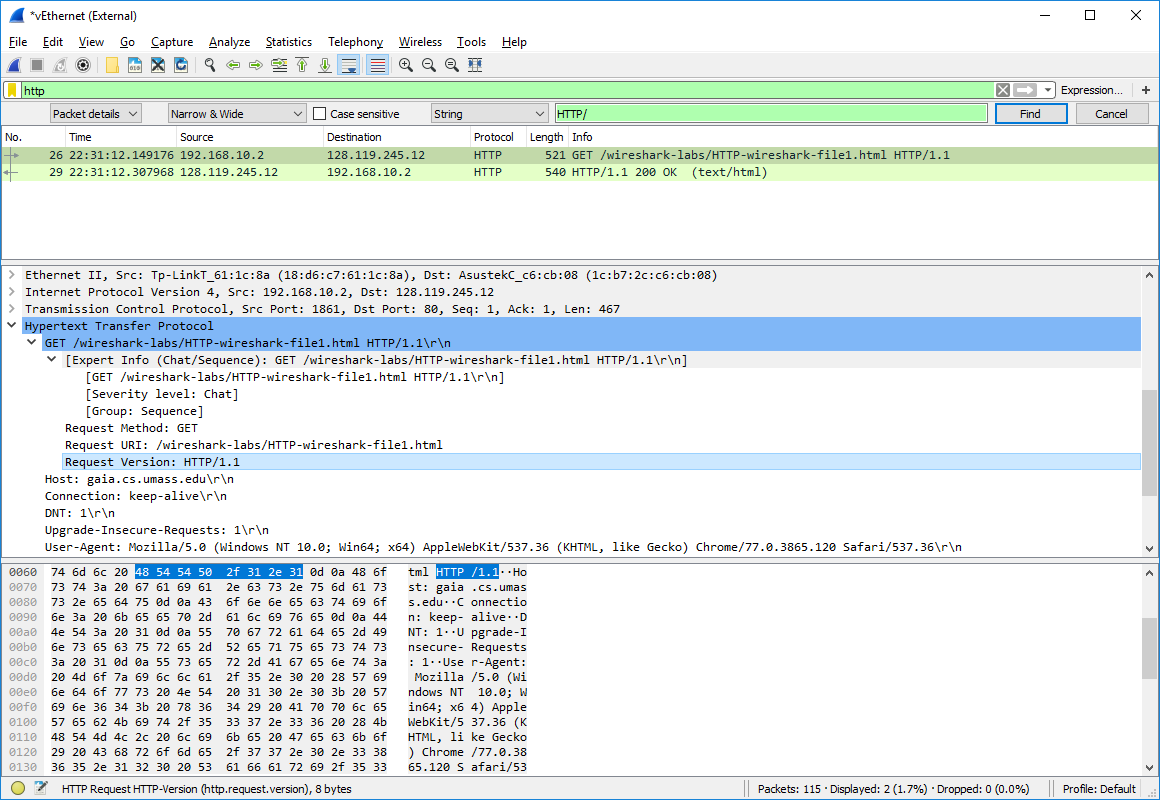
|  |  |
| --- | --- |
| CS372-400 | Edmund Dea |
| 10/13/2019 | ID# 933280343 |

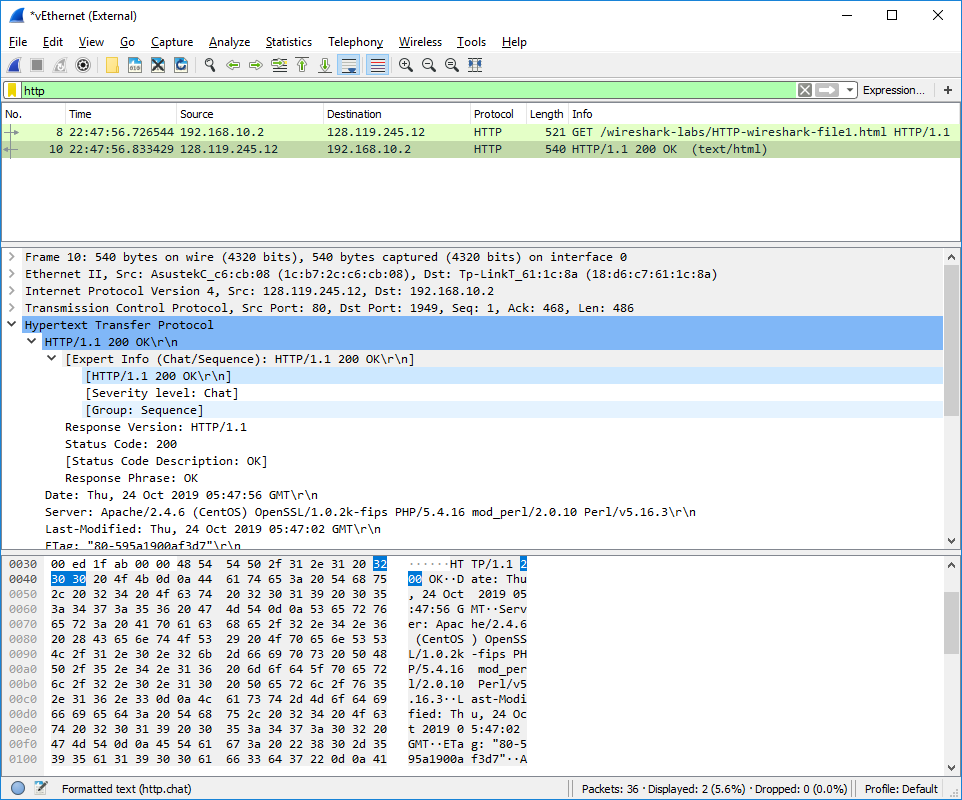
**Lab 2: Wireshark**

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 1.1.

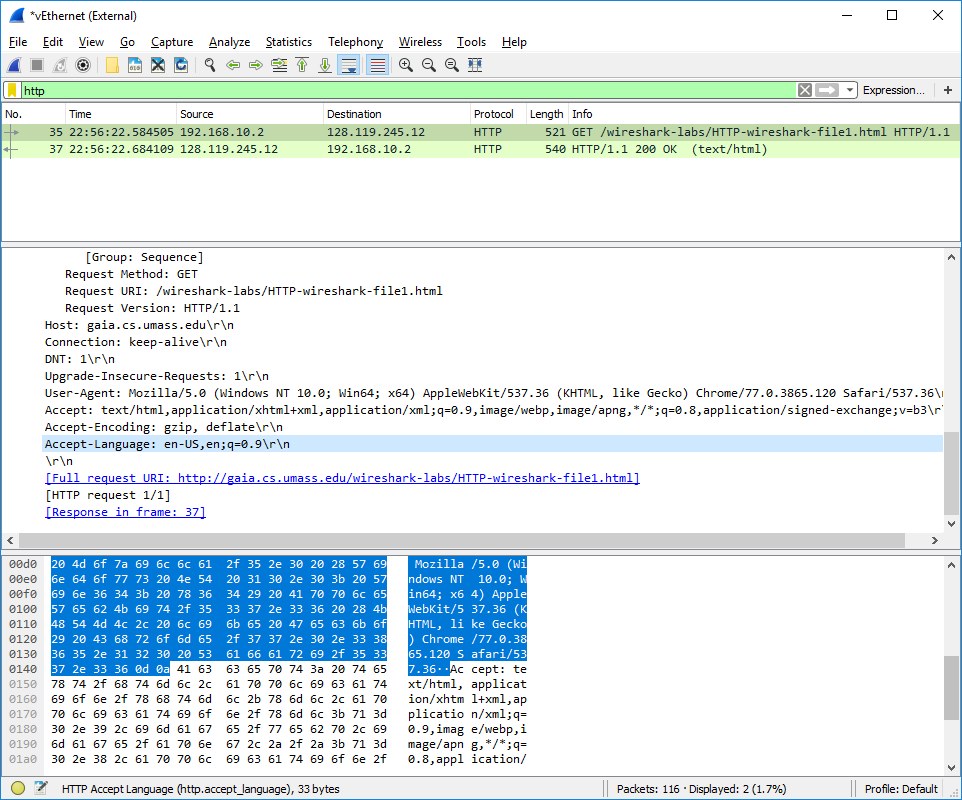


The server is also running HTTP 1.1.



