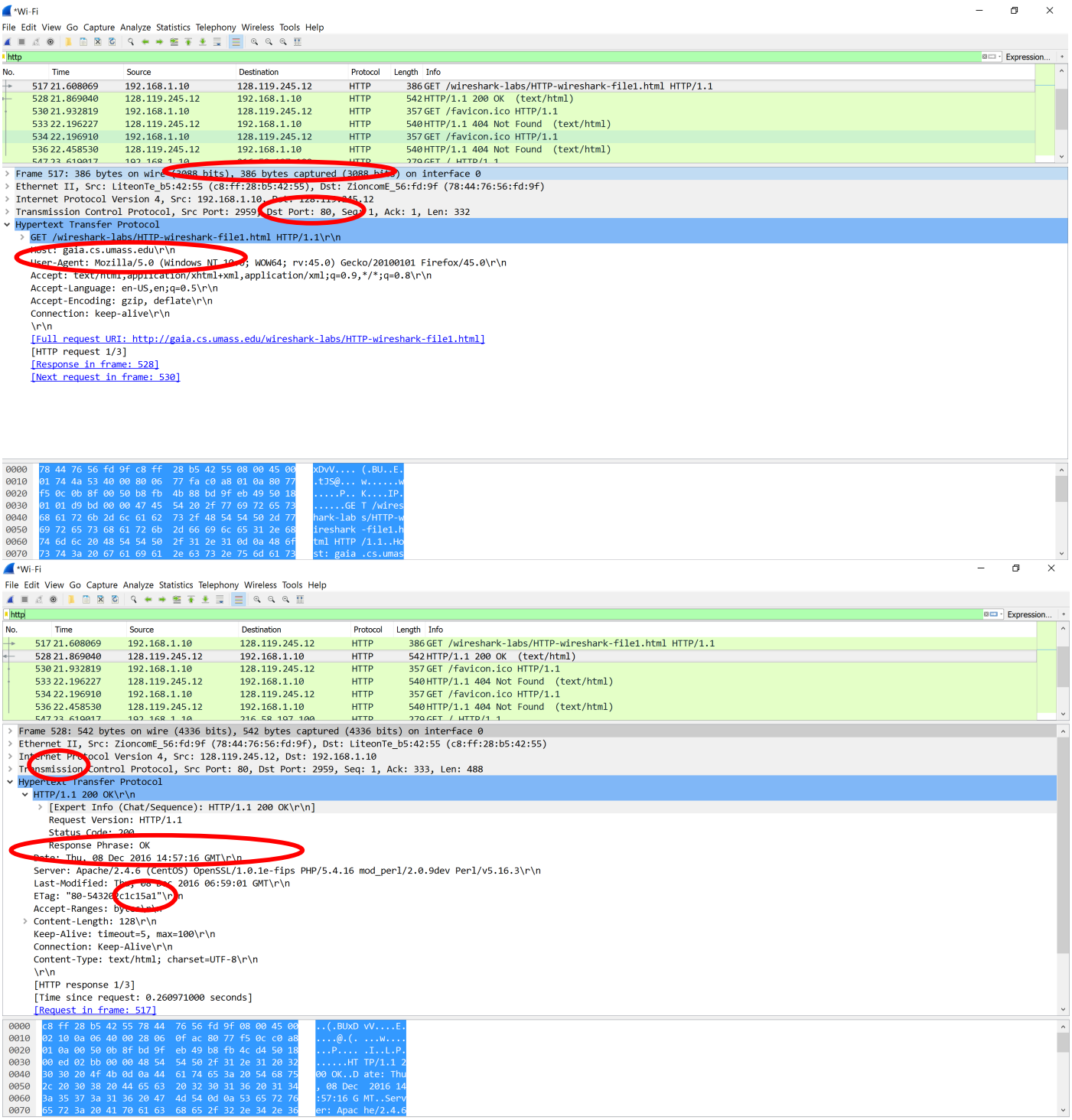
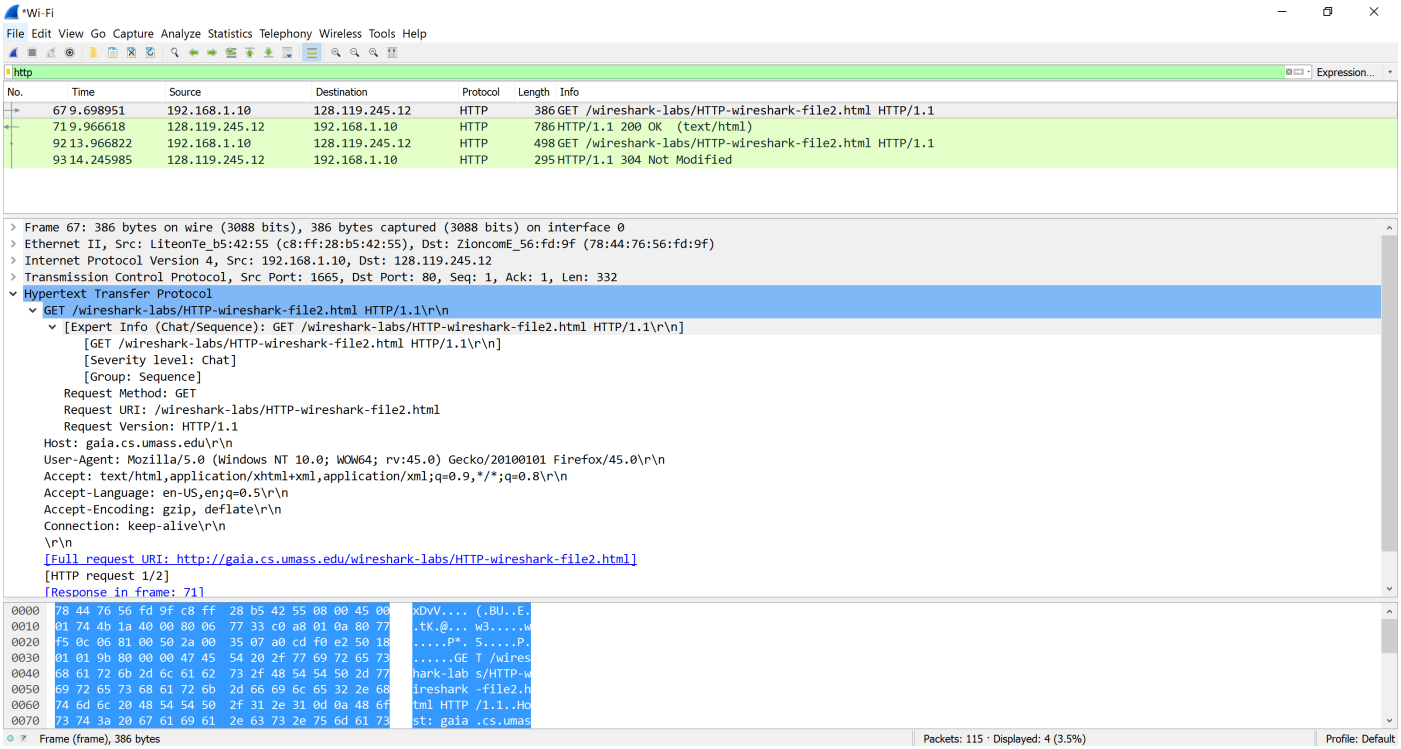
Wireshark HTTP

