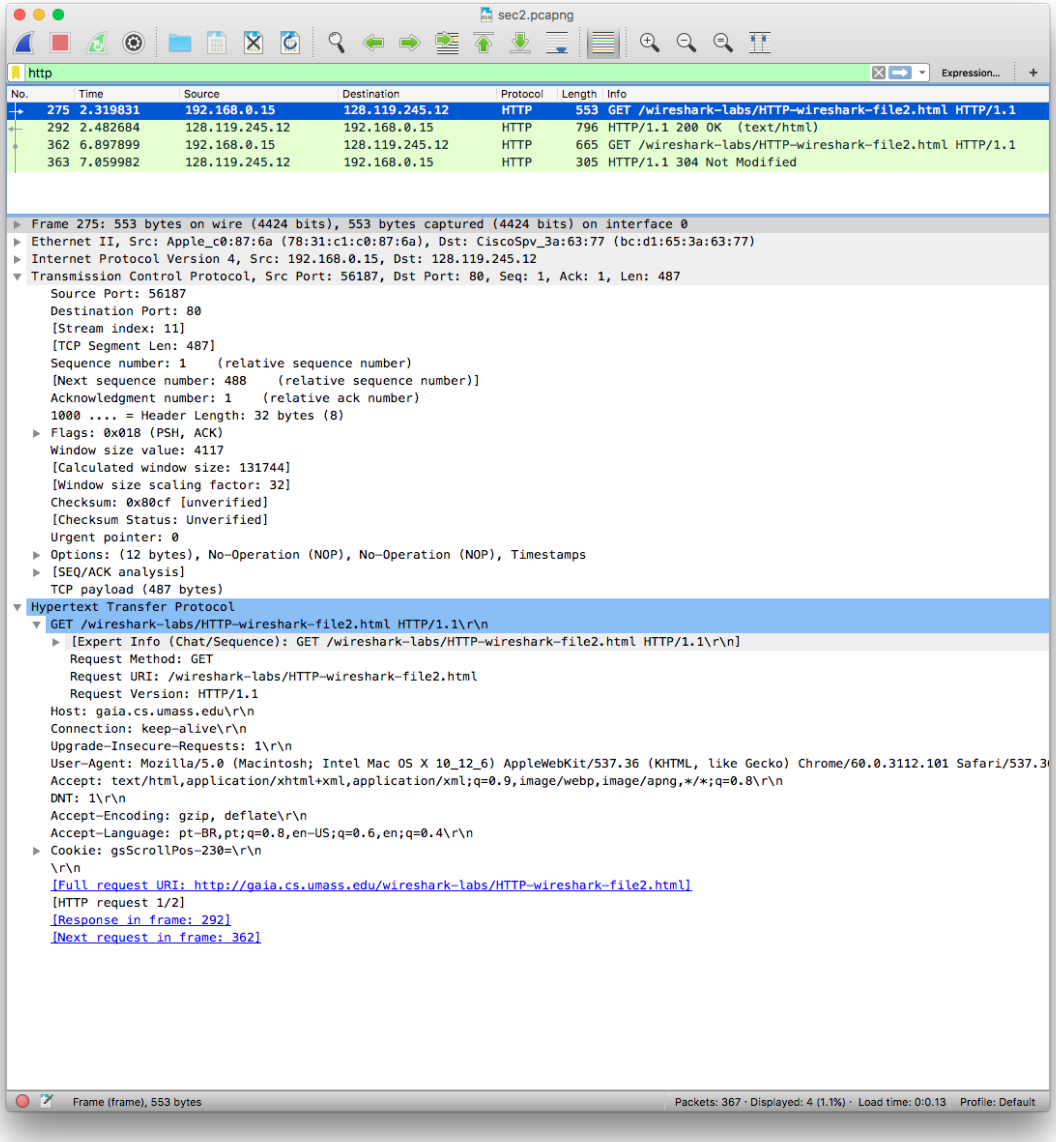
  No, all headers can be found in the raw data.

