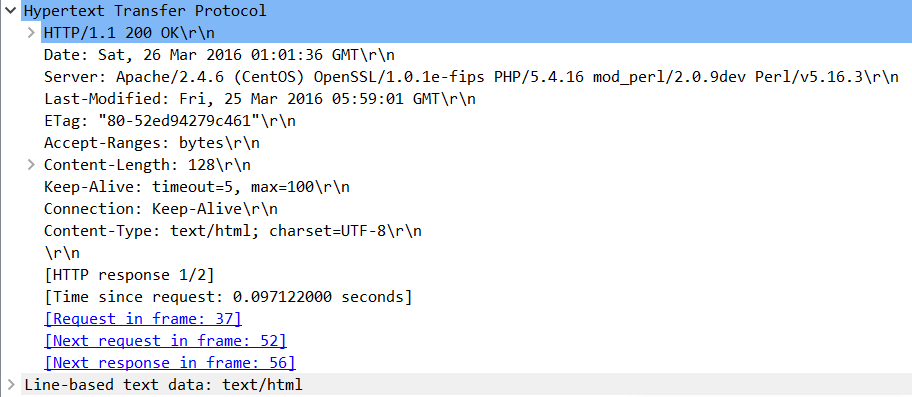
# Wireshark Lab 2

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

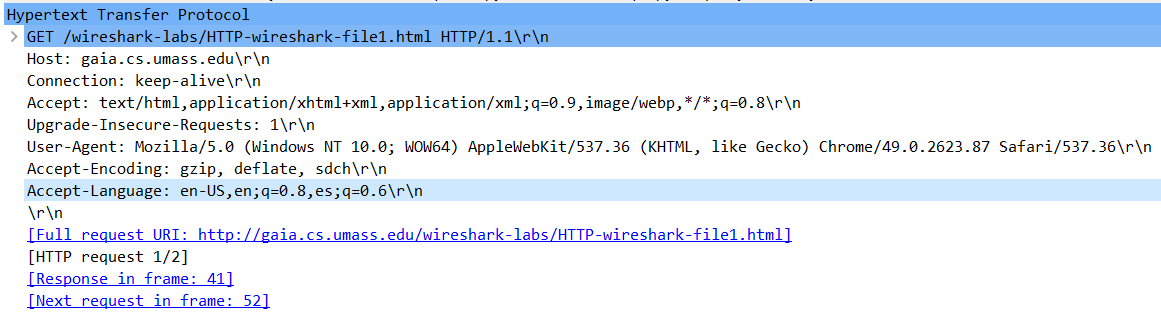


This previous image denotes that my browser is running HTTP/1.1. The GET line in the header clearly shows this right before CRLF.

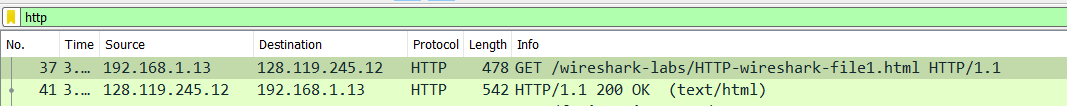


This image shows that the server is also running HTTP/1.1

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

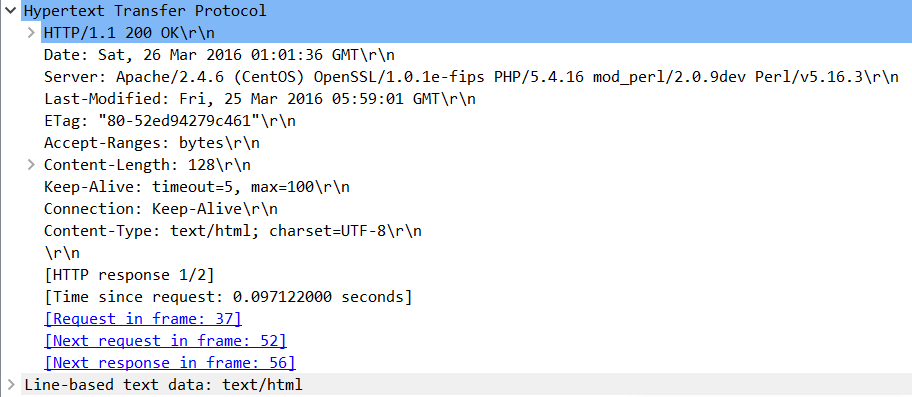
According to the highlighted portion of the last image, the browser can accept only US English.

