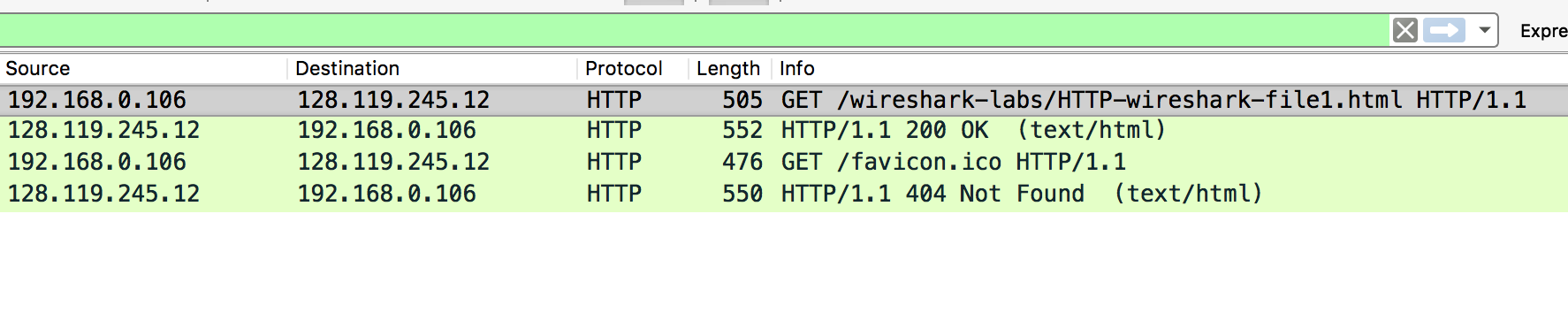
Nathan Flack

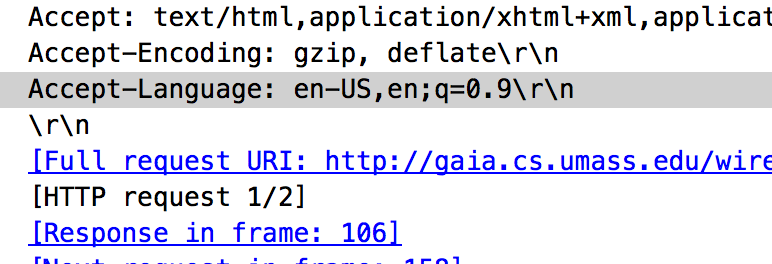
Wireshark Lab #2

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? 1.1



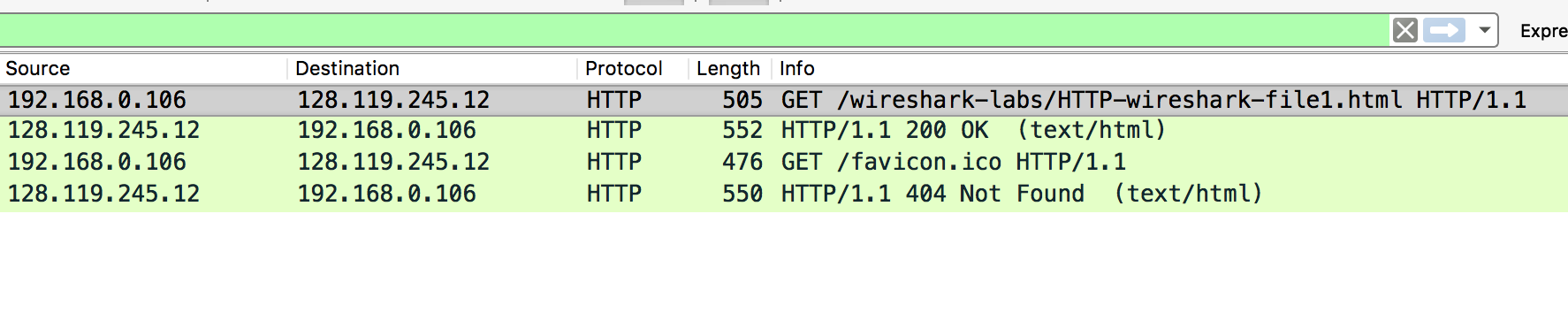


1. What languages (if any) does your browser indicate that it can accept to the server? en-US and en  
   



