**CSCE 560**

**Wireshark Lab 2**

**24 Oct 18**

**Marvin Newlin**

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

server running?

**Sol’n:** As we can see from the red box, the browser is running HTTP 1.1.

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

server?

**Sol’n:** As we can see from the black box it wants US English.

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

**Sol’n:** The green box shows my source IP of 192.168.1.9 and the purple box shows the UMass IP of 128.119.245.12

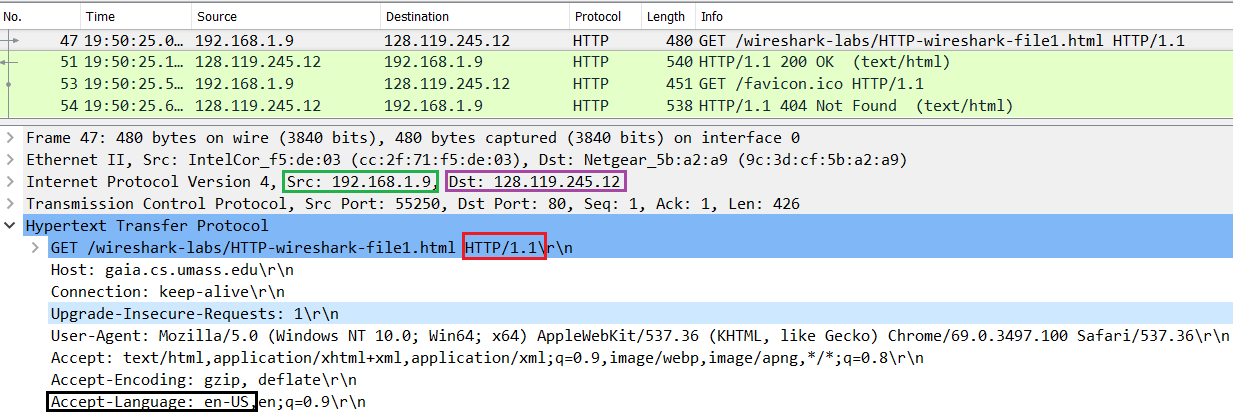


Figure 1: Used for questions 1-3

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

**Sol’n:** The red box shows that it is an HTTP 200 OK response code.

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

**Sol’n:** The green box shows that the file was last modified 23 Oct 18 at 0559 GMT (0059 EST)

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

**Sol’n:** The Black box shows us that there is 128 bytes of content being returned.

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.

**Sol’n:** The Keep Alive header is one that is not displayed in the packet listing (blue box)

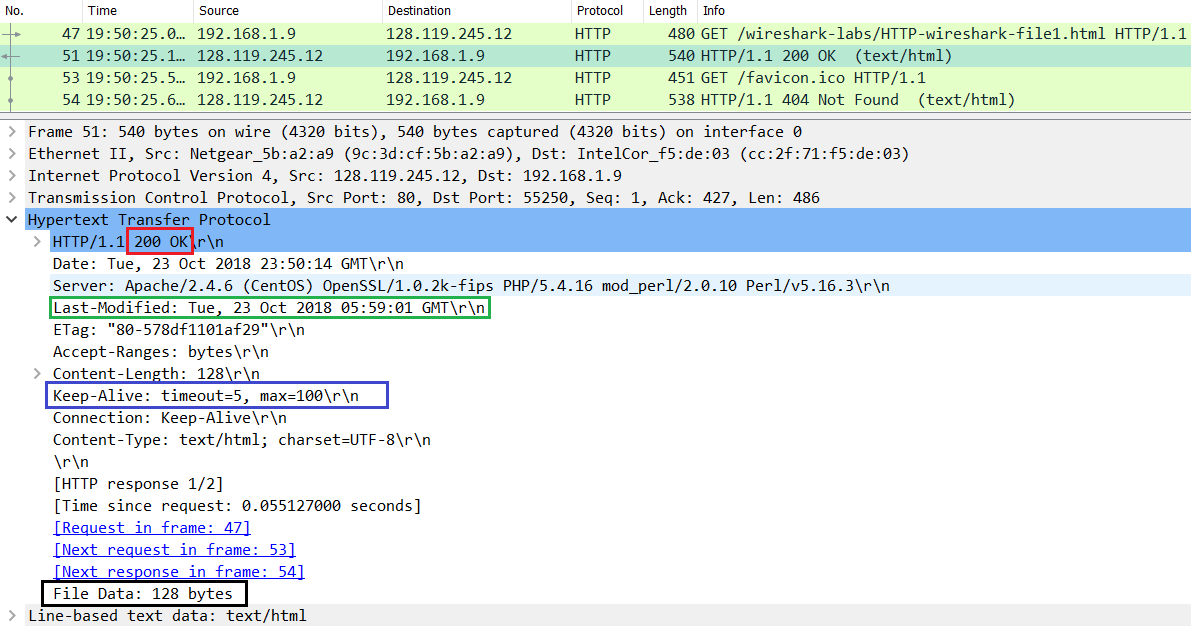
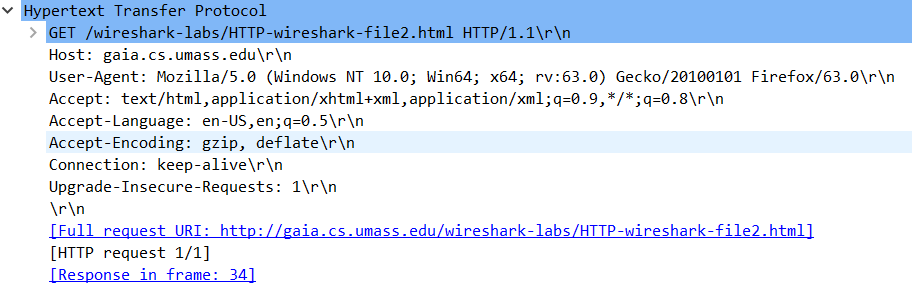