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



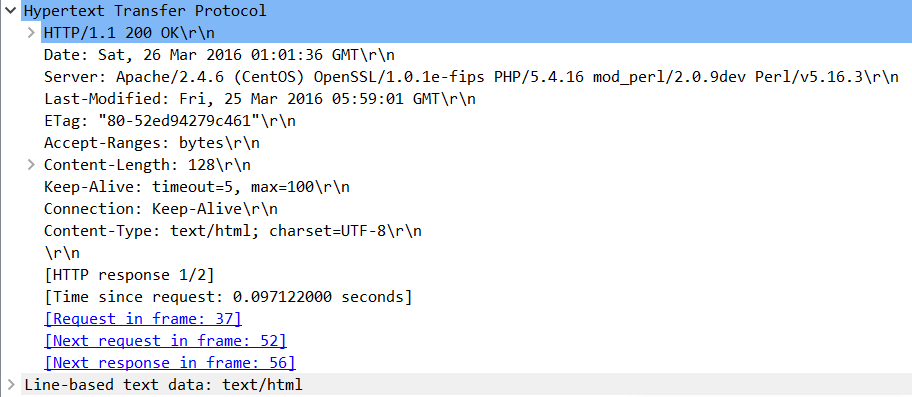
Number 37 shows that my source IP is 192.168.13. The address of gaia.cs.umass.edu is shown on the same line as destination and is 128.119.245.12

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



This image shows that the Response was 200 OK

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



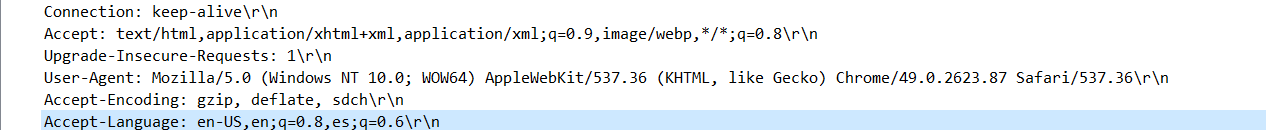
Highlighted in the previous image states that this was last modified Fri, 25 March 2016 05:59:01 GMT

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

Highlighted in pink on the last image shows that the Content-Length of the document was 128 bytes.

7. By inspecting the raw data in the packet content window, do you see any headers

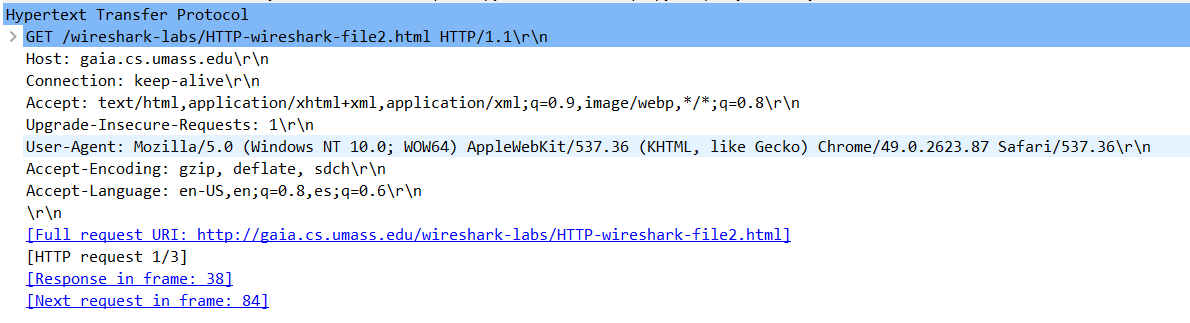
within the data that are not displayed in the packet-listing window? If so, name one.



Accept-Encoding is a header that is not found in the packet-listing window pane.

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

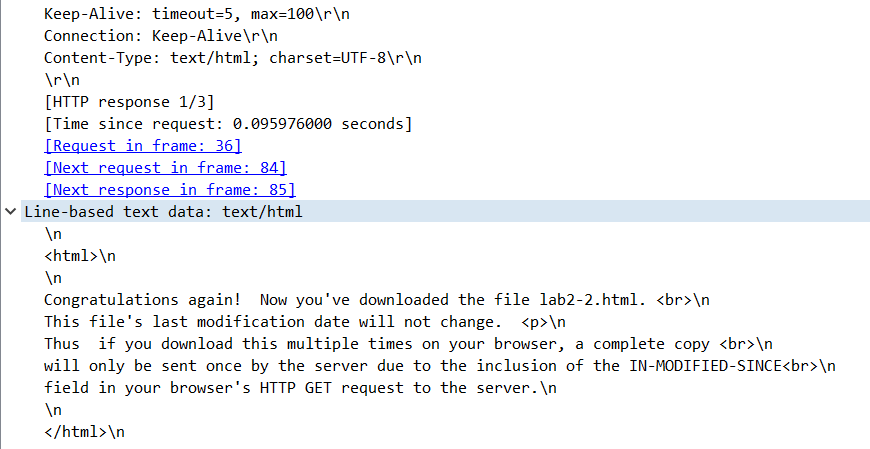
server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?