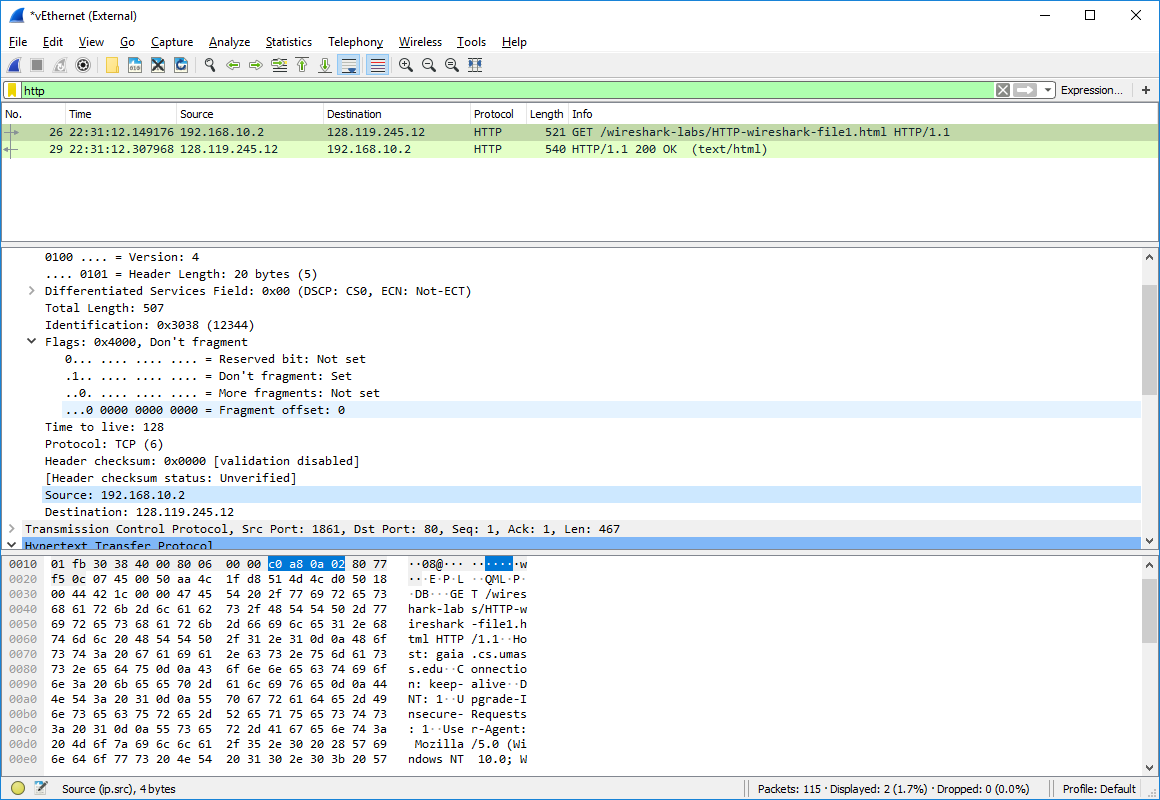
1. What languages (if any) does your browser indicate that it can accept to the server?

My browser indicates that it can accept “en-US, en; q=0.9\r\n”, which means that my browser can accept English US or English language with a q-factor weighting of 0.9.



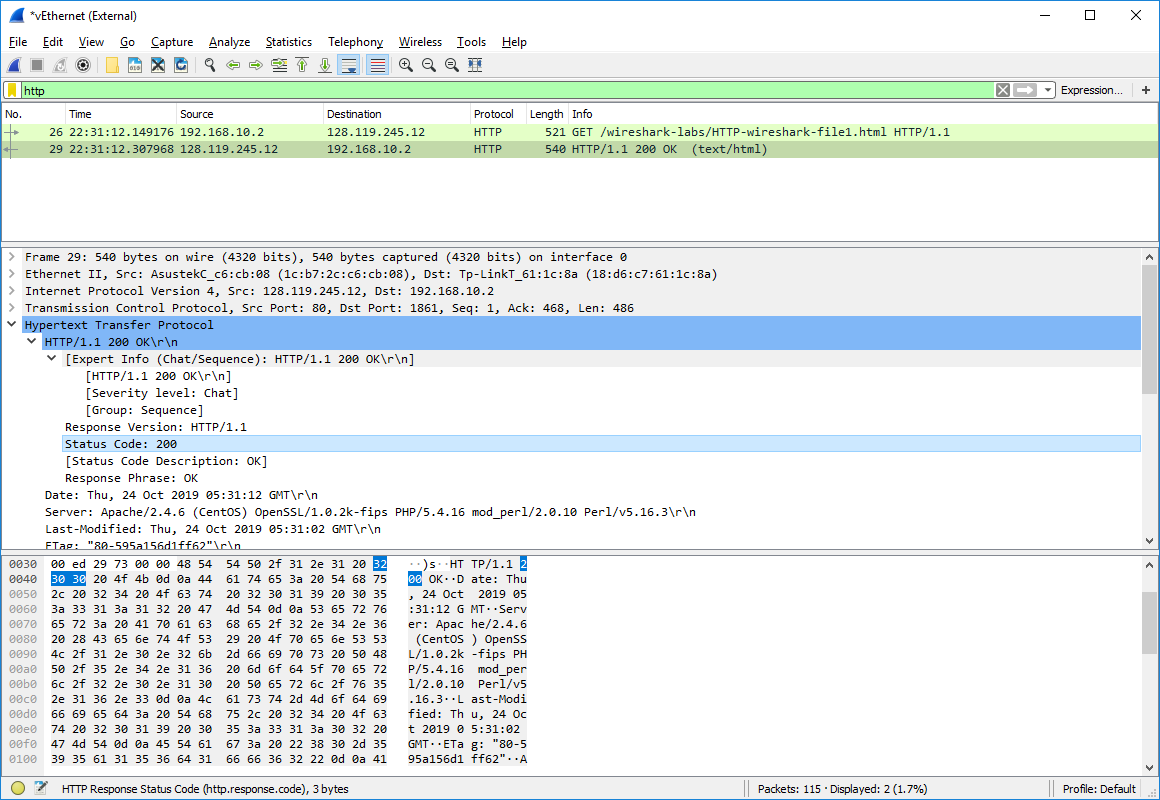
1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

The IP address of my computer is 192.168.10.2, which is the source address. The IP address of gaia.cs.umass.edu is 128.119.245.12, which is the destination address.