Figure 2: Used for questions 4-7

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

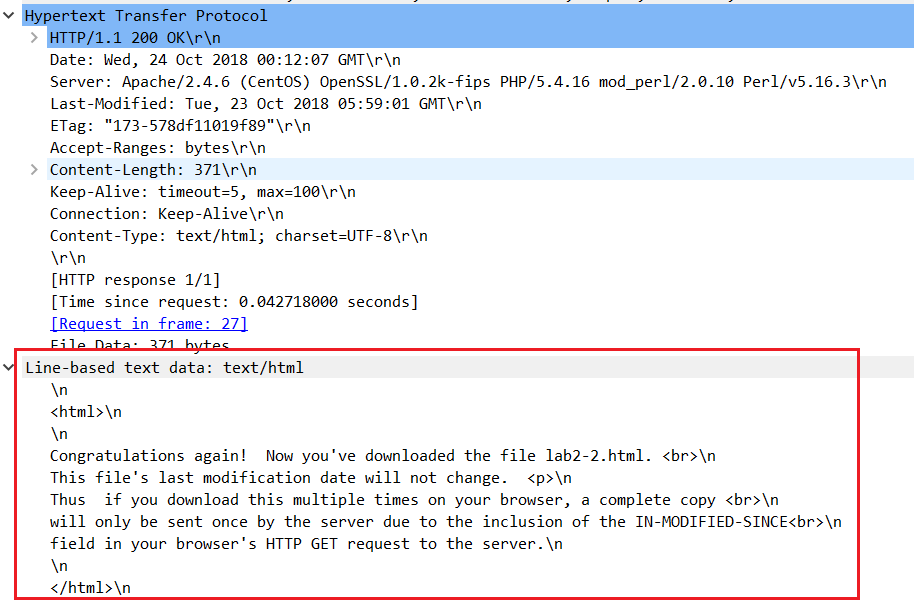
server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?



**Sol’n:** As wee can see, there is no IF-MODIFIED-SINCE header in the initial HTTP GET.

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

contents of the file? How can you tell?

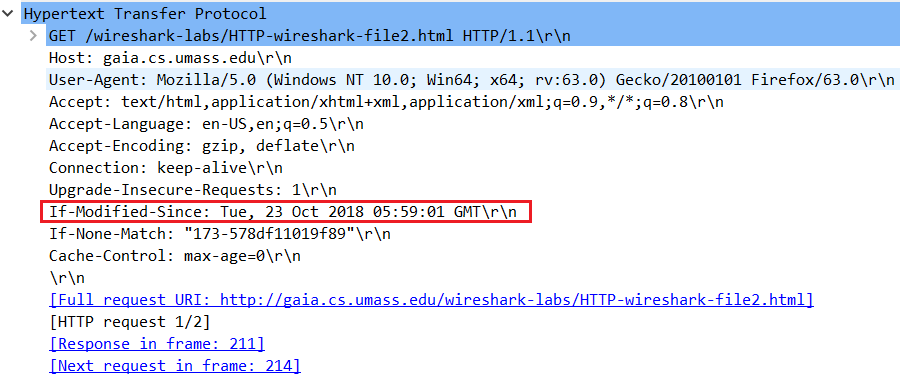


**Sol’n:** As we can see in the red box, the file contents are explicitly returned from the server.

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?

