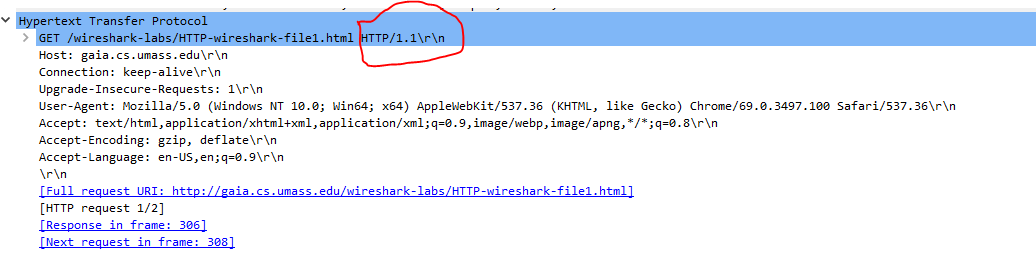
2d Lt James Marvin

Wireshark Lab 2

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

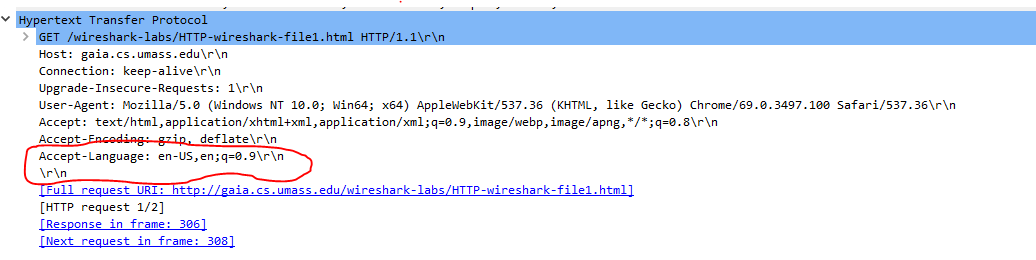
server running?



**My browser is run HTTP 1.1. You can see that in the GET header of this HTTP request.**

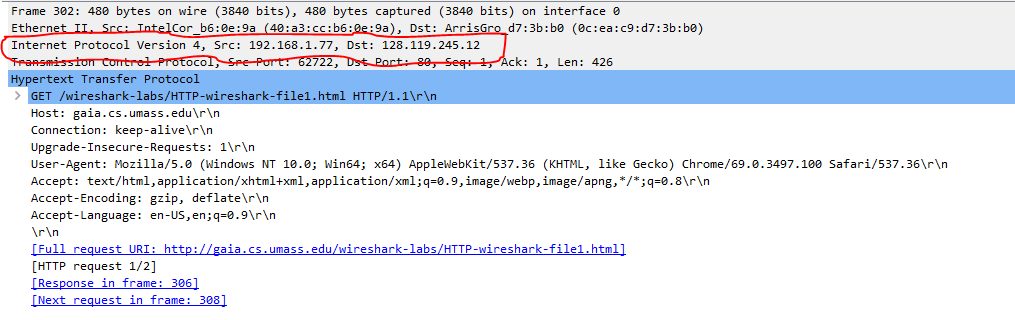
2. What languages (if any) does your browser indicate that it can accept to the

server?



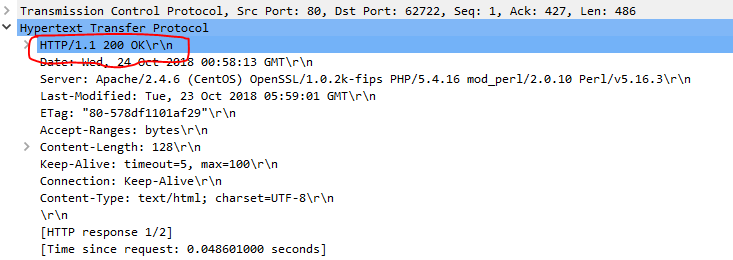
**It can accept US English and English. You can see it in the Accept-Language header in the screenshot above.**