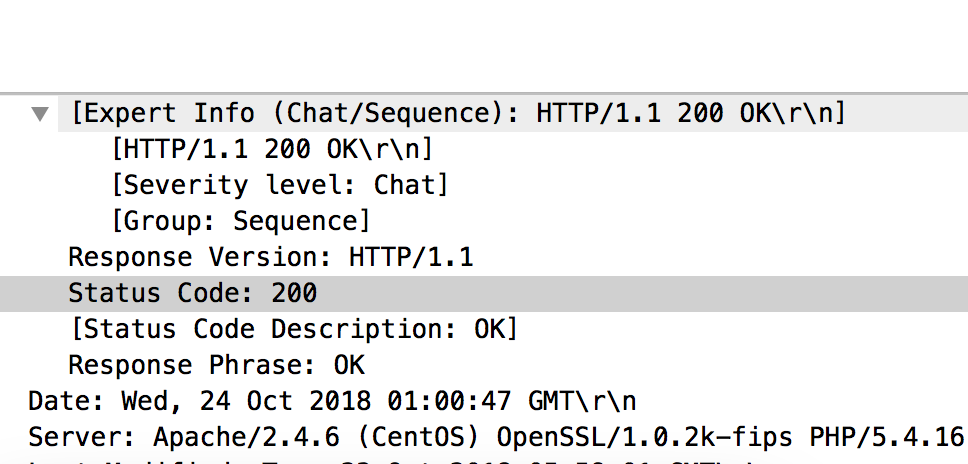
1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

My Computer: 192.168.0.106; umass.edu: 128.119.245.12





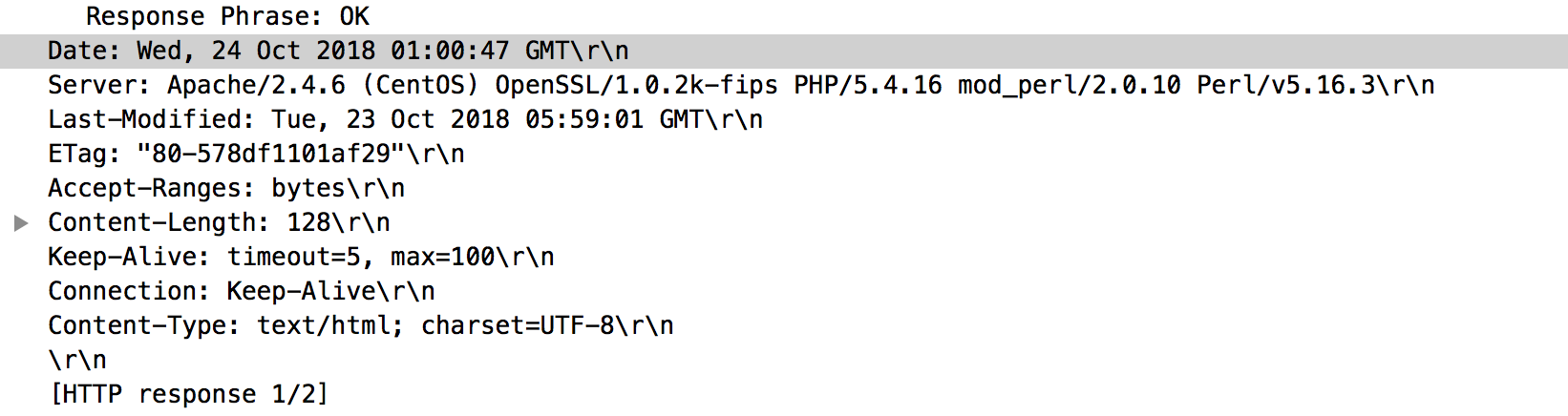
1. What is the status code returned from the server to your browser? 200