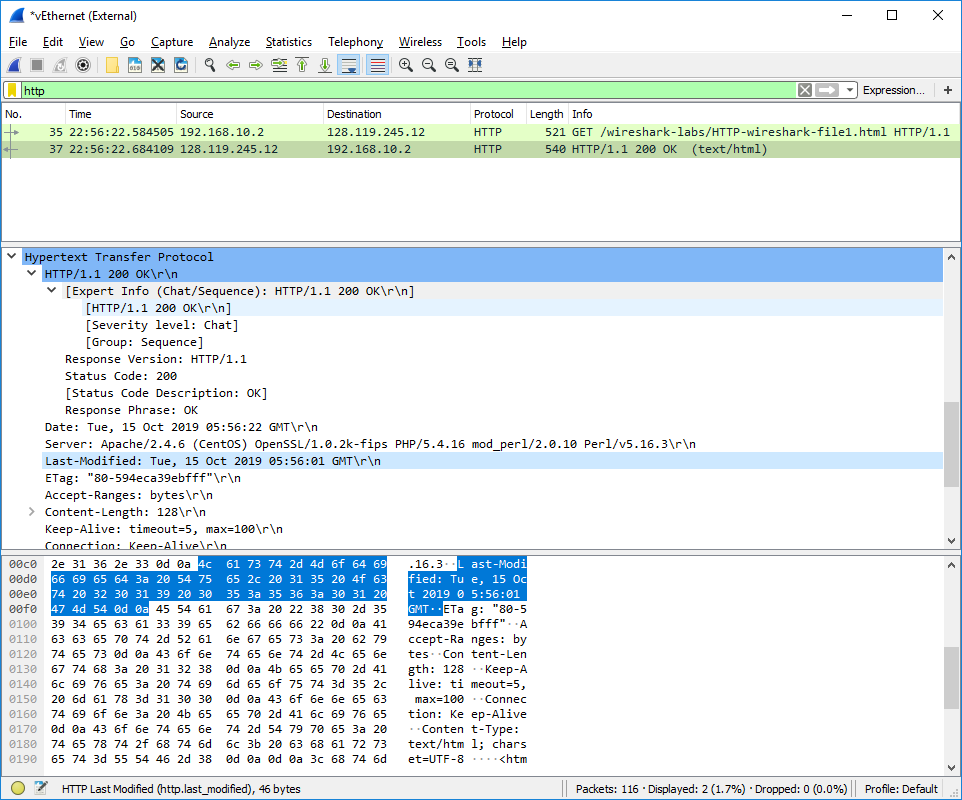
1. What is the status code returned from the server to your browser?

Status code 200 OK was returned from the server to my browser.



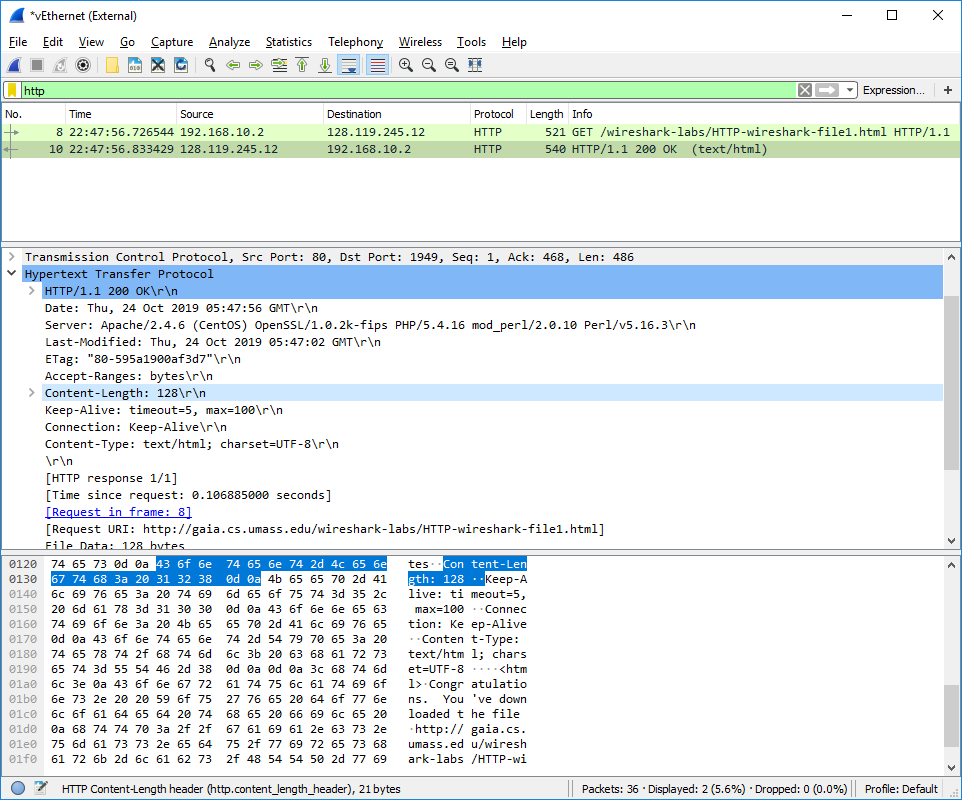
1. When was the HTML file that you are retrieving last modified at the server?

The HTML file that I am retrieving was last modified at the server on “Tue, 15 Oct 2019 05:56:01 GMT”.



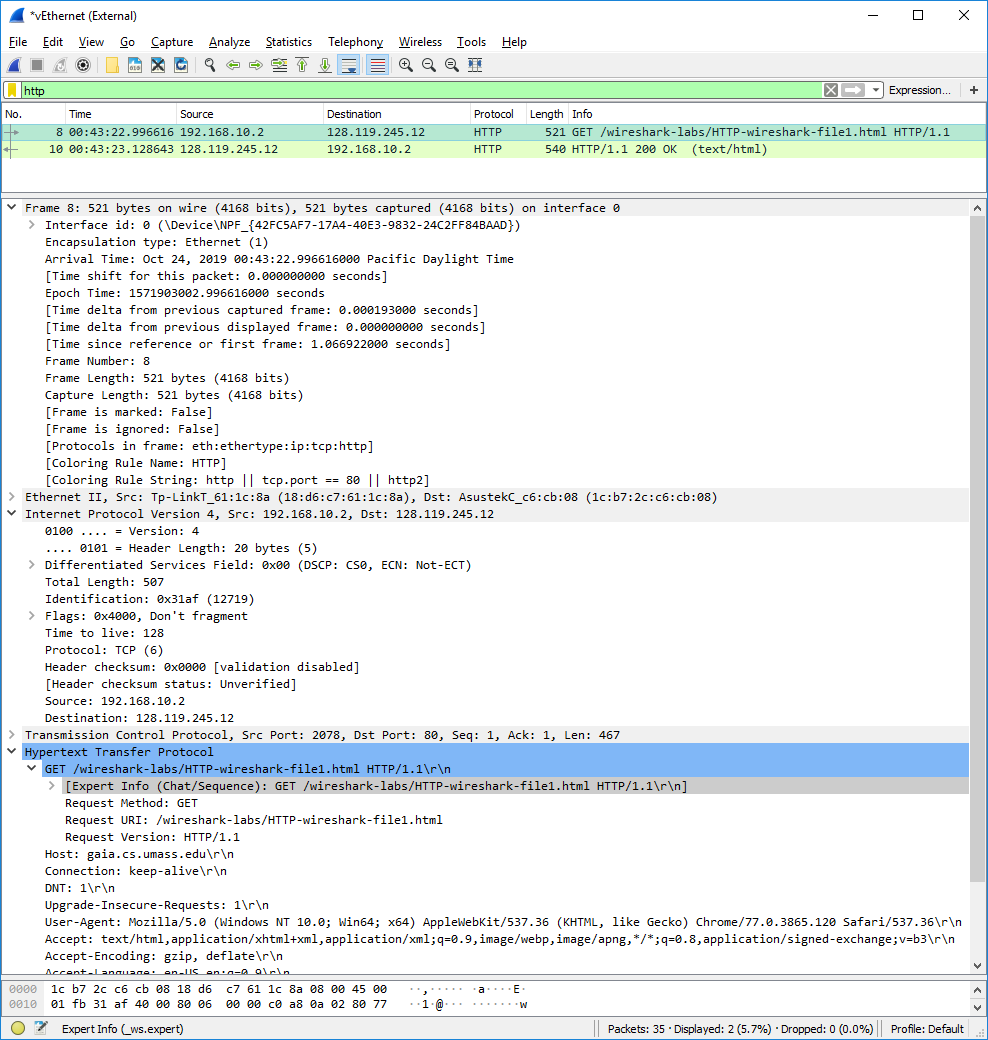
1. How many bytes of content are being returned to your browser?