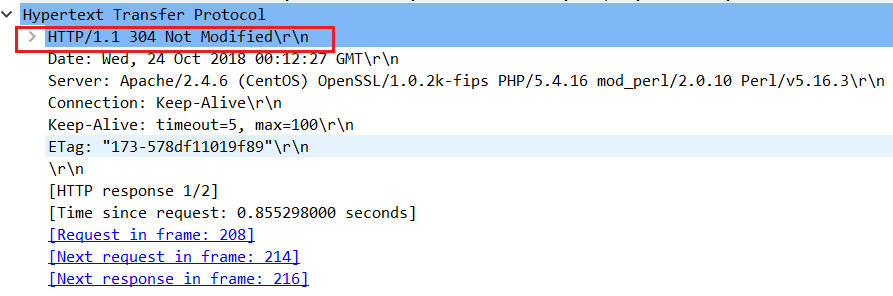


**Sol’n:** From the red box we see the IF-MODIFIED-SINCE header and the date and time of the last modified field from the original GET message is there.

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?

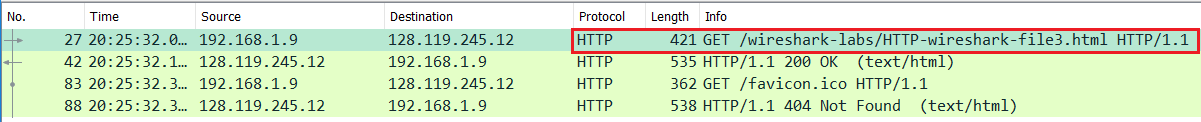
Explain.



**Sol’n:** In the red box we see the response code of 304 Not Modified. Additionally, unlike the initial response there is no section with the file data so the server did not explicitly return the contents of the file.

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

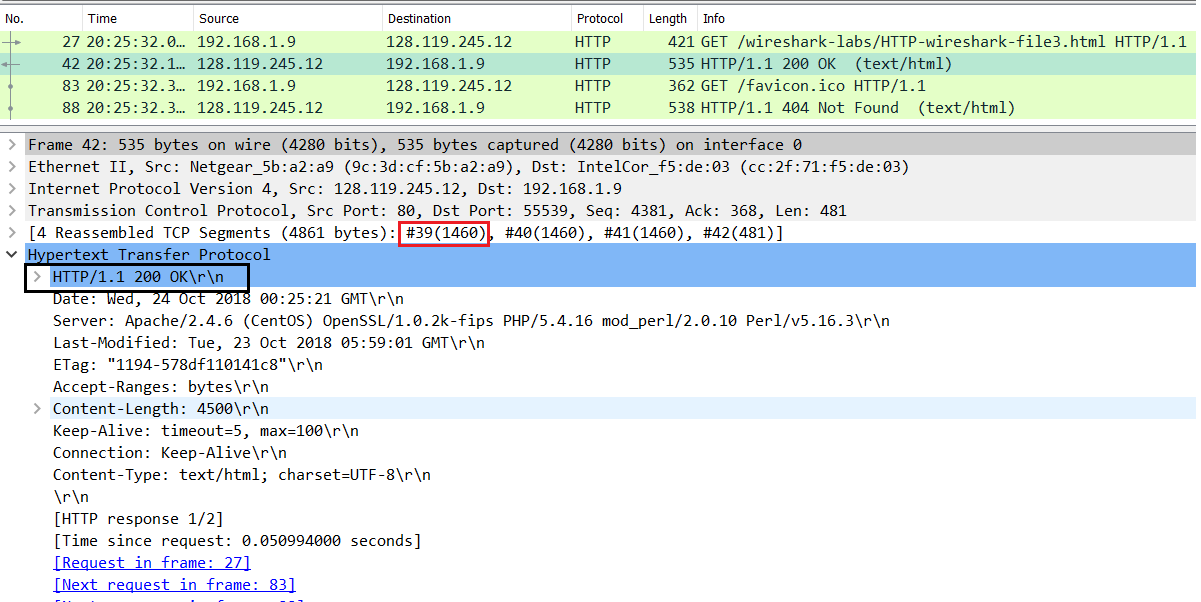
number in the trace contains the GET message for the Bill or Rights?