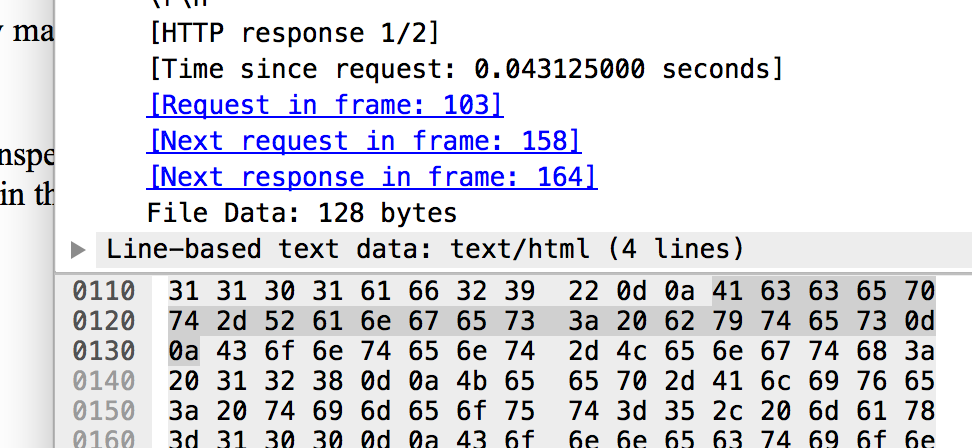
1. When was the HTML file that you are retrieving last modified at the server?

Tue, 23 oct 2018 5:59:01 GMT





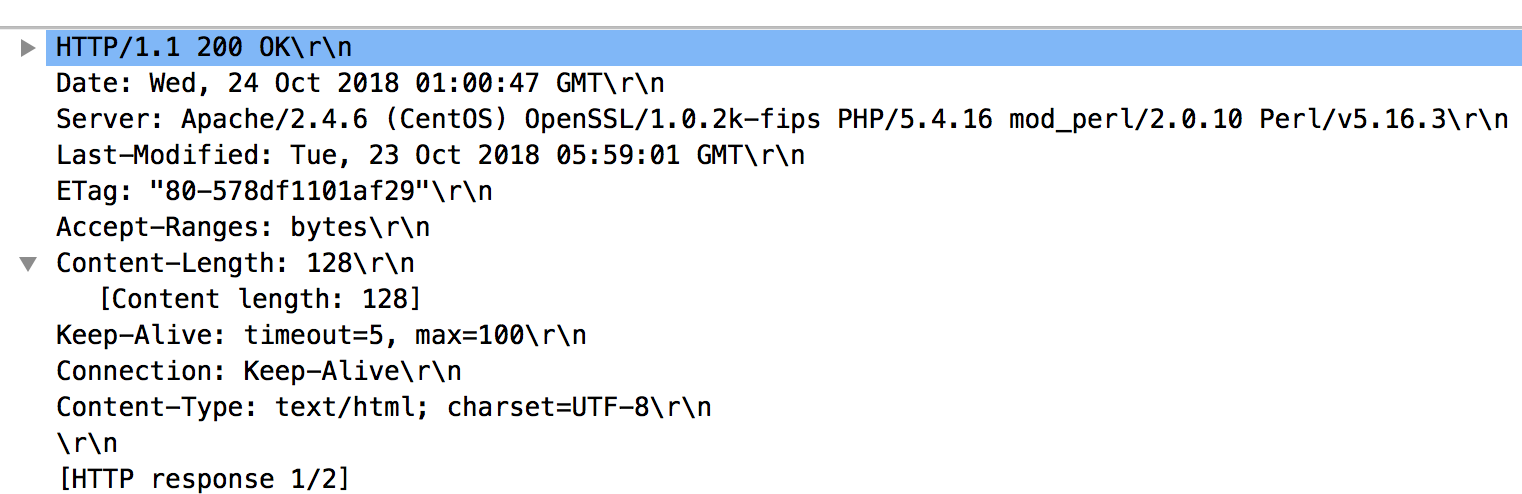
1. How many bytes of content are being returned to your browser? 128 bytes





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.