2 The HTTP CONDITIONAL GET/response interaction

- *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, there isn't an "IF-MODIFIED-SINCE" line in the first HTTP GET.

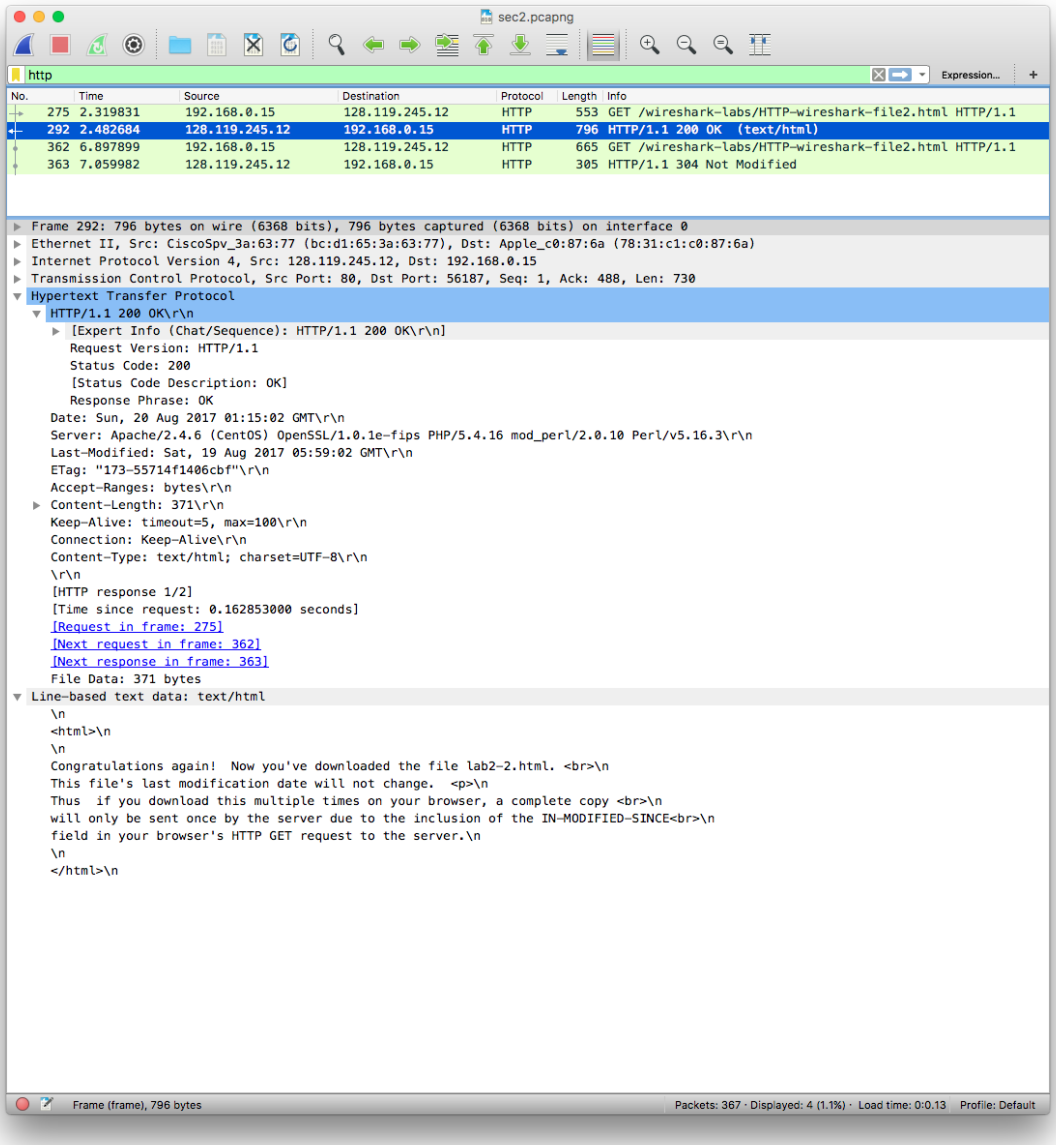
Figure 3: First Request (Section 2)



- *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 HTML file. The content is included in 'Line-based text data: text/html'.