The first GET request does not contain an IF-MODIFIED-SINCE conditional.

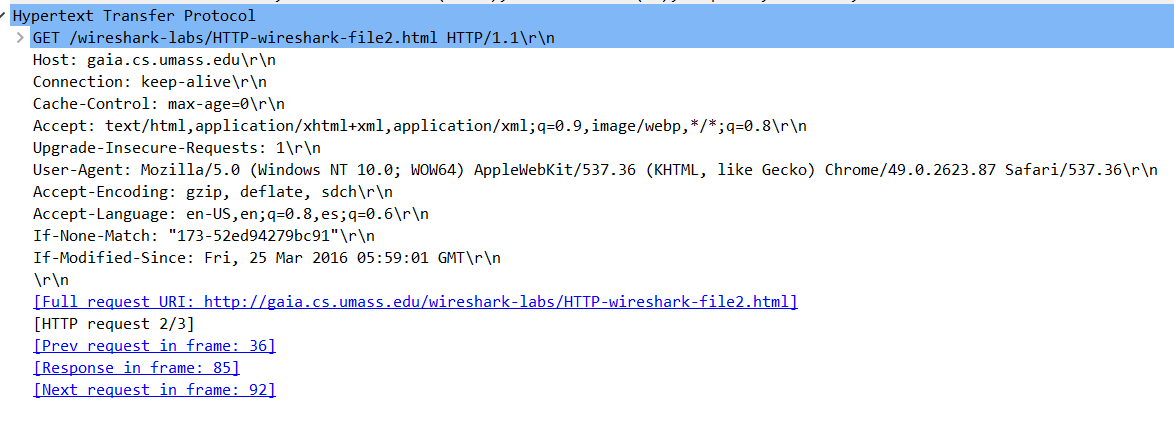
9. Inspect the contents of the server response. Did the server explicitly return the

contents of the file? How can you tell?



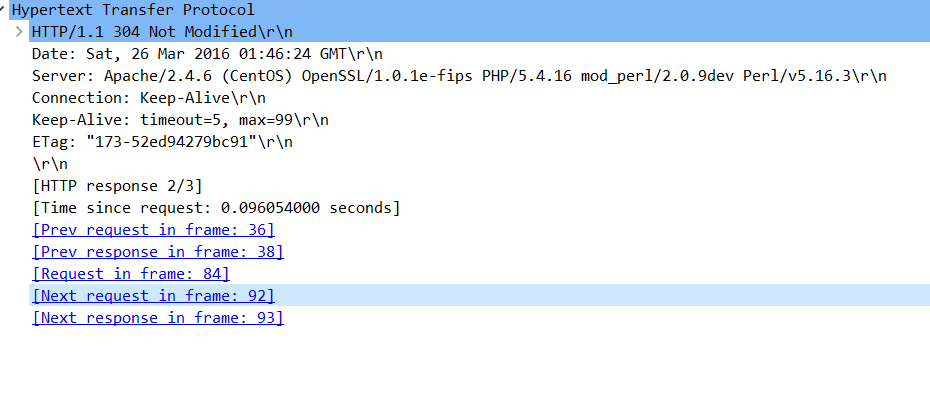
The file is explicitly returned to the requester as shown in the “Line-based text data”. The format of the data is in text/html.

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?