The server name: “Apache/2.4.6”





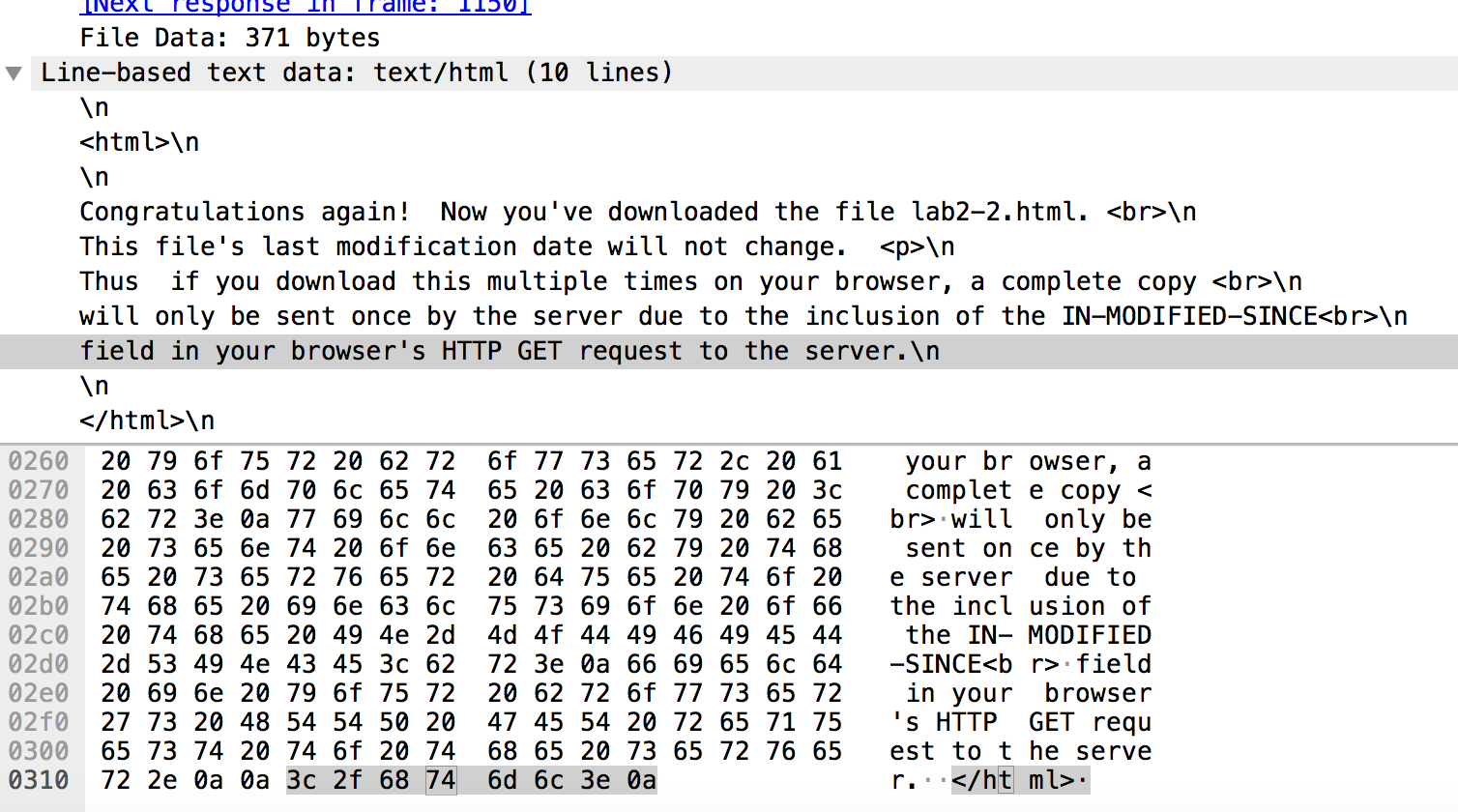
The HTTP Conditional GET/response interaction:

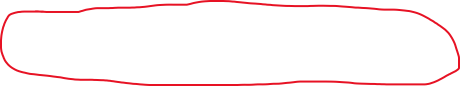
1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No

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

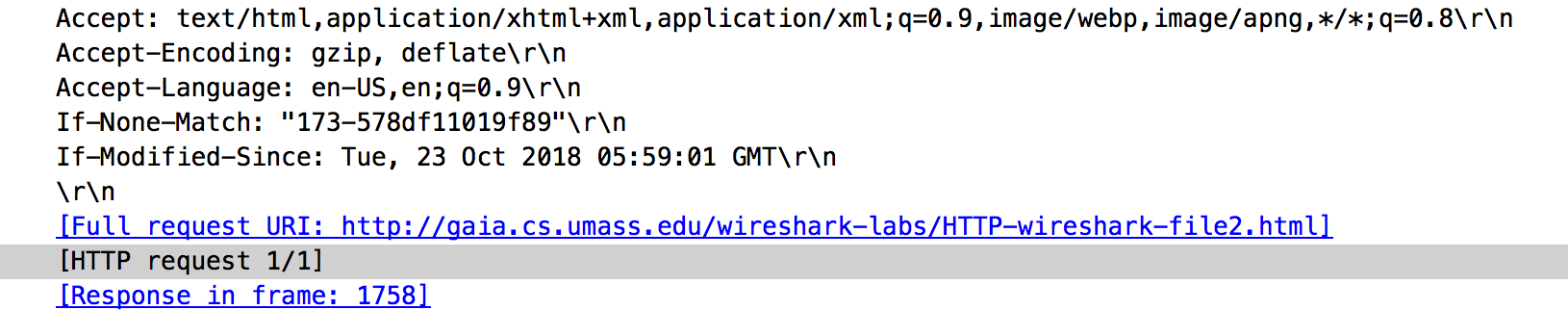
Yes. You can see the data in the packet and in the hex file.





1. 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. “Tue, 23 Oct 2018 5:59:01 GMT”

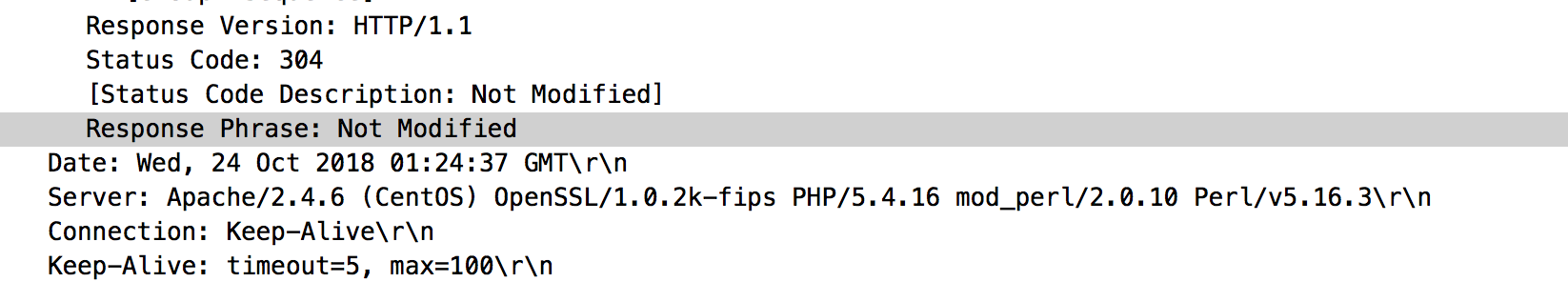




1. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Response Code: 304: Not Modified

The Server did not return the contents of the file because it had not been modified since my previous request. Therefore, my computer showed me the version of the file that it stored in its cache after my first request.

