Arthur Liou

CS372

Lab 2

*Notes: I’ve attached my screenshots and boxed in red where I annotated my output.*

**Section 1**

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

Running HTTP/v1.1

Running HTTP/v1.1

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

I’m assuming the language/file type that the server can accept, but also adding languages to

Accept:

* text/html,
* application/xhtml+xml,
* application/xml;

From “Accept languages:”

* en-US
* en

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

My Computer: 192.168.146.130

Server: 128.119.245.12

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

200

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

Monday, October 15, 2018 05:59:01 GMT

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

552 bytes are returned in the 200 status code request.

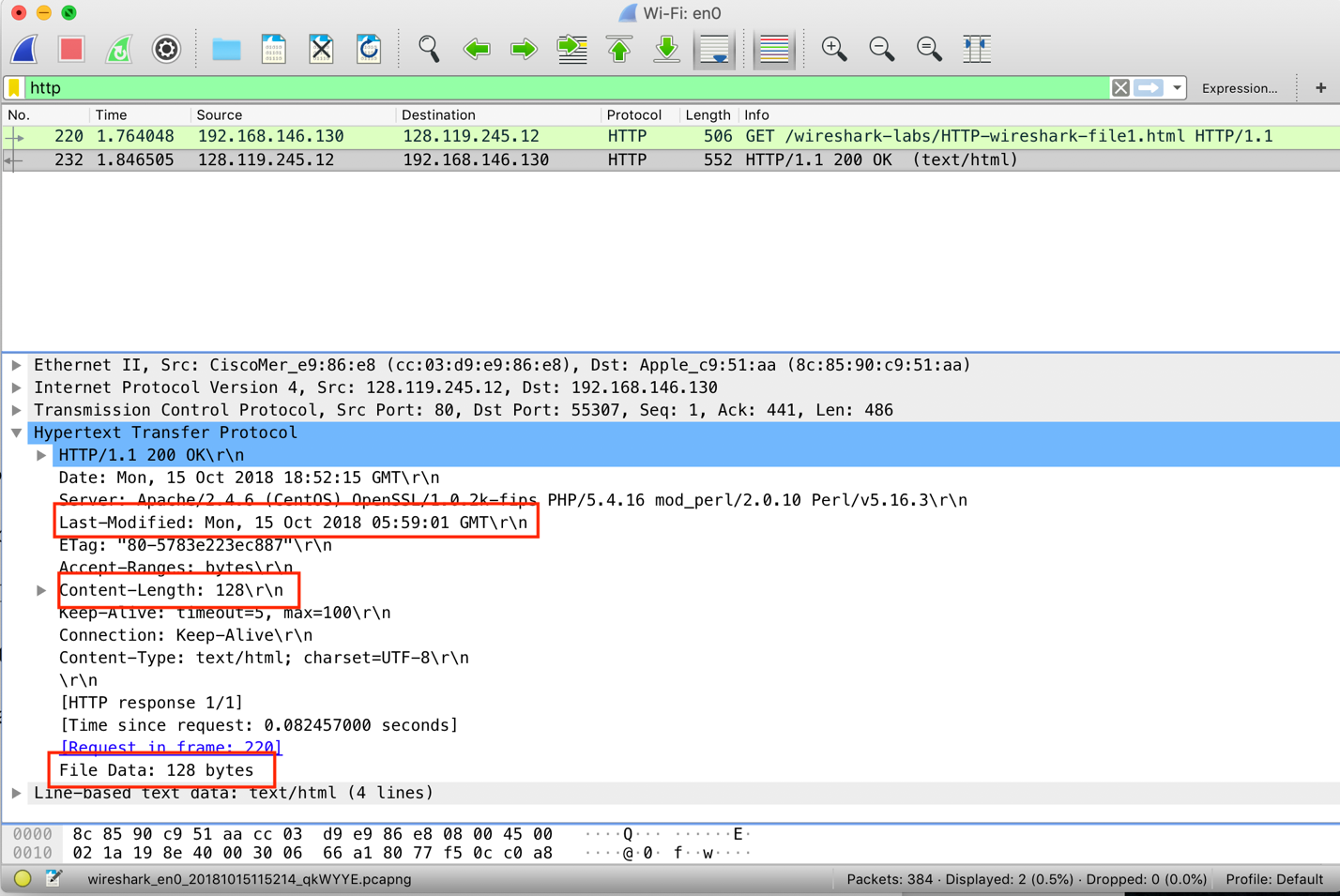
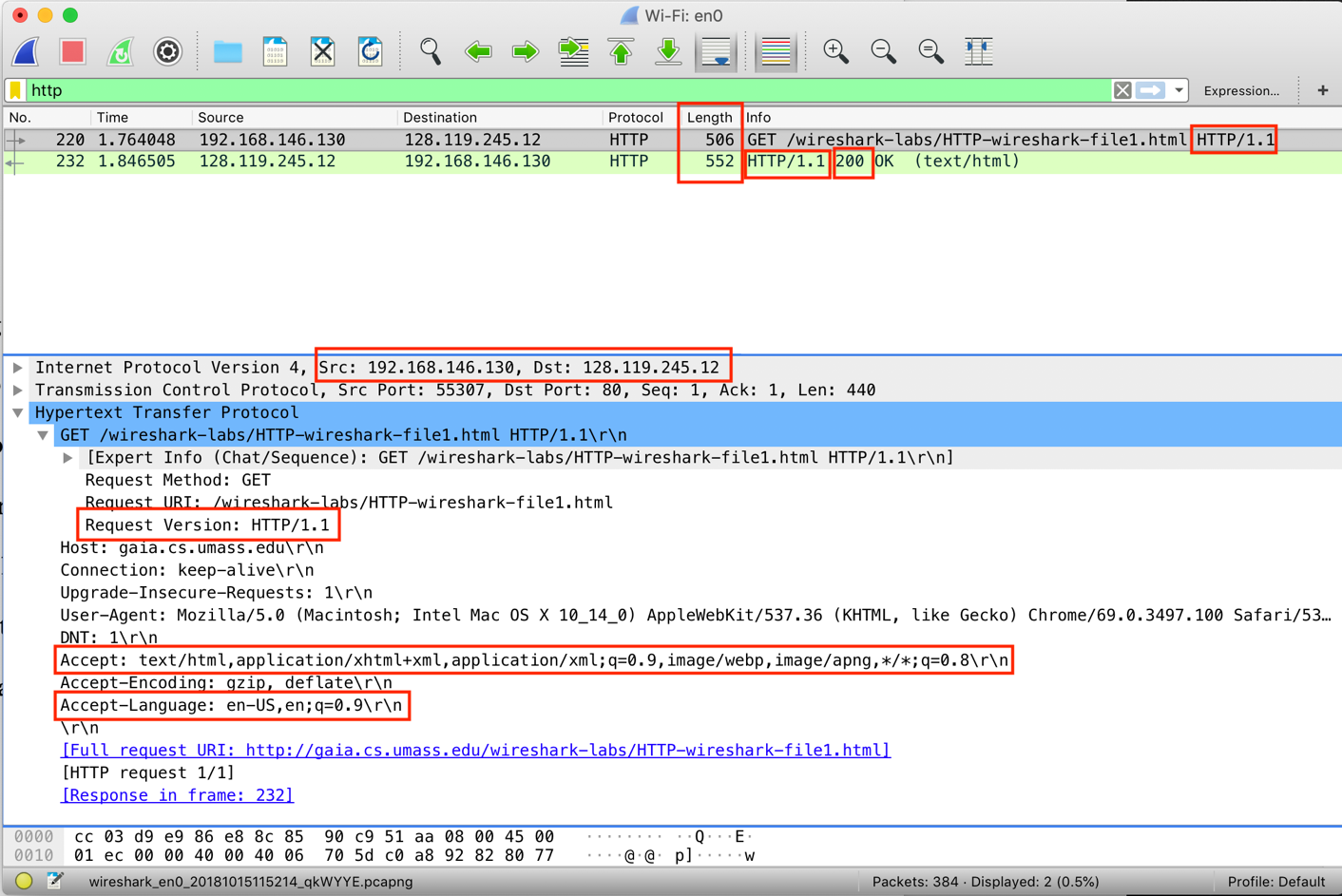
For content, it shows that file data is **128 bytes.**