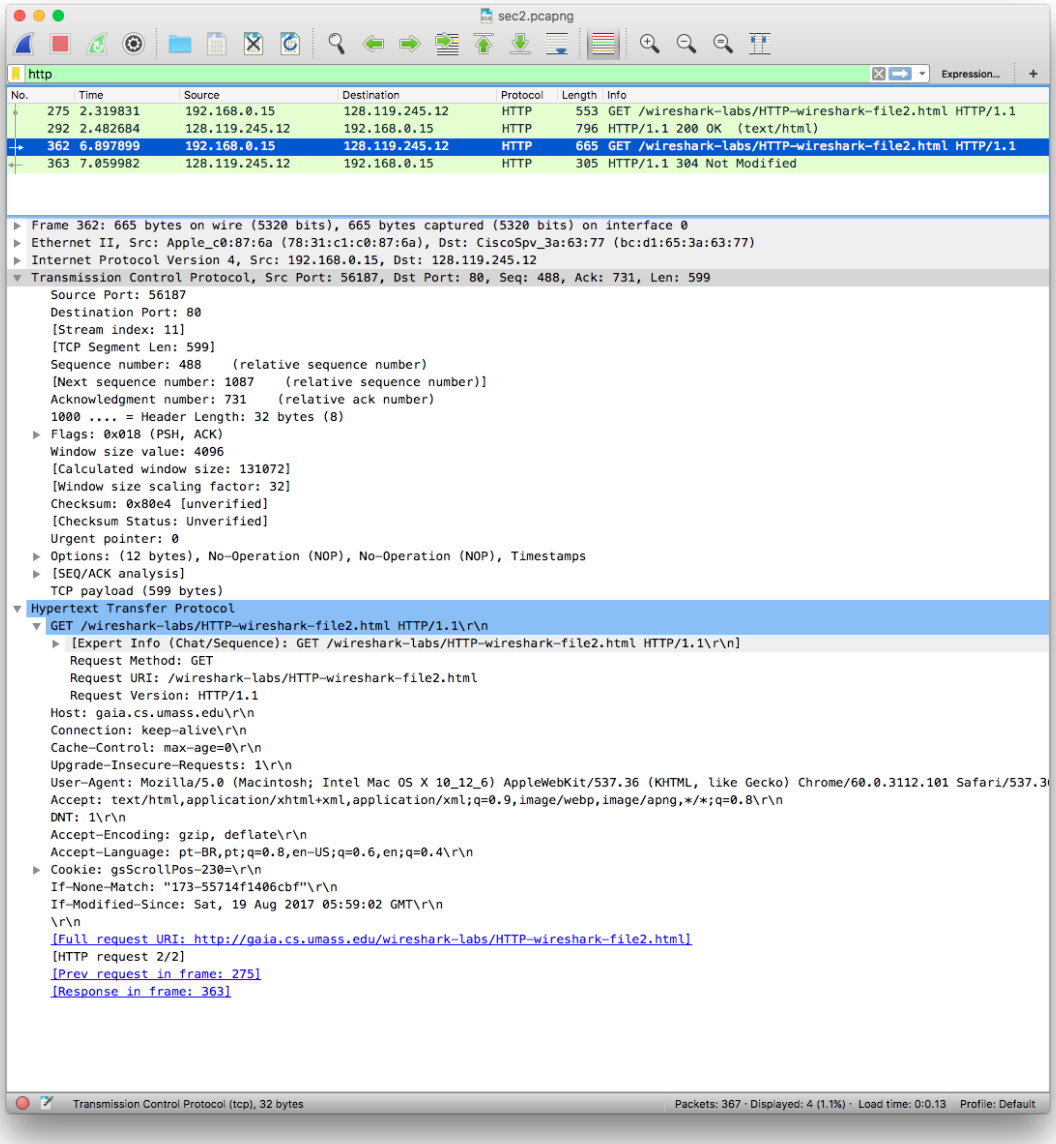
Figure 4: First Response (Section 2)



- *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, the information that followed the "IF-MODIFIED-SINCE:" header was the data it was modified 'If-Modified-Since: Sat, 19 Aug 2017 05:59:02 GMT'.