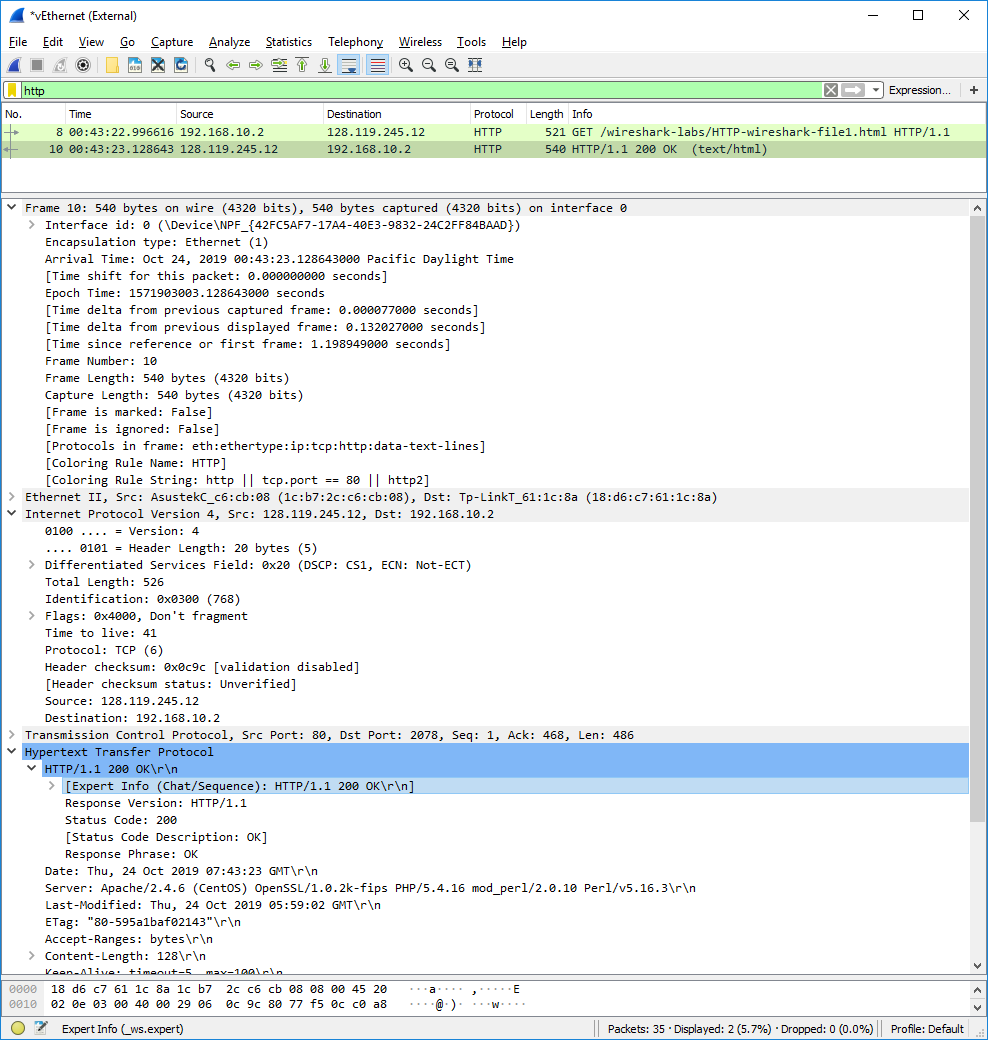
128 bytes of content were returned to my browser.



1. 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.

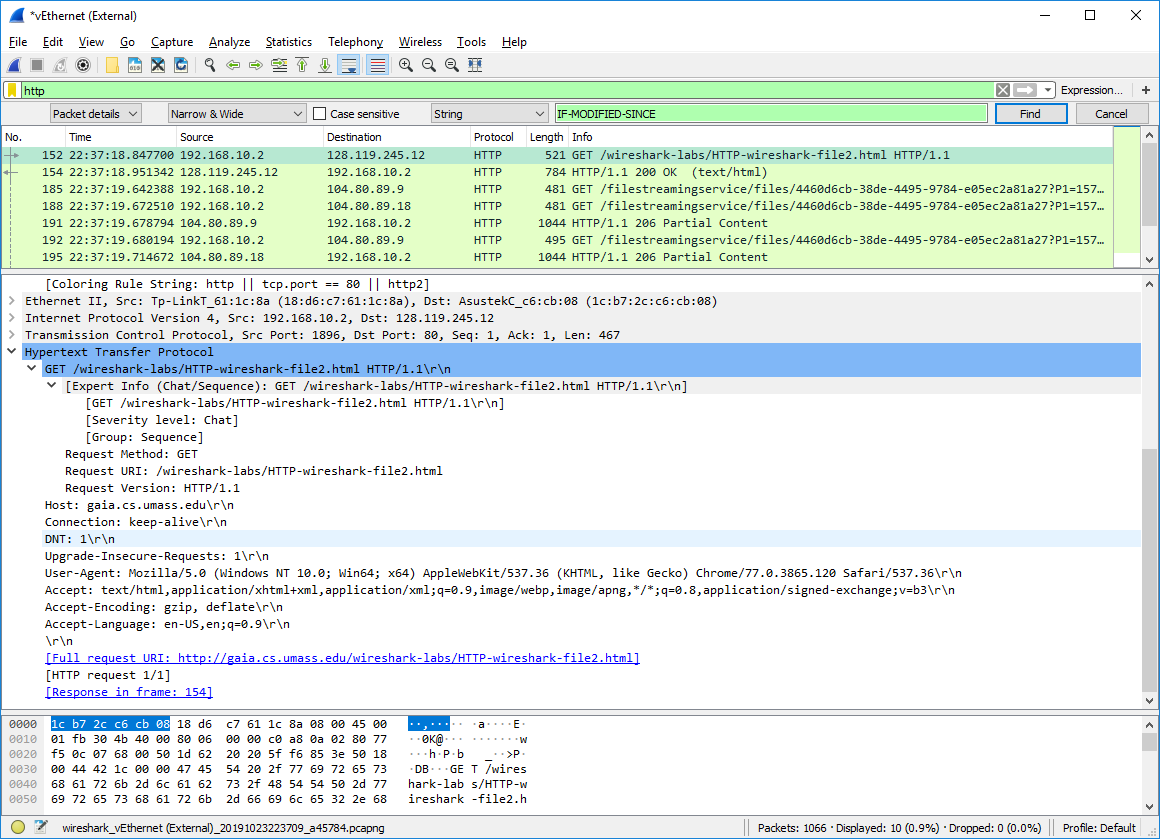
No, all of the headers in the packet content window are displayed in the packet-listing window, as shown below. The No header is shown in the Frame field, the Time header is displayed in the Frame Arrival Time field, the Source/Destination headers are displayed in the Internet Protocol Source/Destination fields, and Protocol header is displayed in the Hypertext Transfer Protocol field, the Length is displayed in the Frame field’s Frame Length subfield, and the Info header is displayed in the Hypertext Transfer Protocol field’s GET subfield.