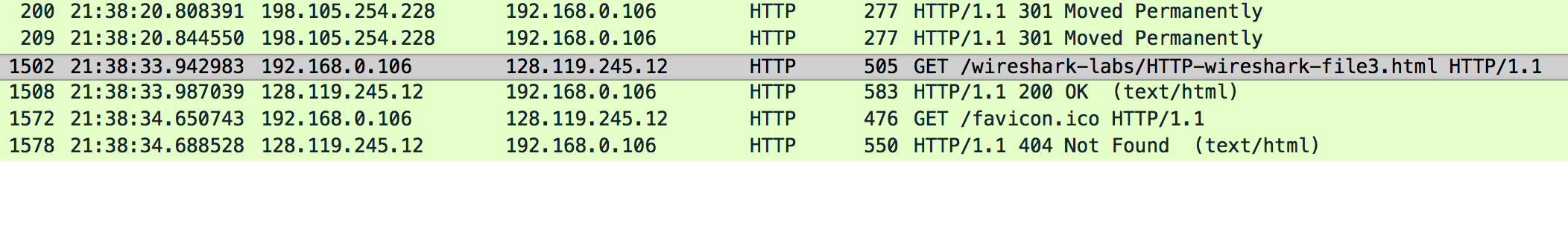




12. How many HTTP GET request messages did your browser send? Which packet

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

1 HTTP GET request. The packet number is 1502

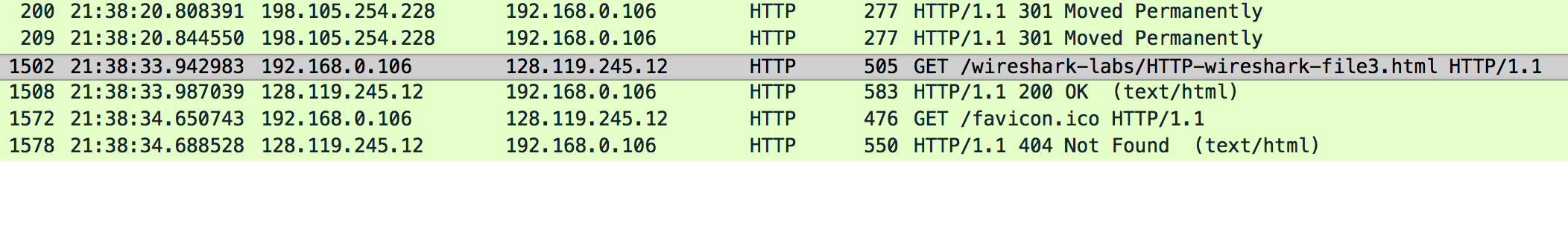




13. Which packet number in the trace contains the status code and phrase associated

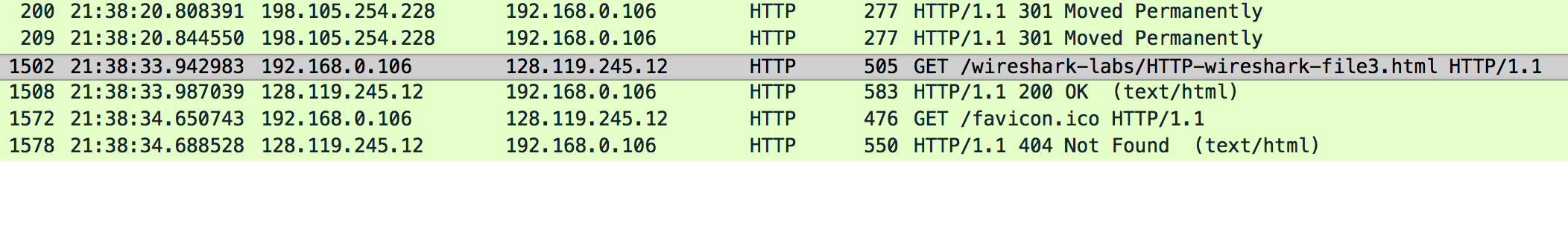
with the response to the HTTP GET request?