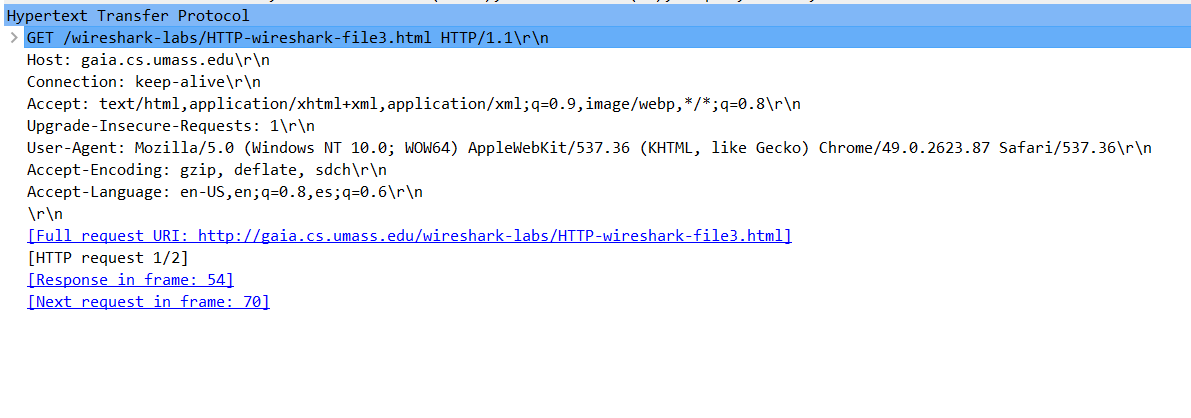


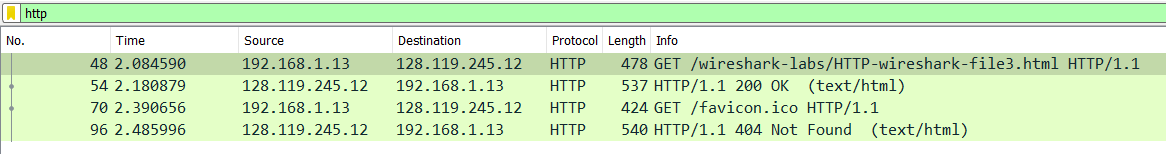
Unlike the first GET request, the second does have an “If-Modified-Since” condition. This is followed by the date that indicates the last modification to the file.

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 HTTP Status code of the second response is “304 Not Modified” which. Also, this second response lacks the “Line-based text data” information, which means the server did not respond explicitly with the file data.

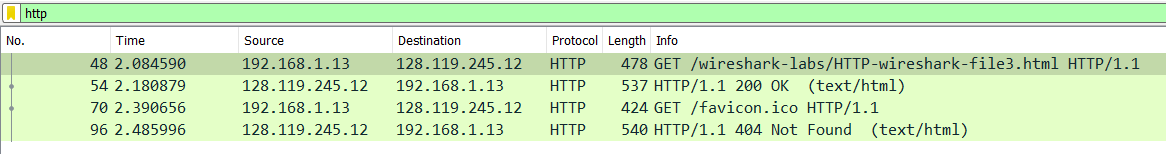
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?



Only a single GET Request was sent by the browser. This is shown above because the trace does not give information to show that it was reassembled from many requests. 

Packet number 48 was the packet that contained the GET message for the Bill of Rights.

13. Which packet number contains the status code and phrase associated with the response to the HTTP GET request.

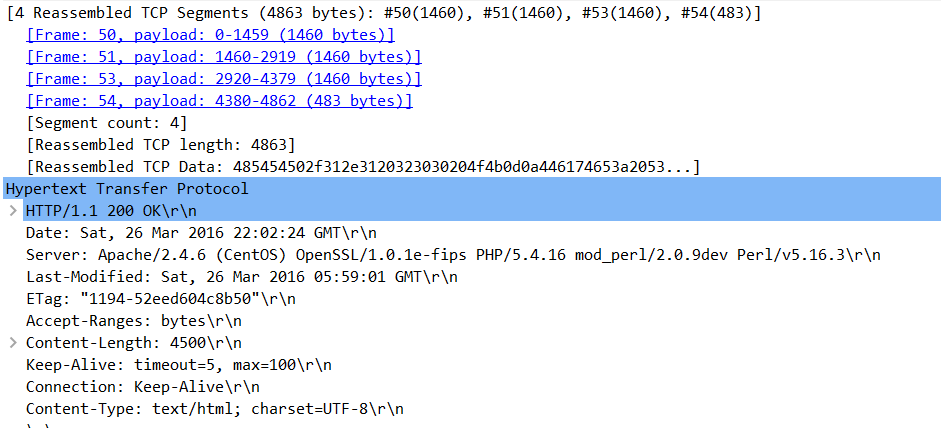


Packet number 54 contains the status code and phrase associated with the HTTP GET request.