Figure 5: Second Request (Section 2)

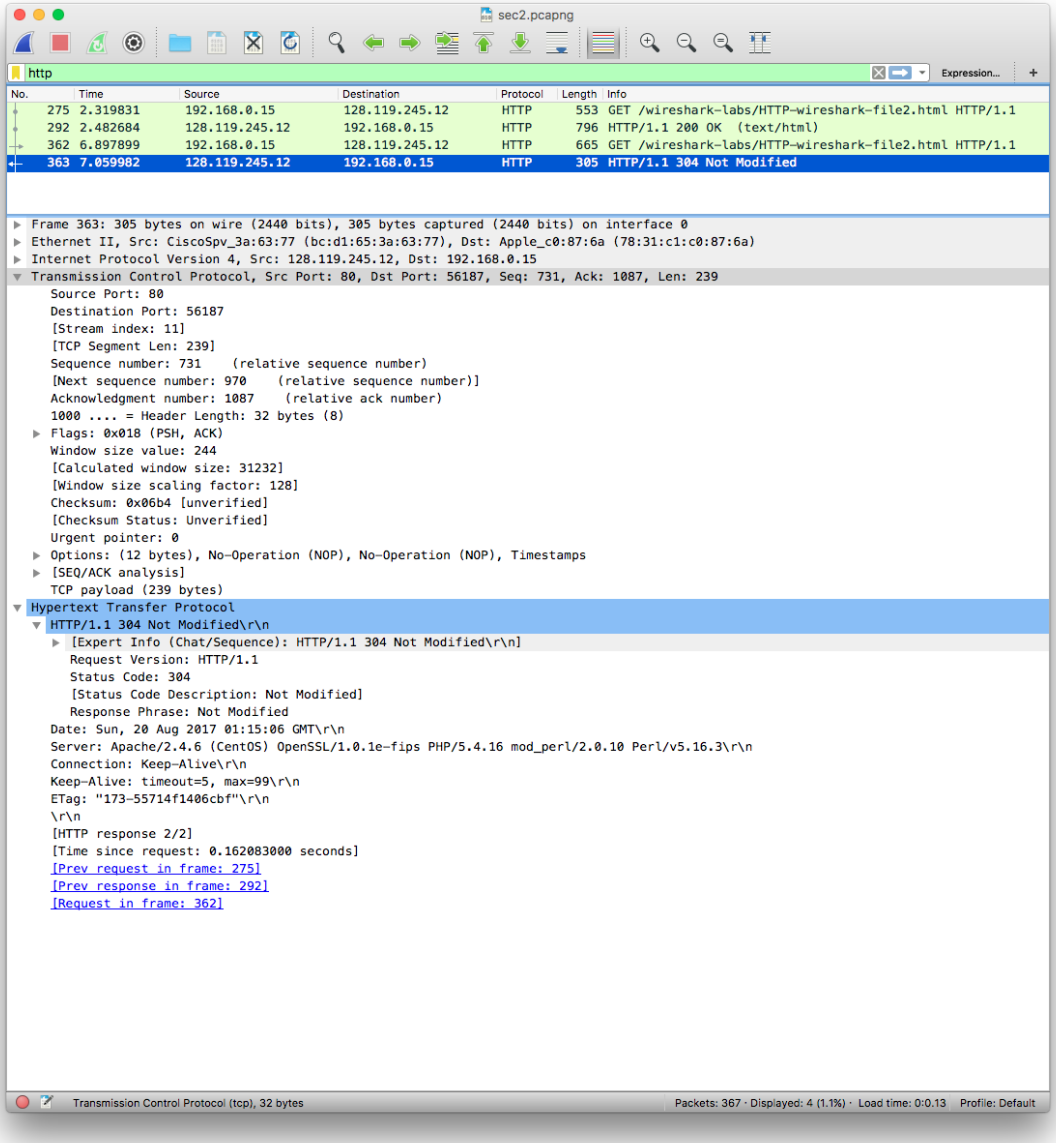


- *What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.*

  Status Code: 304 [Status Code Description: Not Modified]

  The server doesn't return the contents of the file because the information was previously cached by the browser after the first request.