Packet number 1508 contains the 200 OK message





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

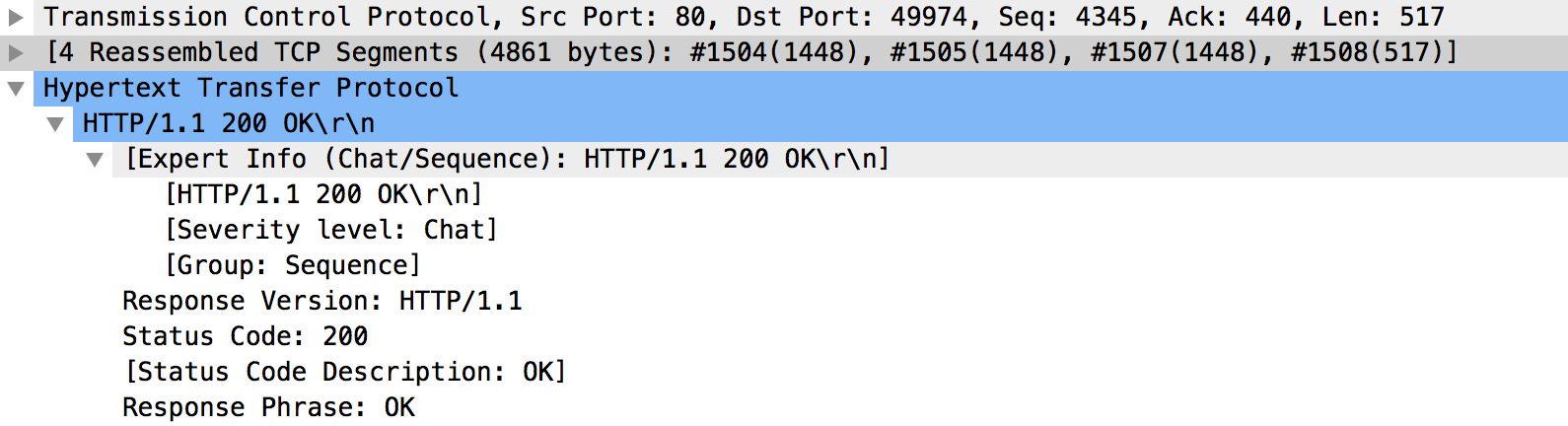
200 OK



15. 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



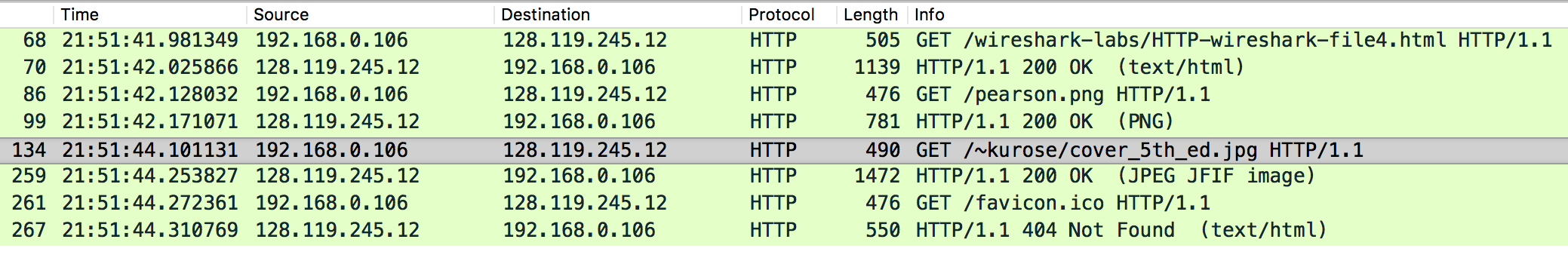


HTML Documents with Embedded Objects

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

Internet addresses were these GET requests sent?

Three. All of them went to destination IP address 128.119.245.12

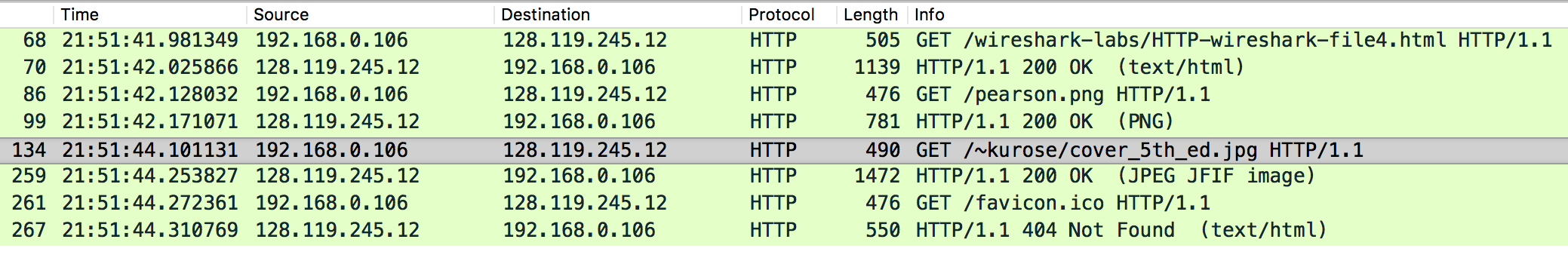




17. Can you tell whether your browser downloaded the two images serially, or