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



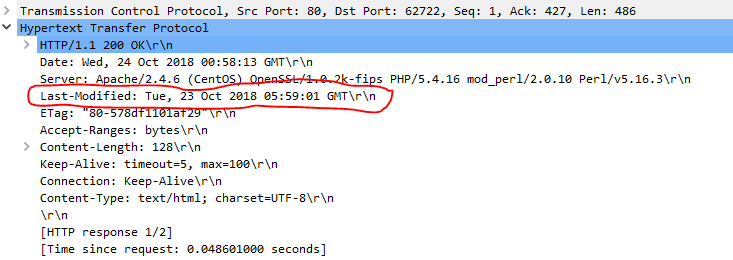
**If you look above at the packet information for the request under the Internet Protocol Version 4 section it lists the Source IP (my computer) as 192.168.1.77 and the Destination IP (gaia.cs.umass.edu) as 128.119.245.12.**

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



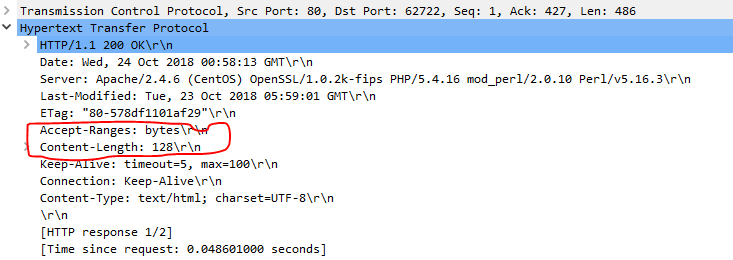
**The status code return from the server was 200 OK. You can see that in the header of the server’s HTTP response packet.**

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



**The HTML file was last modified by the server on Tuesday, 23 October 2018 05:59:01 GMT. You can find that information in the Last-Modified header circled above.**

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



**My browser is receiving 128 bytes. You can find that information within the Accept-Ranges that tells you what unit the data is coming in and Content-Length which tells you how much.**

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 did not find a header in the raw data not listed in the packet window.**

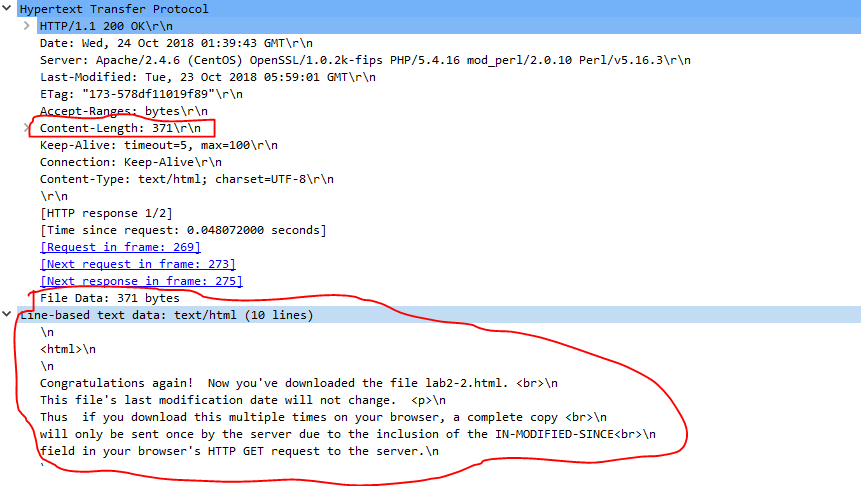
8. Inspect the contents of the first HTTP GET request from your browser to the

server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

**I do not see the “IF-MODIFIED-SINCE” header in the HTTP GET request.**

9. Inspect the contents of the server response. Did the server explicitly return the

contents of the file? How can you tell?