**Sol’n:** We can see that there was one GET request (red box) and that it was packet number 27.

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

with the response to the HTTP GET request?



**Sol’n:** In the red box we see that it was packet 39 (first TCP segment) and a 200 OK response.

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

**Sol’n:** It is an HTTP 200 OK Response.

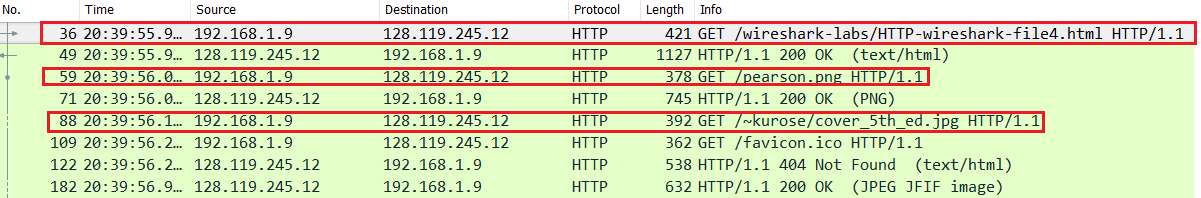
15. How many data-containing TCP segments were needed to carry the single HTTP

response and the text of the Bill of Rights?

**Sol’n:** As we can see from the line with the red box, it took 4 TCP segments to carry the HTTP response and data.

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

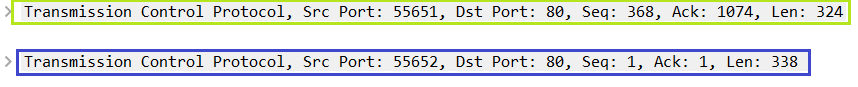
Internet addresses were these GET requests sent?



**Sol’n:** We can see from the red boxes that there were 3 GET requests sent and they were all sent to the same IP address.

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

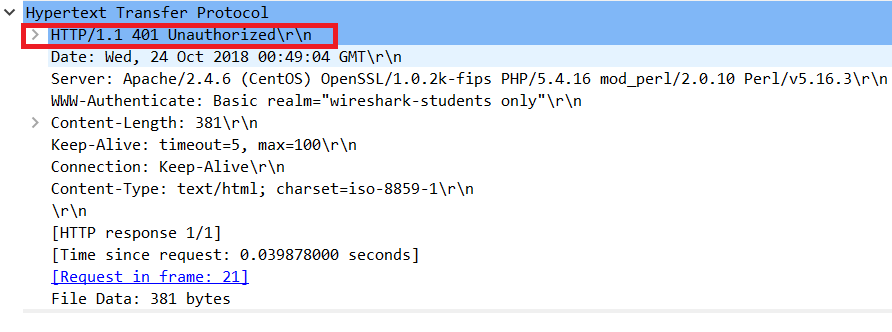
whether they were downloaded from the two web sites in parallel? Explain.



The top line is the TCP information for the first image and the bottom is the TCP information for the second. We can see that the source ports are different for the two images indicating that they were sent over different TCP connections, so they were downloaded in parallel.

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

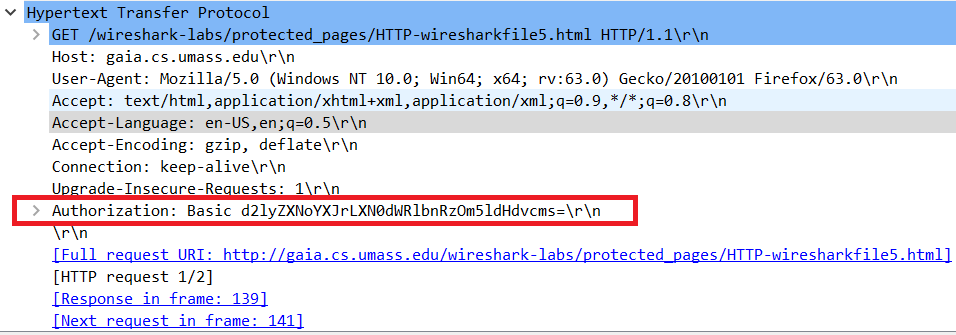
HTTP GET message from your browser?



**Sol’n:** It is an HTTP 401 Unauthorized response

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

new field is included in the HTTP GET message?



**Sol’n:** We can see that an Authorization header is added in the second GET request.