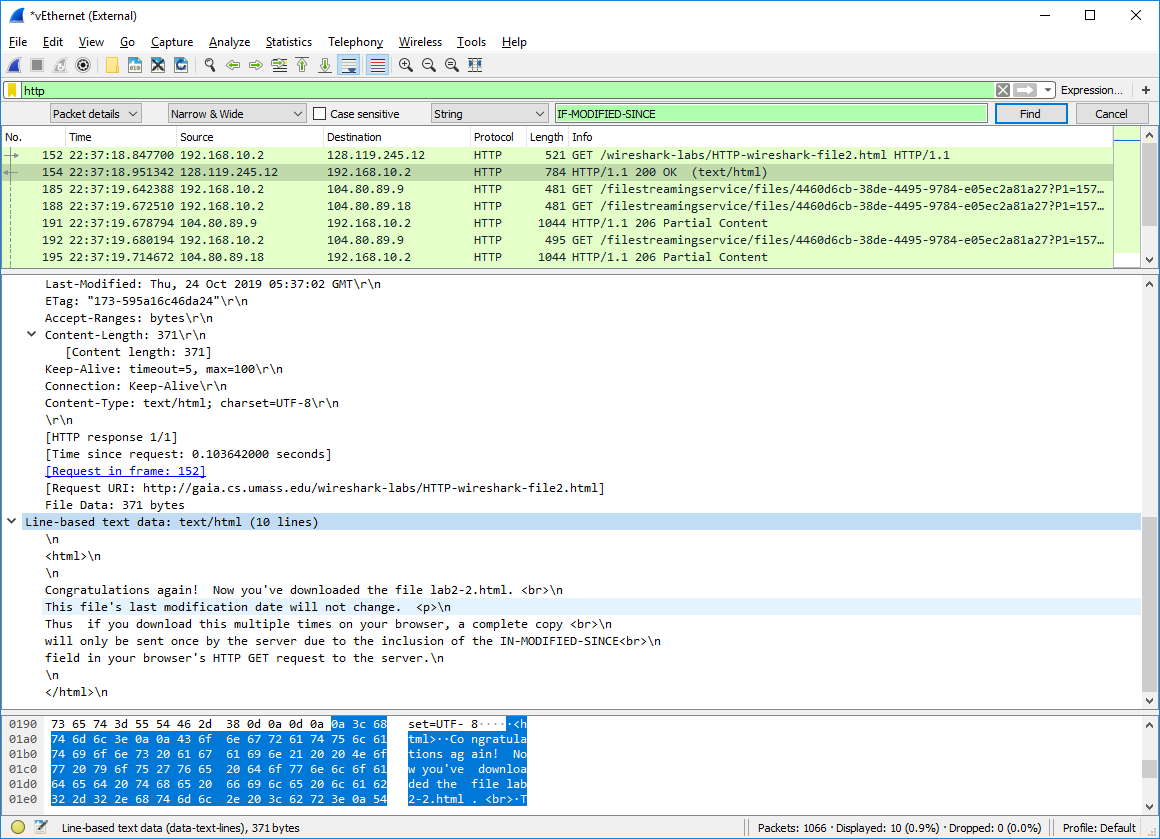
1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No, there is no IF-MODIFIED-SINCE line in the first HTTP GET message, as shown below.



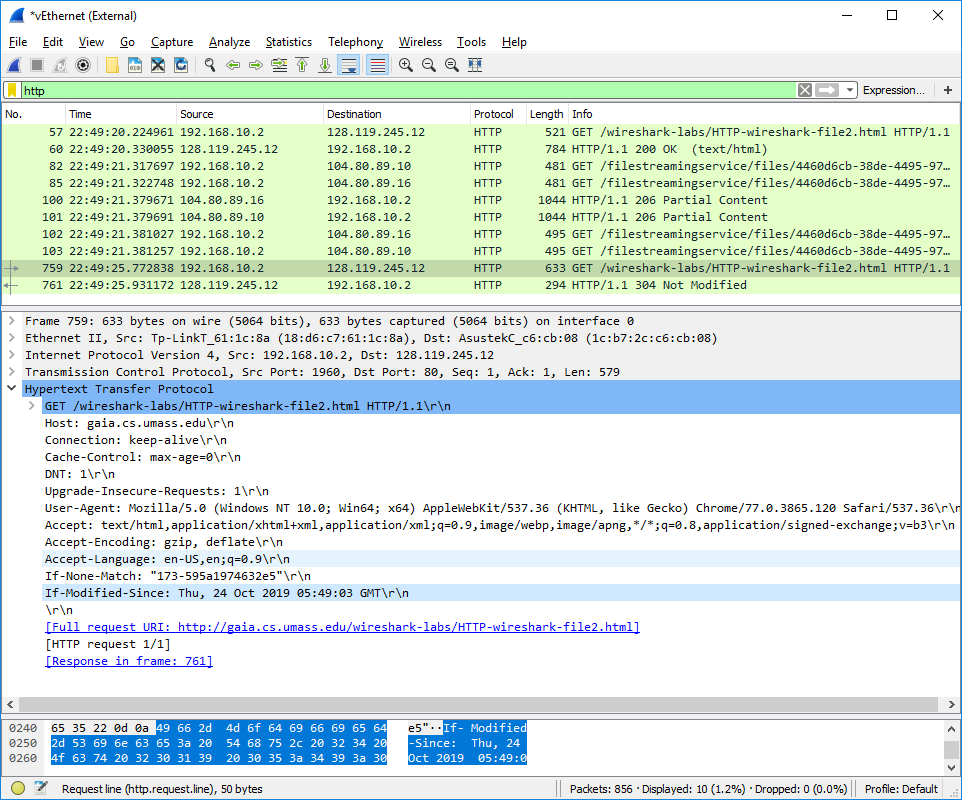
1. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes, the server explicitly returned the contents of the file. The server response message contains a “line-based text data” field that displays the raw text of the file contents.