Figure 6: Second Response (Section 2)



3 Retrieving Long Documents

Figure 7: Request (Section 3)

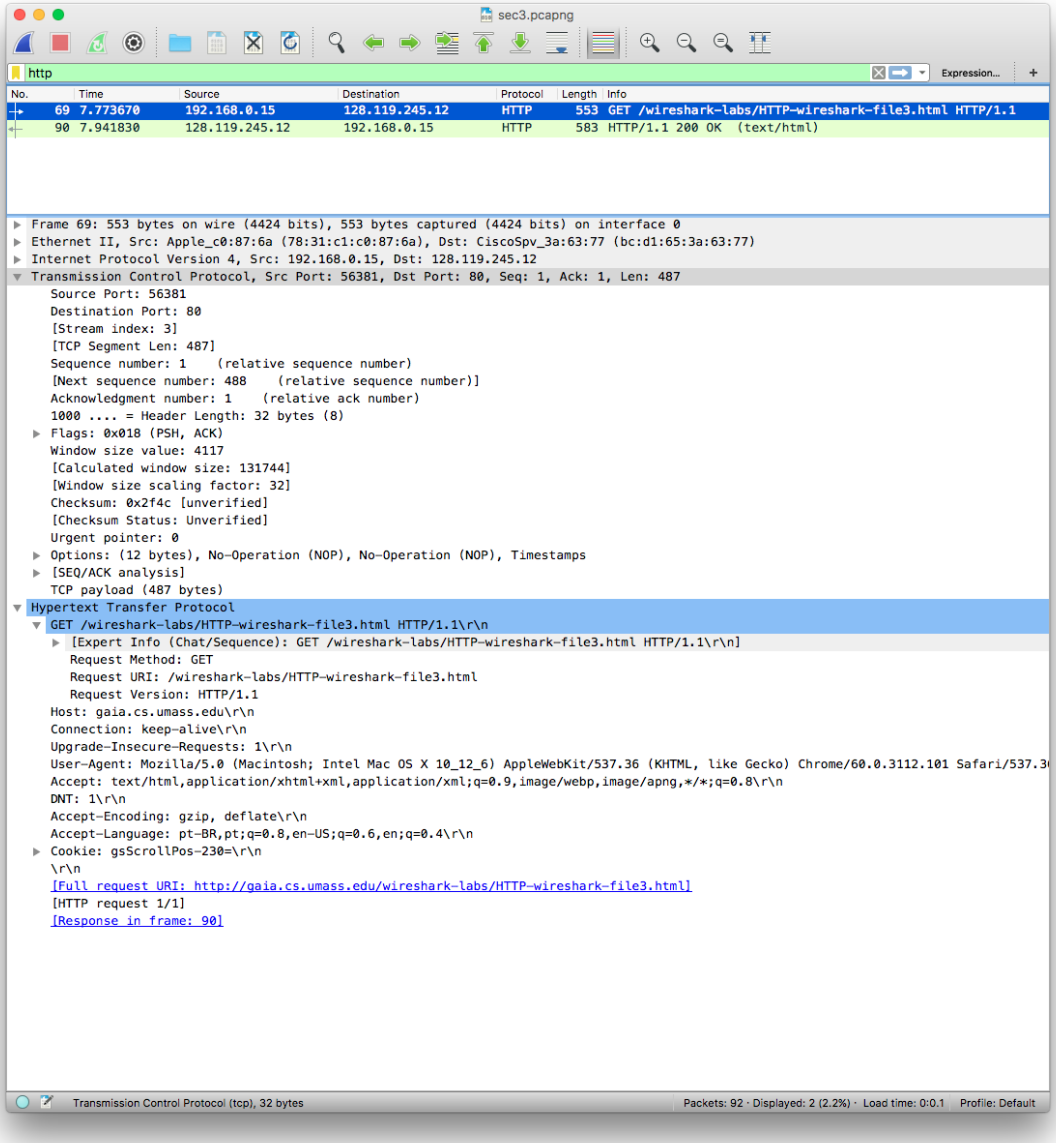
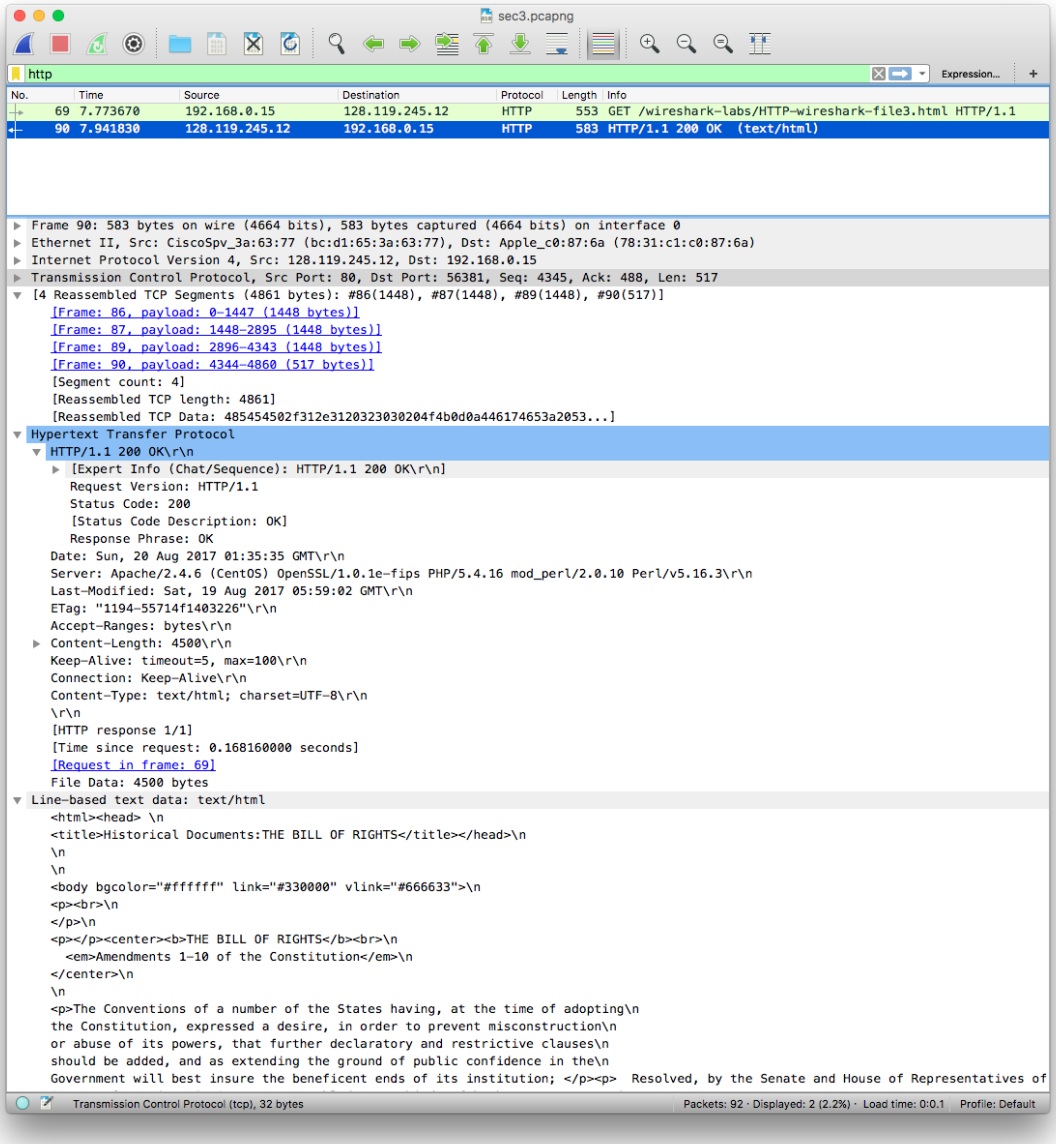