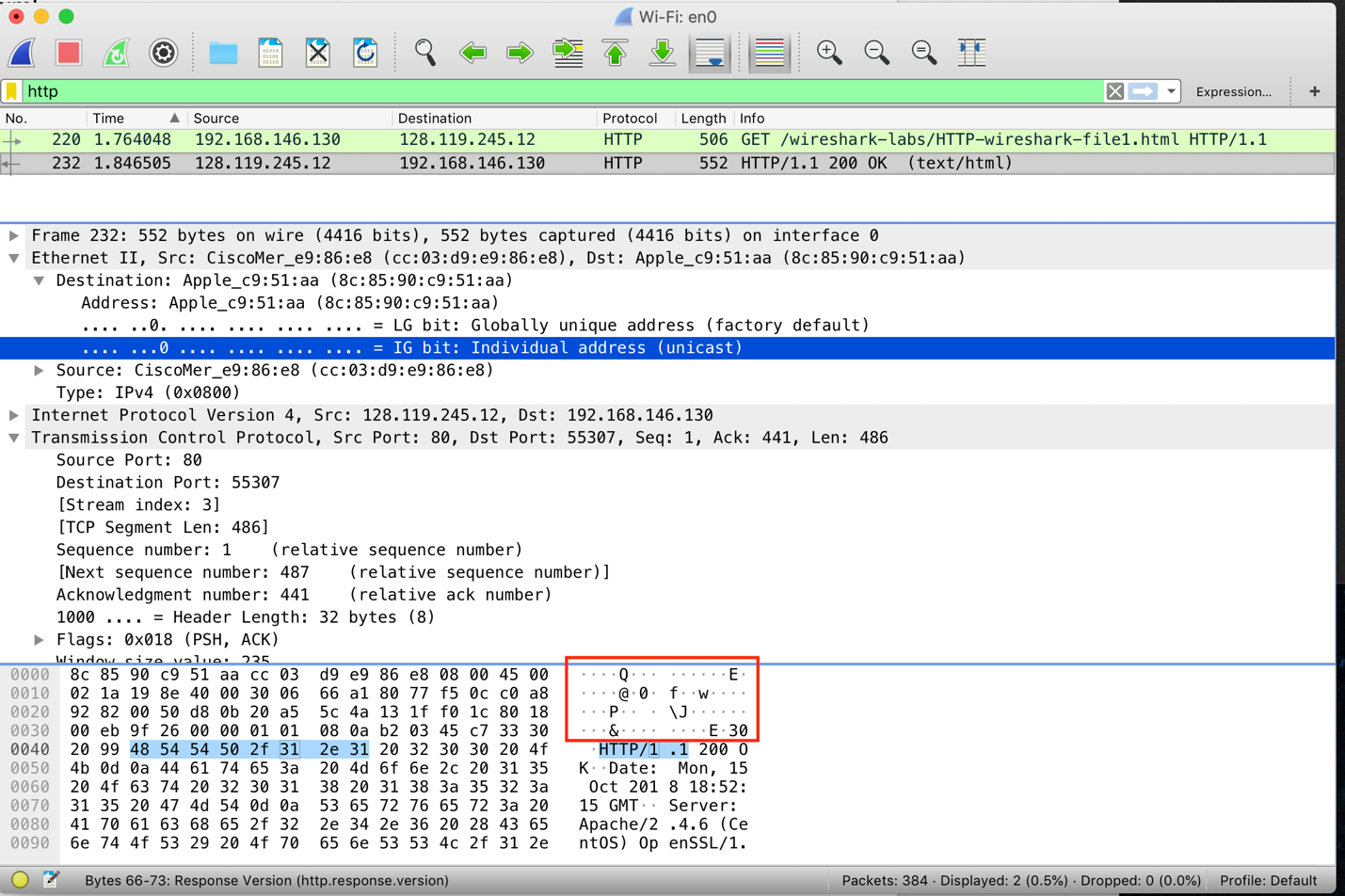
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one