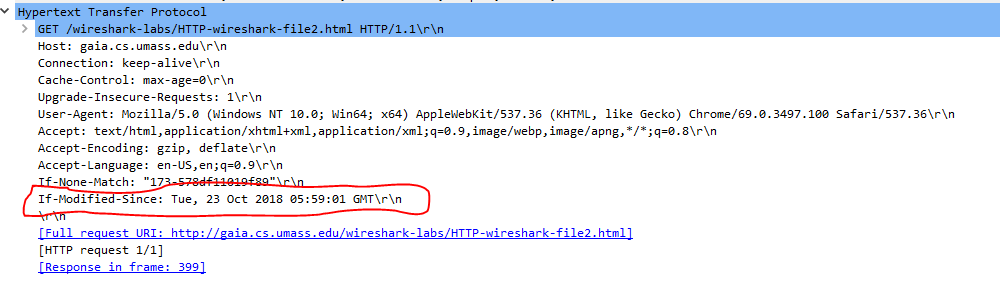


**Yes, the server did explicitly return the contents of the file. You can tell because the content length is 371 bytes and Wireshark gives helpful information about the line-based text data it received. Also the Content-Type header is text/html.**

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?

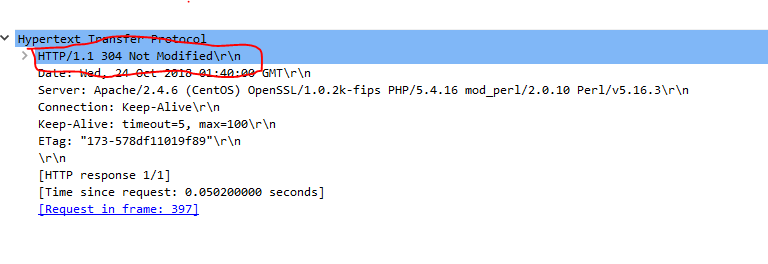


**Yes, I do see the “IF-MODIFIED-SINCE:” headers in the HTTP GET. The information that follows it is the time stamp that from the previous identical GET that the browser cached.**

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?

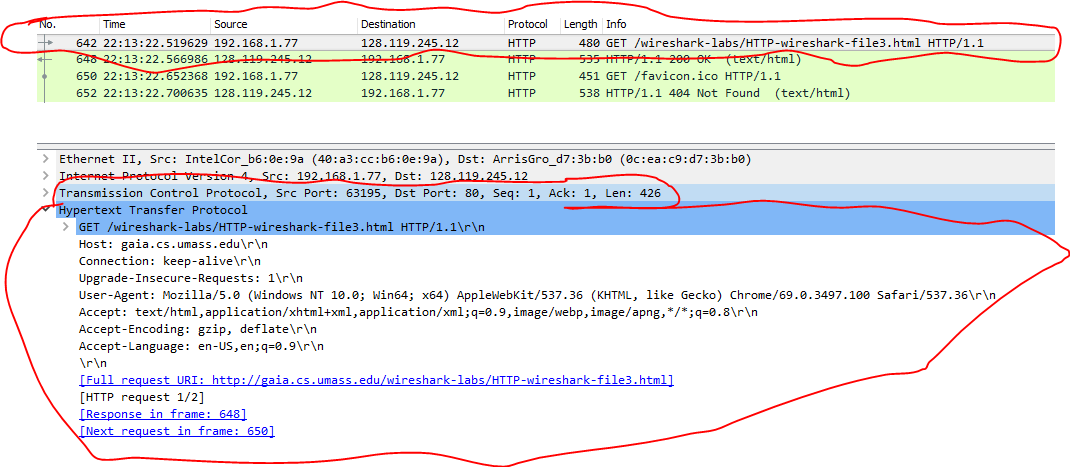
Explain.