Figure 8: Response (Section 3)



- *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?*

  A single HTTP GET request was sent. Packet number 69 contained the GET message for the Bill of Rights.

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

  Packet number 90 contained the response to the request.

- *What is the status code and phrase in the response?*

  Status Code: 200 [Status Code Description: OK]

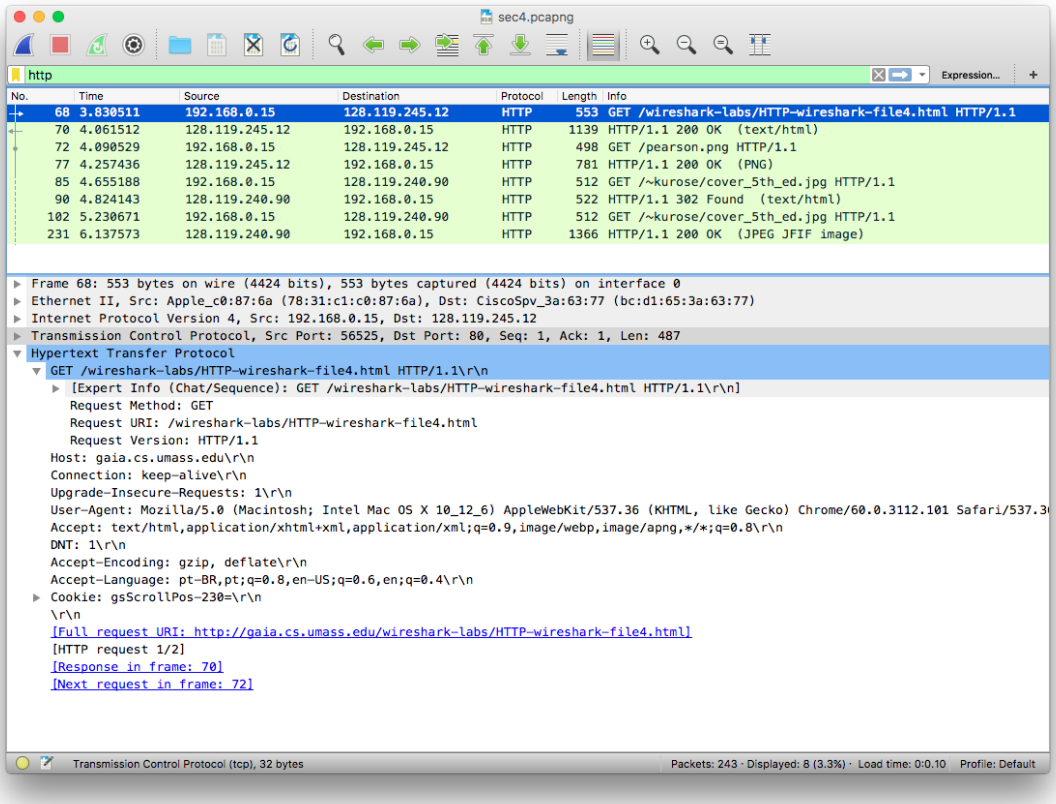
  Response Phrase: OK

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

  4 TCP segments were needed to carry the HTTP response.

4 HTML Documents with Embedded Objects

Figure 9: Request (Section 4)



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

  4 HTTP GET requests were sent. Each one of the following addresses received two GET requests: 128.119.245.12 and 128.119.240.90.