Yes, Server info (Apache, etc.), Date, last modified, etc. These, and more, are not shown in the packet-listing window (I’m assuming just the summary), but are shown in the details of the selected packet from the packet-listing window.

Headers wise, I see an interesting “Q…E…@...(and more)”. Please see the screenshots for what I’m taking about

Screenshots for Section 1 (3x)





**Section 2**

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?

No, not in the first 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, I can see it under the “Line-Based Text Data” field.

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?

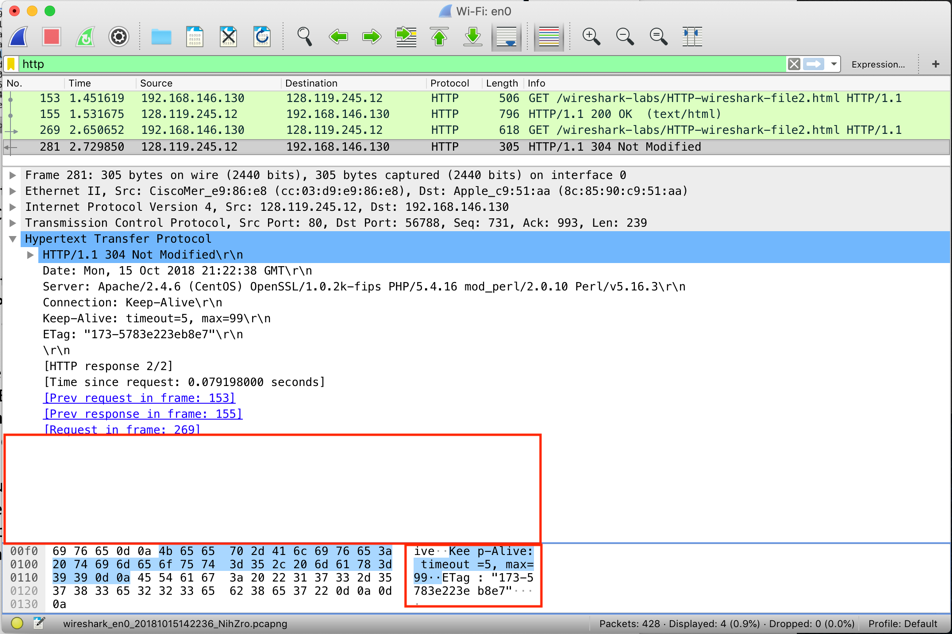
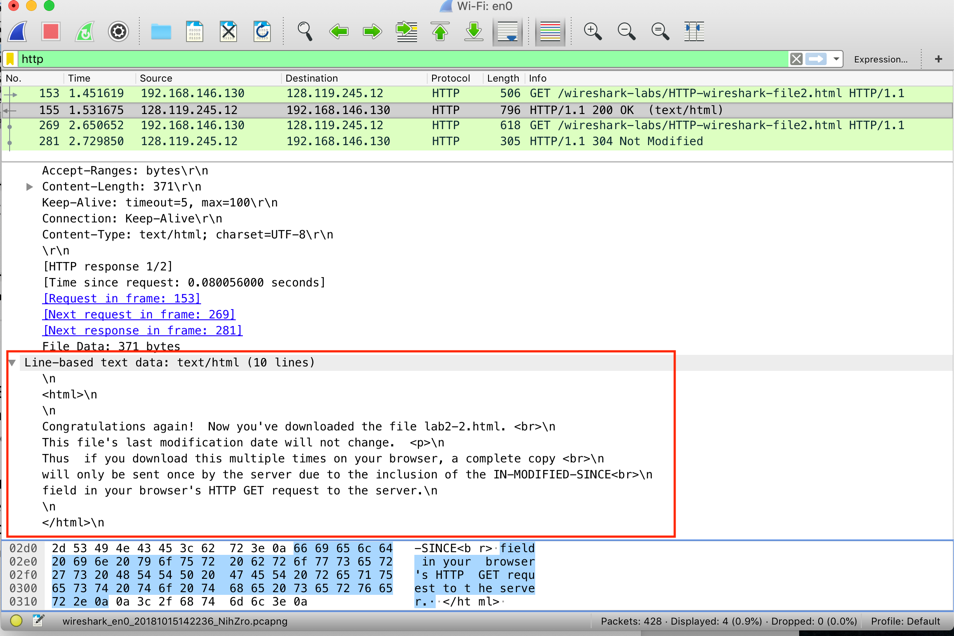
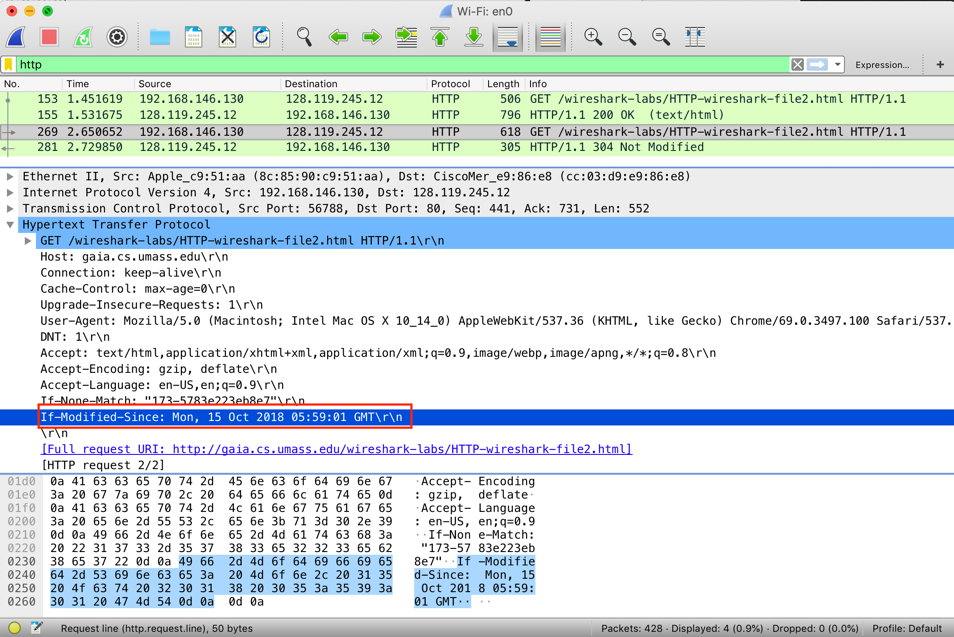
Yes, “If-Modified-Since: Mon, 15 Oct 2018 05:59:01 GMT\r\n”

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.

HTTP Status Code: 304 (Not Modified)

No, the server did not. I looked for the “Line-Based Text Data” field and within the raw data and didn’t see the file contents being explicitly returned by the server

**Screenshots for Part 2 (3x)**



**Section 3**

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?