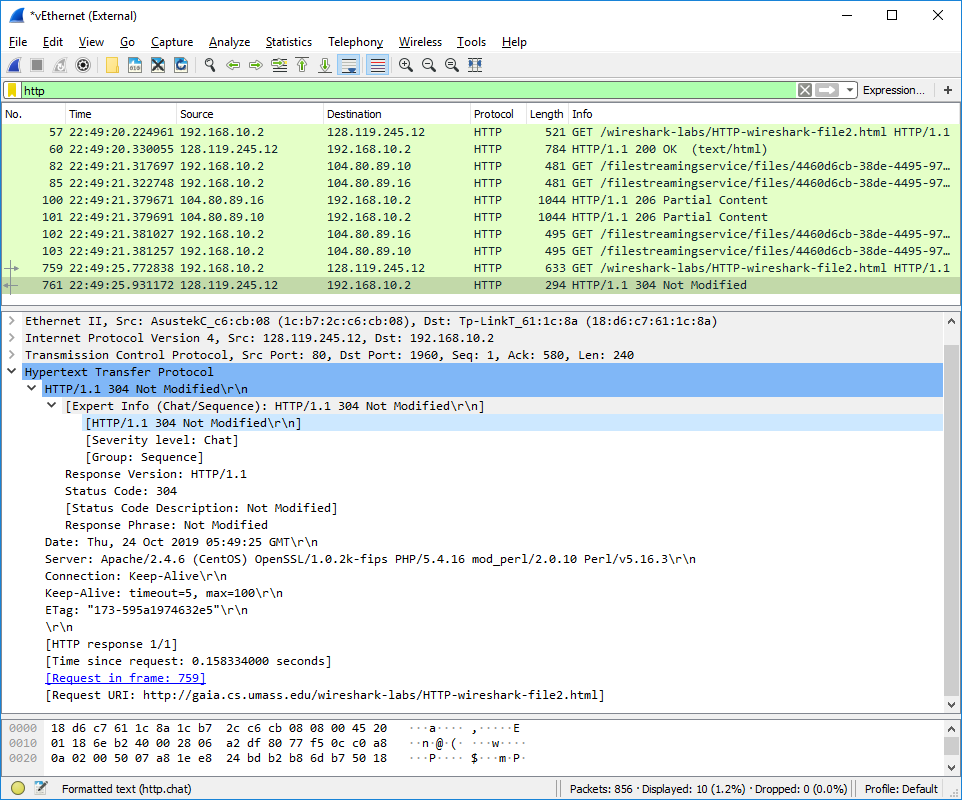
1. Now inspect the contents of the second and third HTTP GET requests from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in one of the HTTP GETs? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Yes, the second and third HTTP GET requests do contain an IF-MODIFIED-SINCE line. The If-Modified-Since header displays the date “Thu, 24 Oct 2019 05:49:03 GMT”, which is the date of the server’s response to the last HTTP GET request for the file HTTP-wireshark-file2.html.



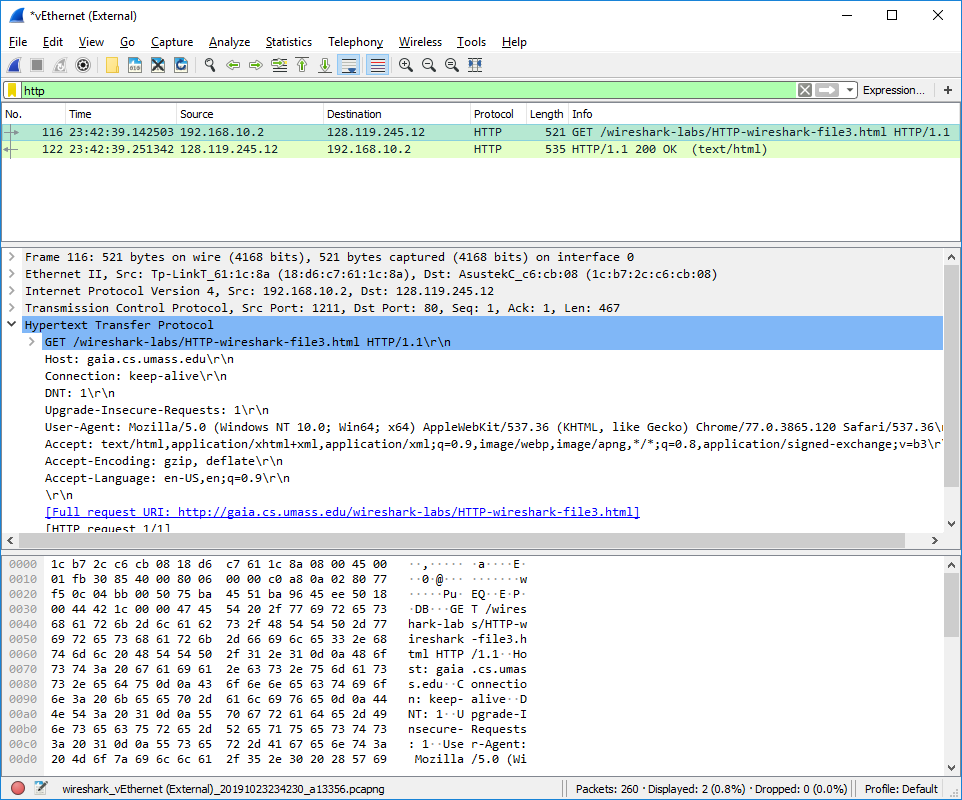
1. What is the HTTP status code and phrase returned from the server in response to the HTTP GET with IF MODIFIED SINCE (if there is one)? Did the server explicitly return the contents of the file? Explain.

The HTTP status code is 304 (Not Modified). No, the server did not explicitly return the contents of the file, which is apparent in the image below since the “Line-based text data” header is missing. This implies that the server’s version of the file has not been modified more recently than the browser’s version of the file stored in cache, so the server did not need to send the file.



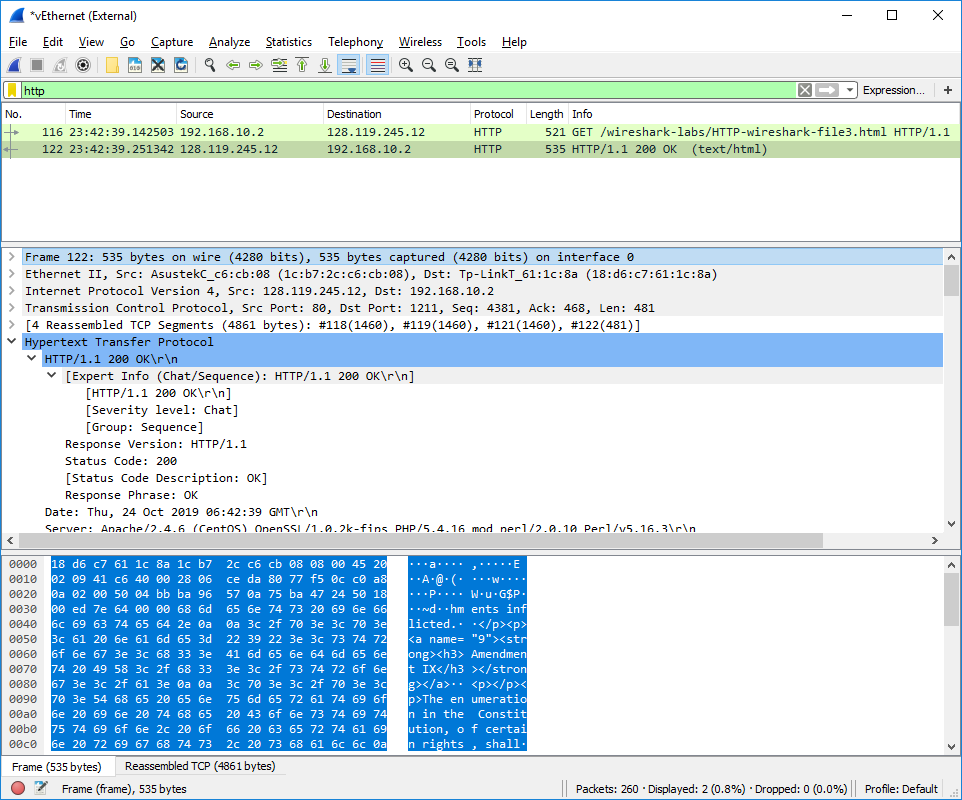
1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

My browser sent 1 HTTP GET request message. Frame 116 contains the GET message for the Bill of Rights.