- *Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.*

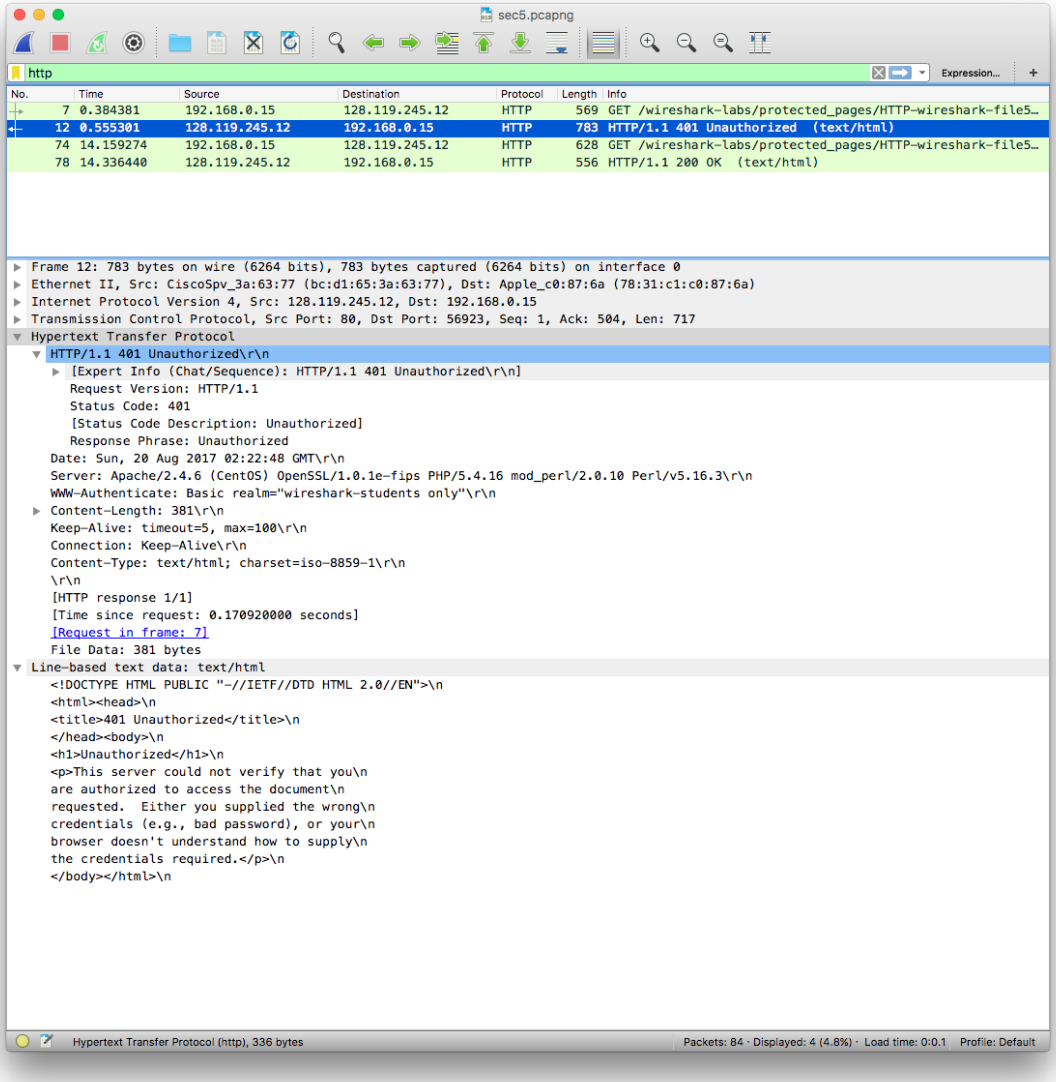
  The browser downloaded them serially because each request received a response before a new request was made.

5 HTTP Authentication

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

  Status Code: 401 - Response Phrase: Unauthorized

Figure 10: First Response (Section 5)



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

  'Authorization' is the new field included. This new field provides the credentials (username and password).

Figure 11: Second Request (Section 5)