1x HTTP GET request messages

Packet Number 117

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

Packet Number 124

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

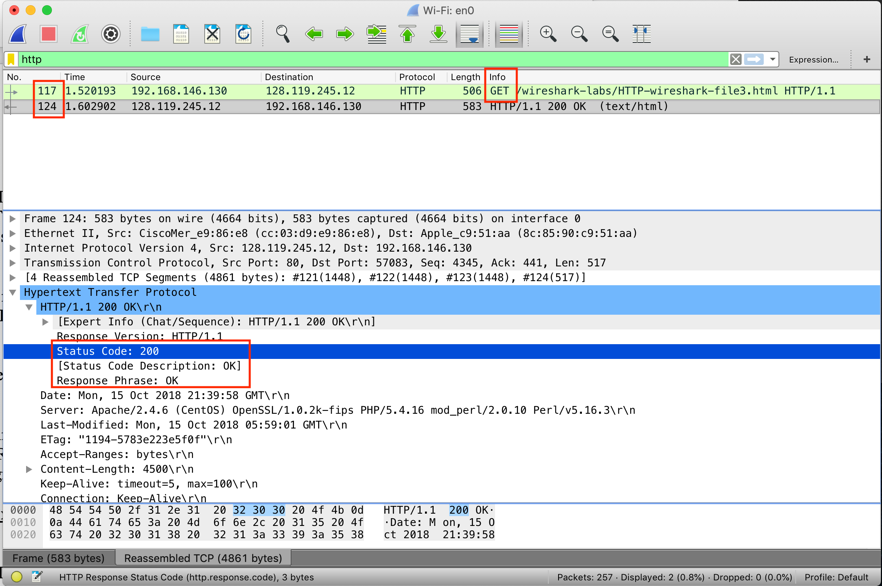
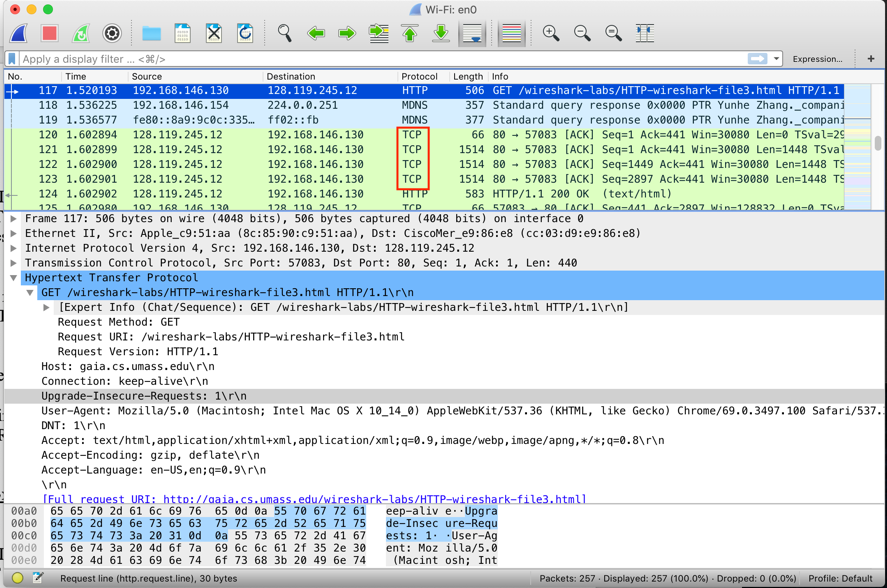
Status Code: 200

Response Phase: 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 data-containing TCP segments were needed.

**Screenshots for Part 3 (2x)**



**Section 4**

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

a) 3 HTTP GET request messages

@Instructors, please specify whether you want the IP address or the URL/web address (question could be considered ambiguous)