**The status code is 304 Not Modified. The server did not explicitly return the contents of the file because the browser already had it in its cache. You can see that there is no content headers in the response.**

12. How many HTTP GET request messages did your browser send? Which packet

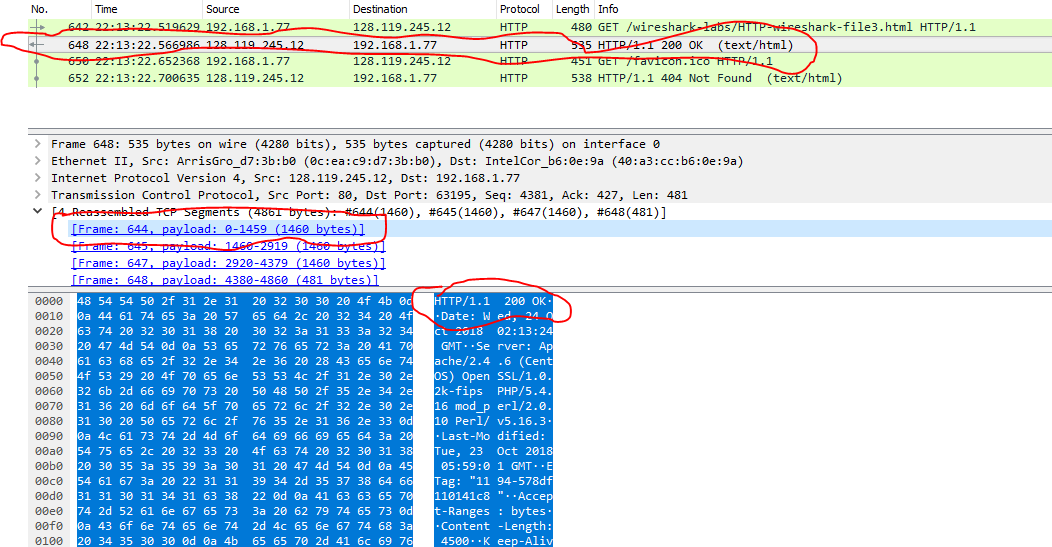
number in the trace contains the GET message for the Bill or Rights?



**My browser sent one GET request. Packet number 642 sent the GET request.**

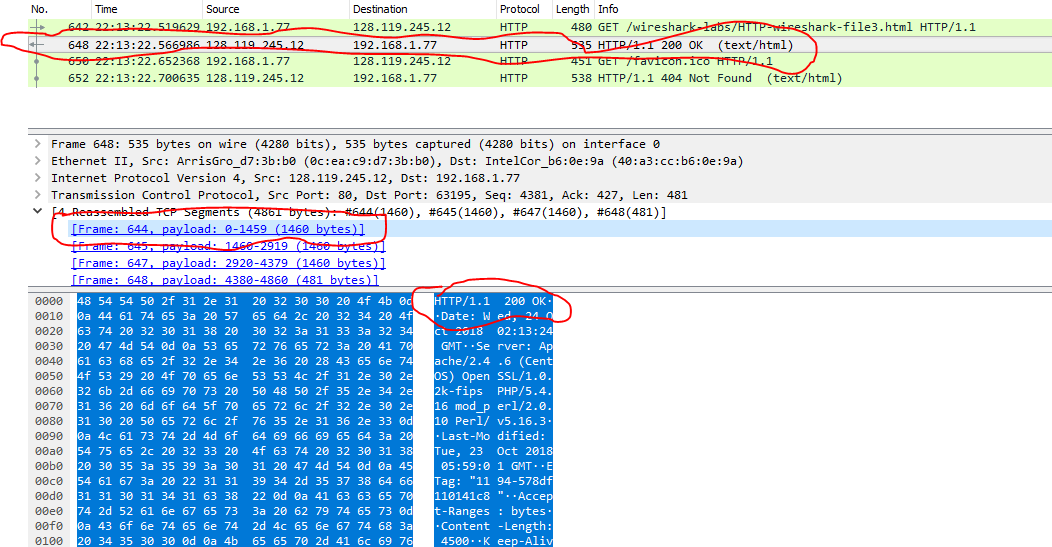
13. Which packet number in the trace contains the status code and phrase associated

with the response to the HTTP GET request?