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

It looks like they were downloaded serially, because the first HTTP GET/response (for the pearson.png image) was sent and completed before the GET request was sent for the Kurose jpg image.





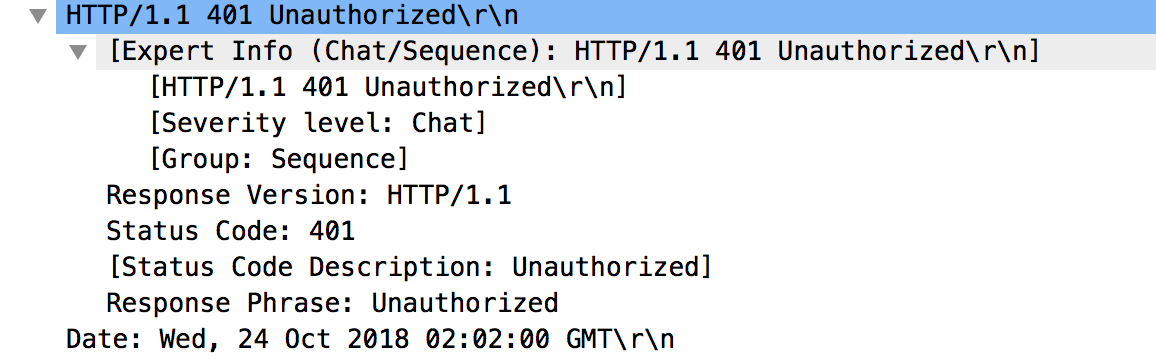
HTTP Authentication:

18. 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





19. When your browser’s sends the HTTP GET message for the second time, what

new field is included in the HTTP GET message?

“Authorization”