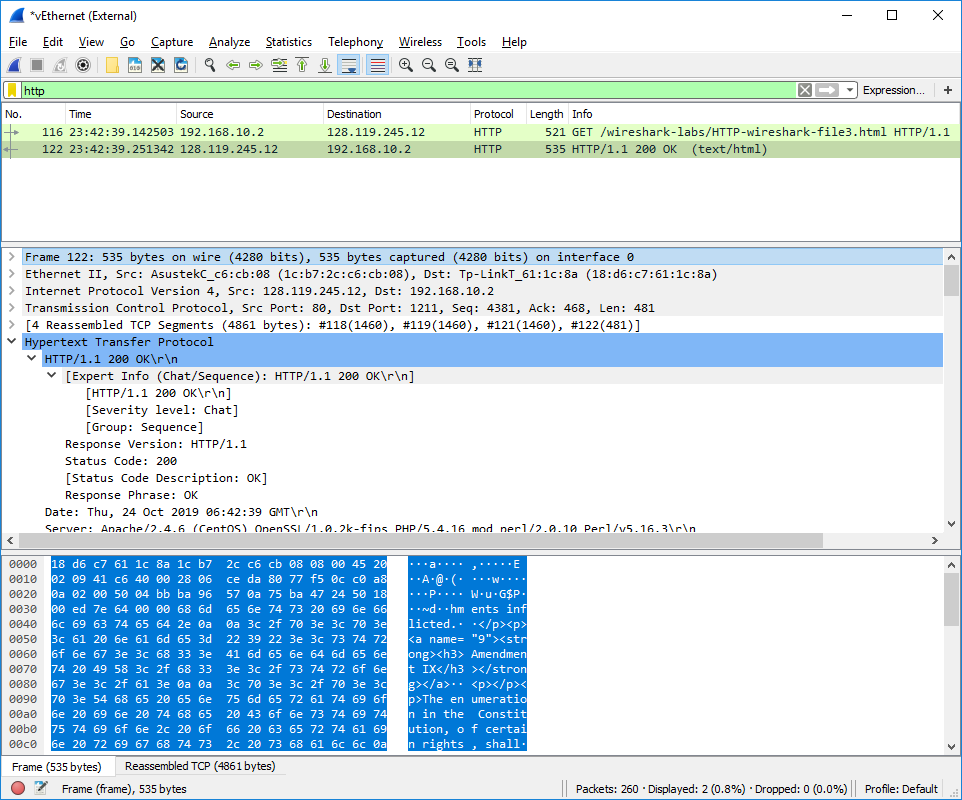
1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Frame 122 contains the response to the HTTP GET request.



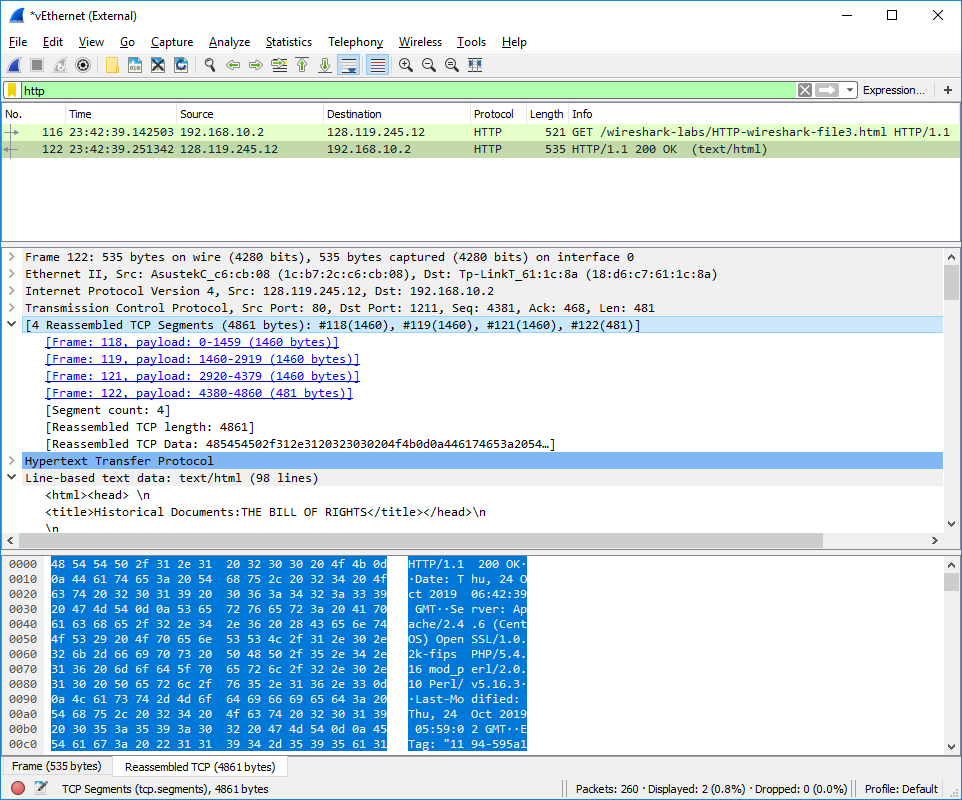
1. What is the status code and phrase in the response?

The response’s status code is 200 and the phrase is “OK”.



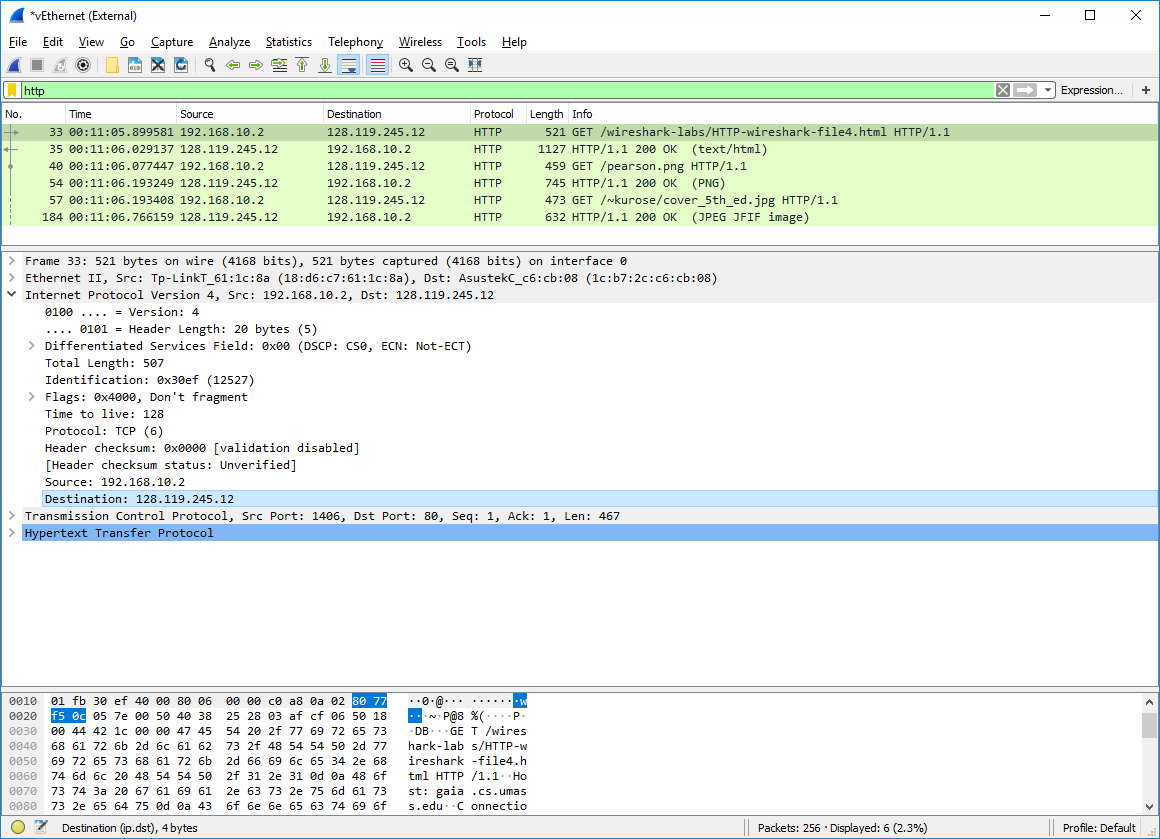
1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

There were 4 TCP segments needed to carry the single HTTP response and the text of the Bill of Rights.