**Packet 644, when you examine the response in wireshark you can see that it was split into 4 tcp segments. When you click on packet 644 it shows you the raw data which is highlighted in blue. You can see the response phrase in the first line.**

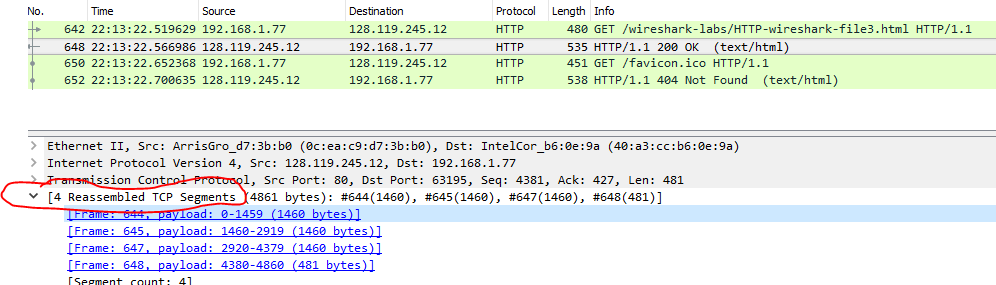
14. What is the status code and phrase in the response?



**200 OK you can see it in the raw data. And in the response overview at the top.**

15. How many data-containing TCP segments were needed to carry the single HTTP

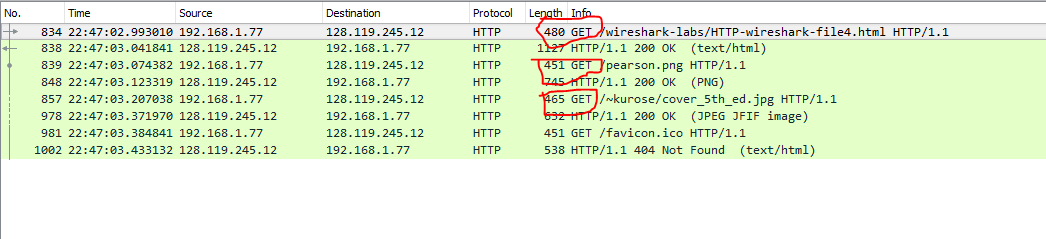
response and the text of the Bill of Rights?



**4 segments**

16. How many HTTP GET request messages did your browser send? To which

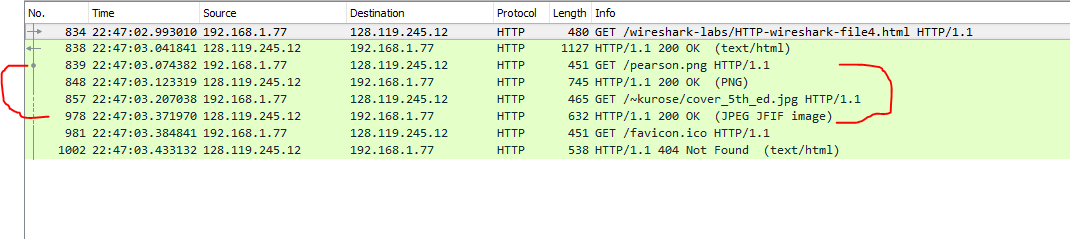
Internet addresses were these GET requests sent?



**3 GET requests. The first sent to** [**http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html**](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html)**,** [**http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html/pearson.png**](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html/pearson.png)**, and** [**http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html/~kurose/cover\_5th\_ed.jpg**](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html/~kurose/cover_5th_ed.jpg)