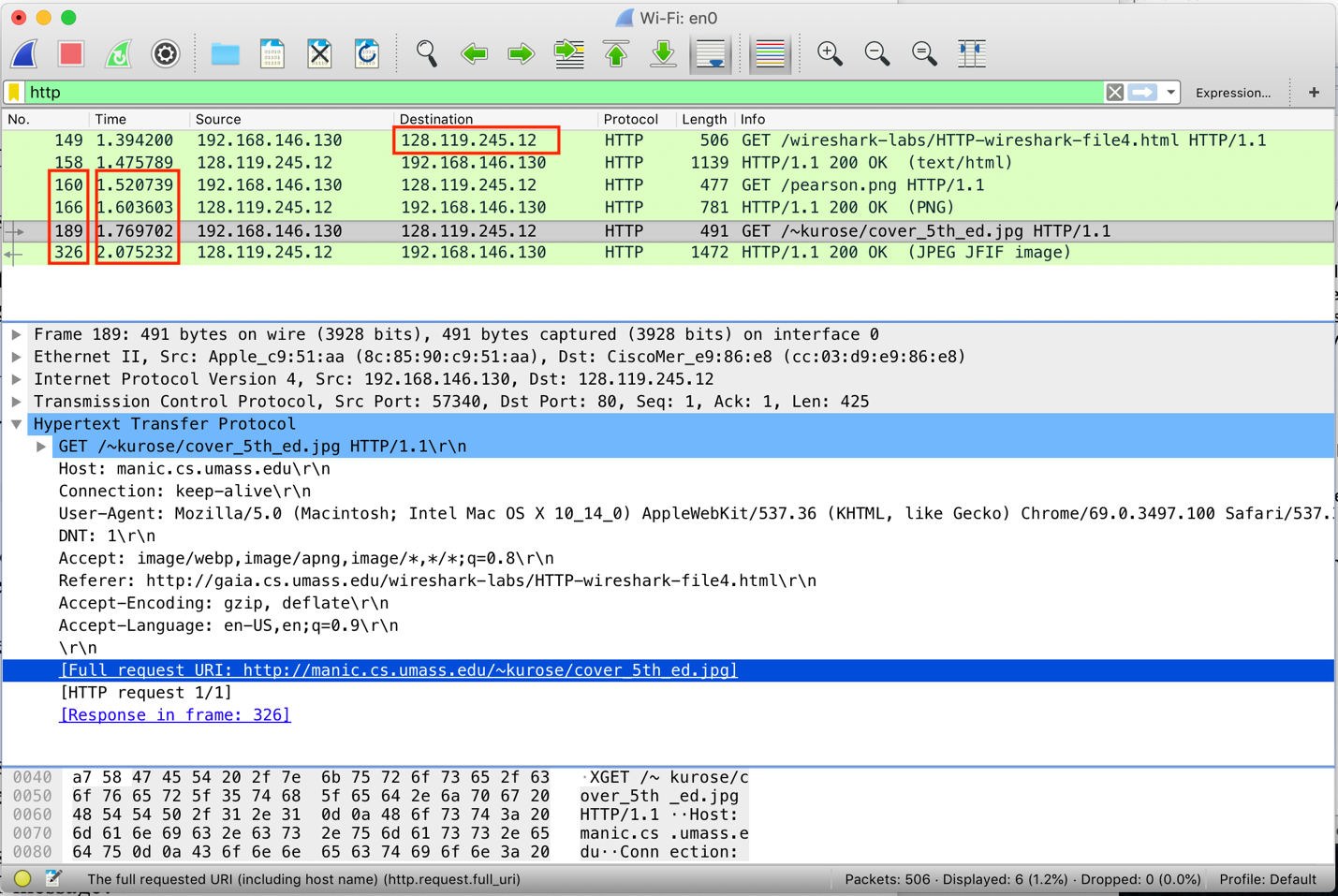
b) All 3 were going to the IP Address: 128.119.245.12

Web Address/URL

1. /wireshark-labs/HTTP-wireshark-file4.html
2. /pearson.png
3. /~kurose/cover\_5th\_ed.jpgs

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. In the screenshot, we can see major differences in time along side the fact that the second image GET occurred significantly after image 1’s GET completed. Packet 189 vs Packet 166. If they were downloaded in parallel, we would have seen both GET requests very close together (time and packet-wise). While it is possible that in parallel, the 1st GET request could come back before the 2nd GET goes out, it is not very likely (time to download from a server vs time to execute a request)



**Section 5**

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 (also includes credentials as a sub-field)

Screenshots for Section 5 (2x)