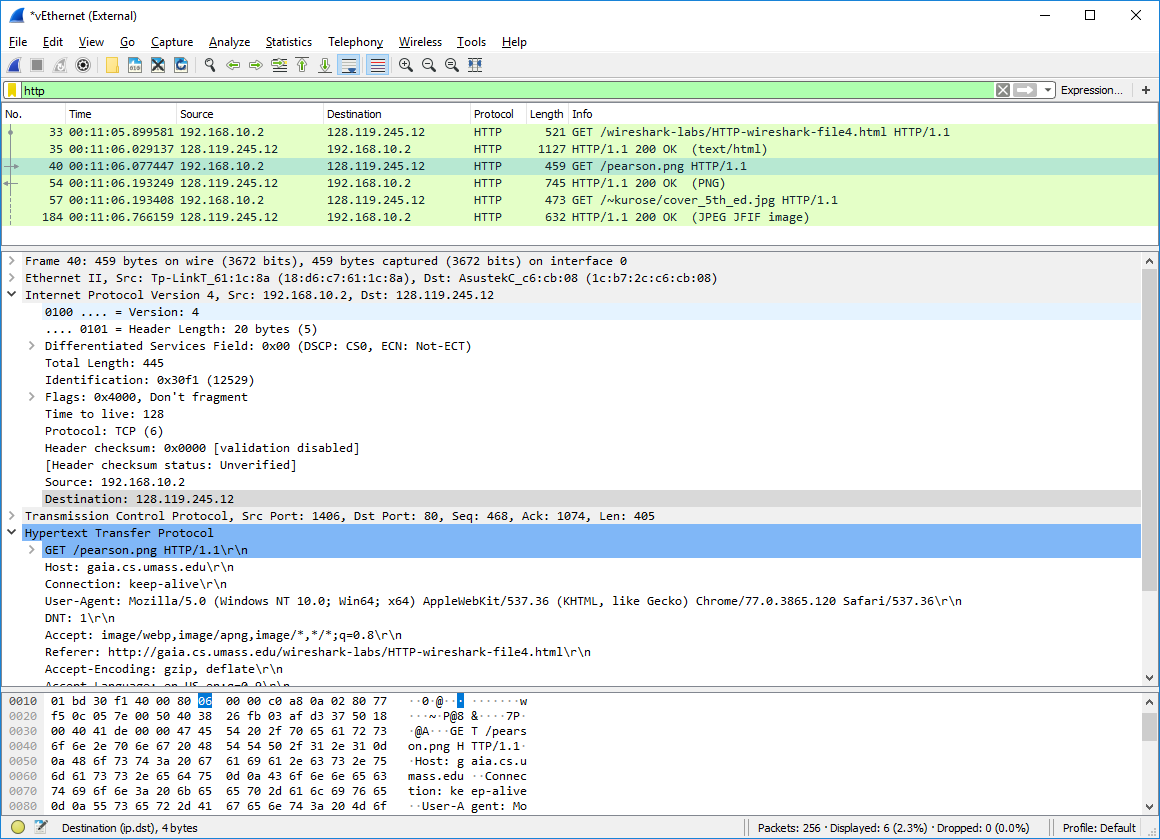
1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

My browser sent 3 HTTP GET request messages to 128.119.245.12.



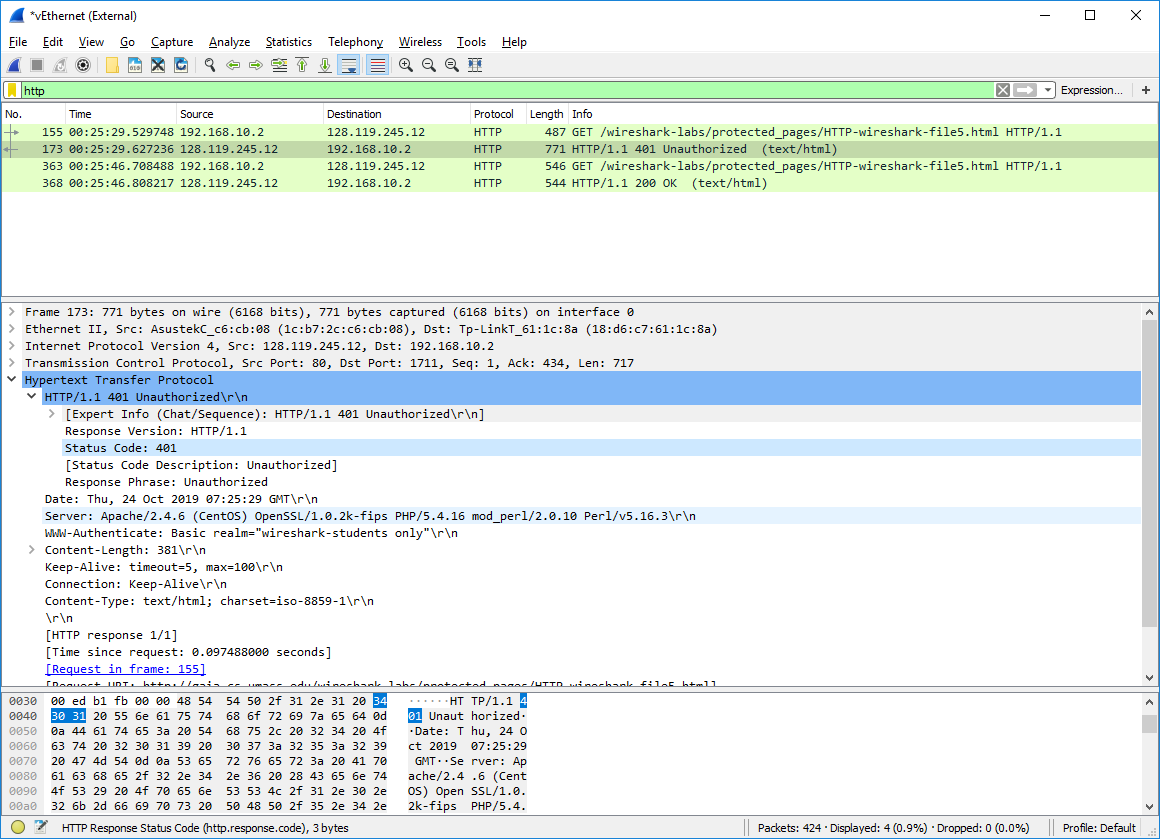
1. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

The two images were downloaded serially because pearson.png was downloaded after the second HTTP GET message and cover\_5th\_ed.jpg was downloaded after the third HTTP GET message. There were 2 HTTP GET requests to download each of the 2 images, and the timestamps for the HTTP GET request messages do not match, so these images must not have been downloaded in parallel.



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

The server’s first response to the initial HTTP GET message is status code 401 and phrase “Unauthorized”.



1. 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: Basic field is the new field that is included in the second HTTP GET message.