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

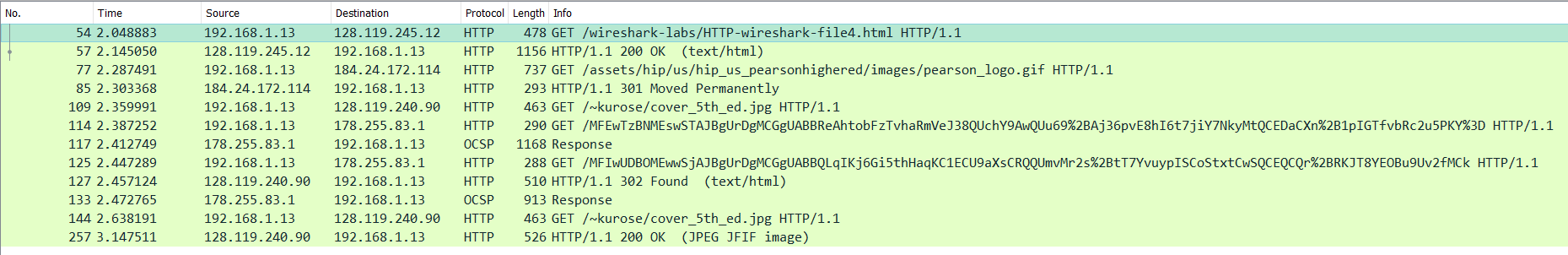
Using the same image above, we can see that the response read status code 200 and phrase OK.

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



The yellow highlighted portion of the packet information shows that there were four data-containing TCP segments used to carry the single HTTP response and text of the Bill of Rights.

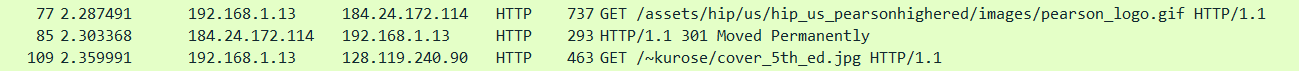
16. How many HTTP GET request messages did your browser send?



There were six GET requests sent by my browser as highlighted above.

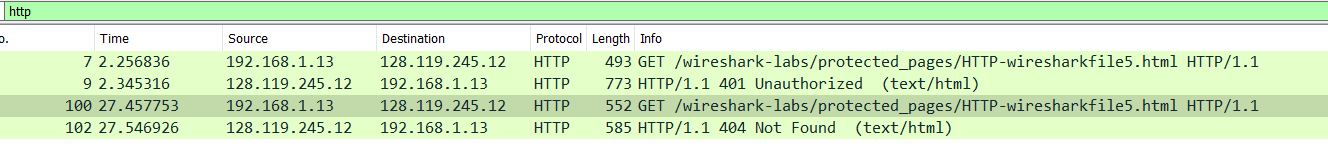
One of the requests was sent to 128.119.245.12, another was sent to 184.24.172.114, the third and last was sent to 128.119.240.90, and two were sent to 178.255.83.1. Upon research and data searching it seems that two of the six requests were anomalies and were sent by Microsoft on behalf of my machine.

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



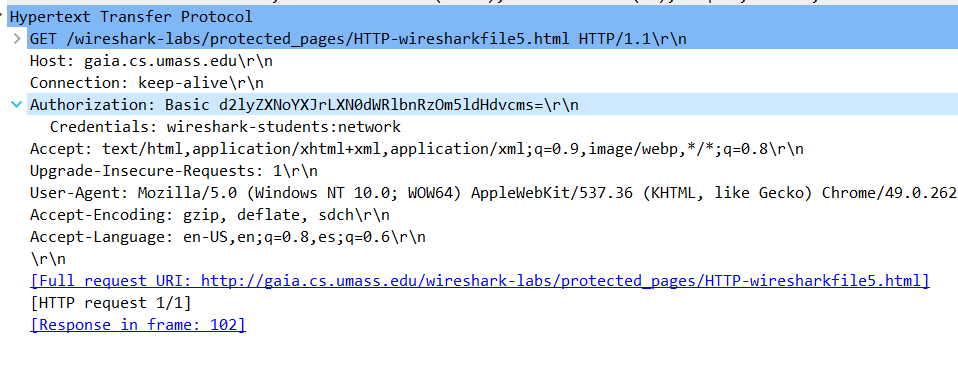
It appears, that the time stamp indicates the images were downloaded serially. That is, because one happened before the other, they couldn’t have been downloaded in parallel.

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



The initial response from the server when my browser sent the GET request was status code 439, with the phrase “Unauthorized.”

19. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?



The second GET request included the “Authorization” field in the headers list. Wireshark decodes the credentials for us and displays this when clicking the drop-down caret.