17. Can you tell whether your browser downloaded the two images serially, or

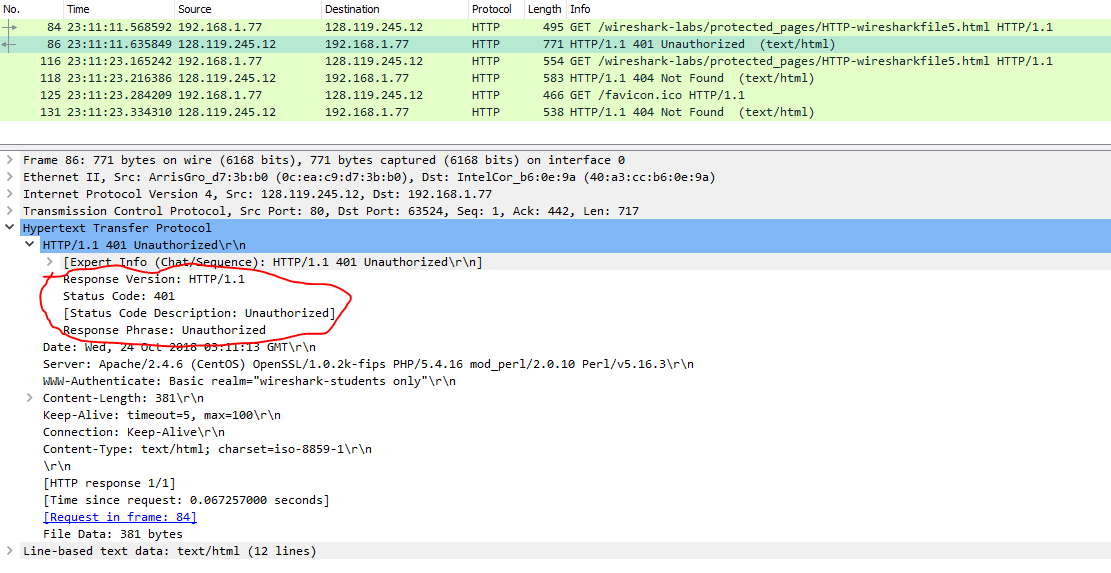
whether they were downloaded from the two web sites in parallel? Explain.



**Serially because it waits for the response from the server before sending the other GET request.**

18. What is the server’s response (status code and phrase) in response to the initial

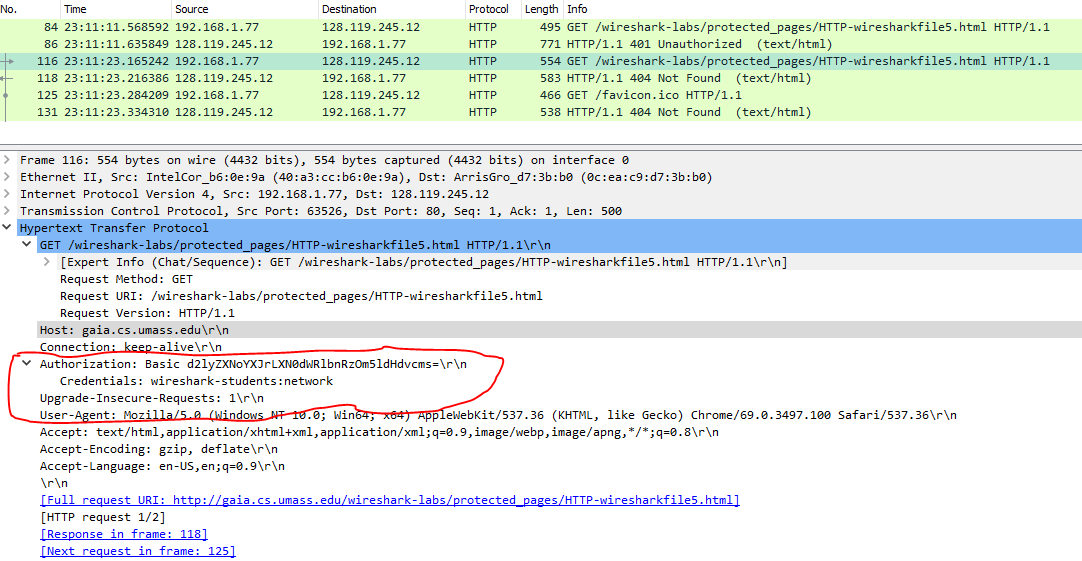
HTTP GET message from your browser?



**401 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 new field included in this GET request is Authorization. It contains the credentials entered by the user in base 64. Wireshark can read it in the line below. It is definitely not encrypted.**