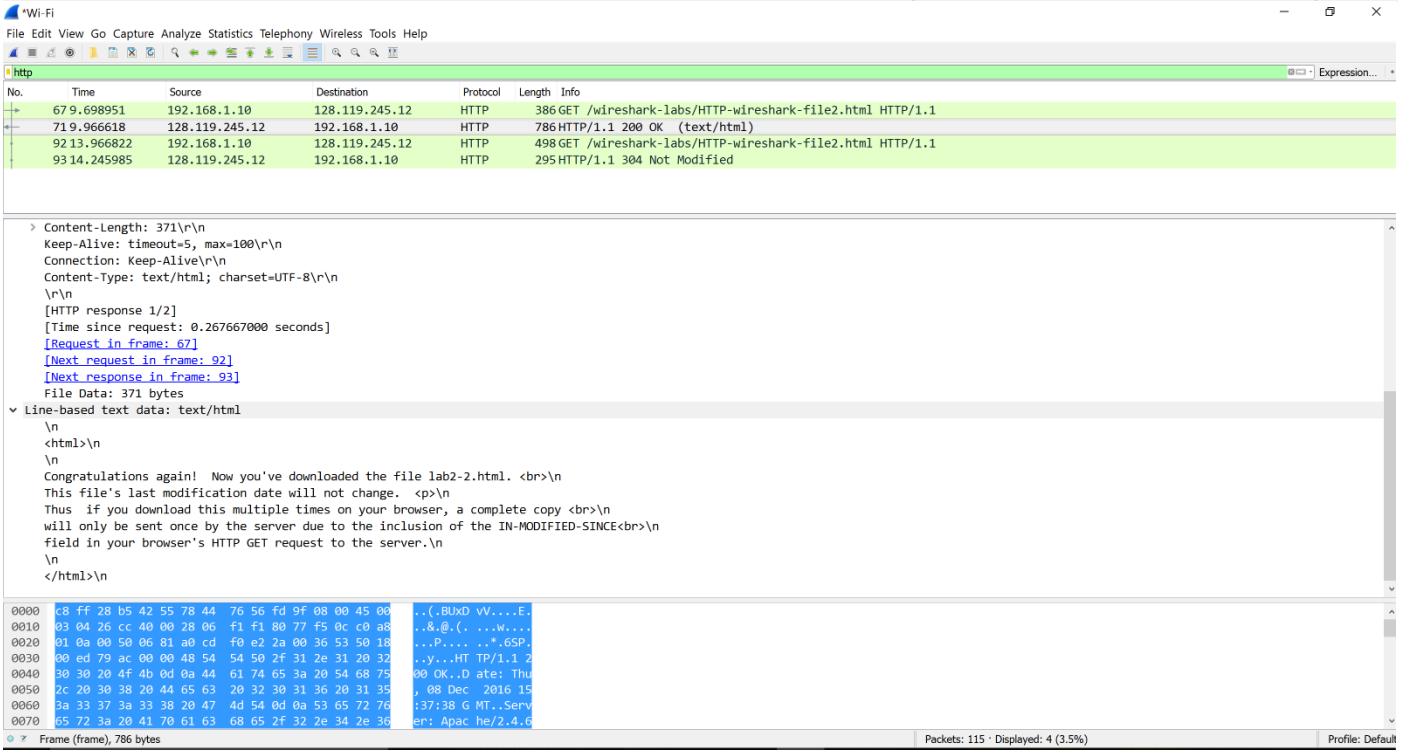


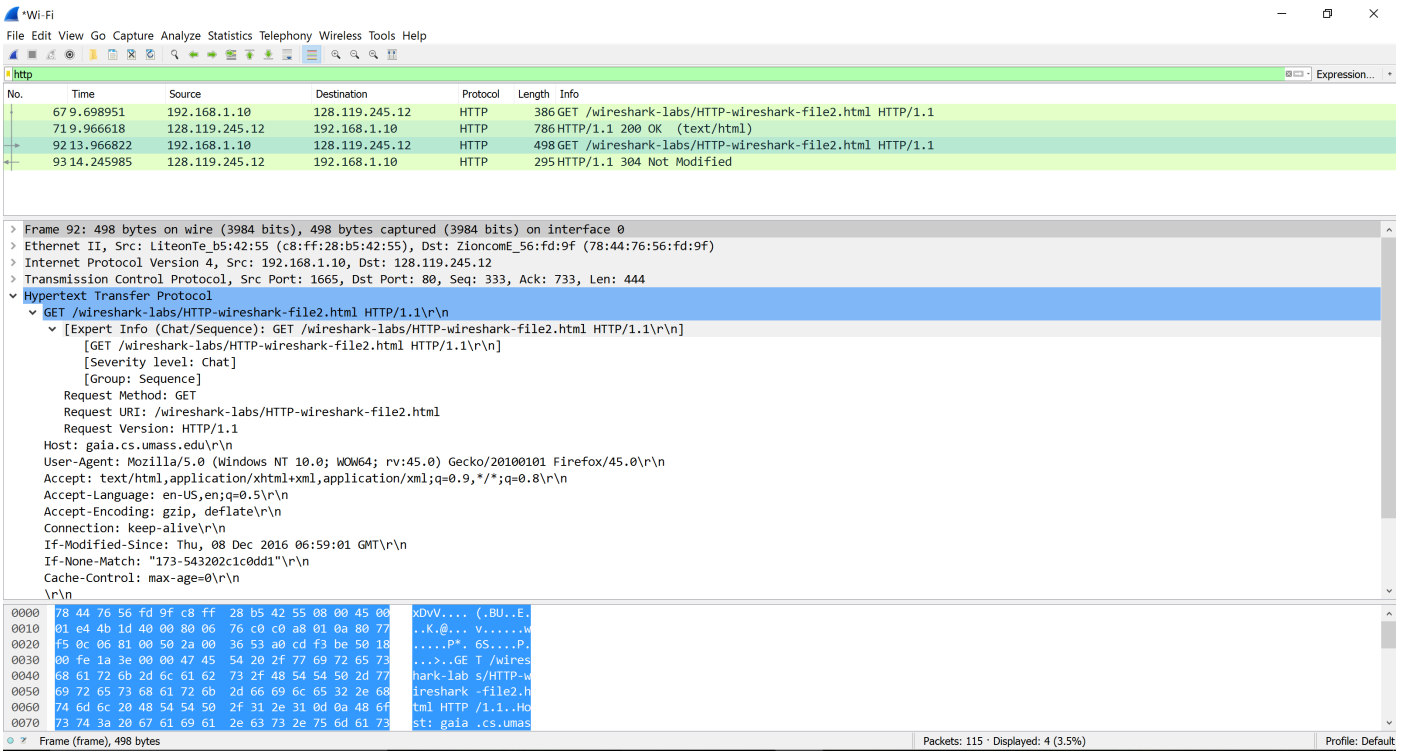
1. **Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?**
   Browser and server are running HTTP 1.1

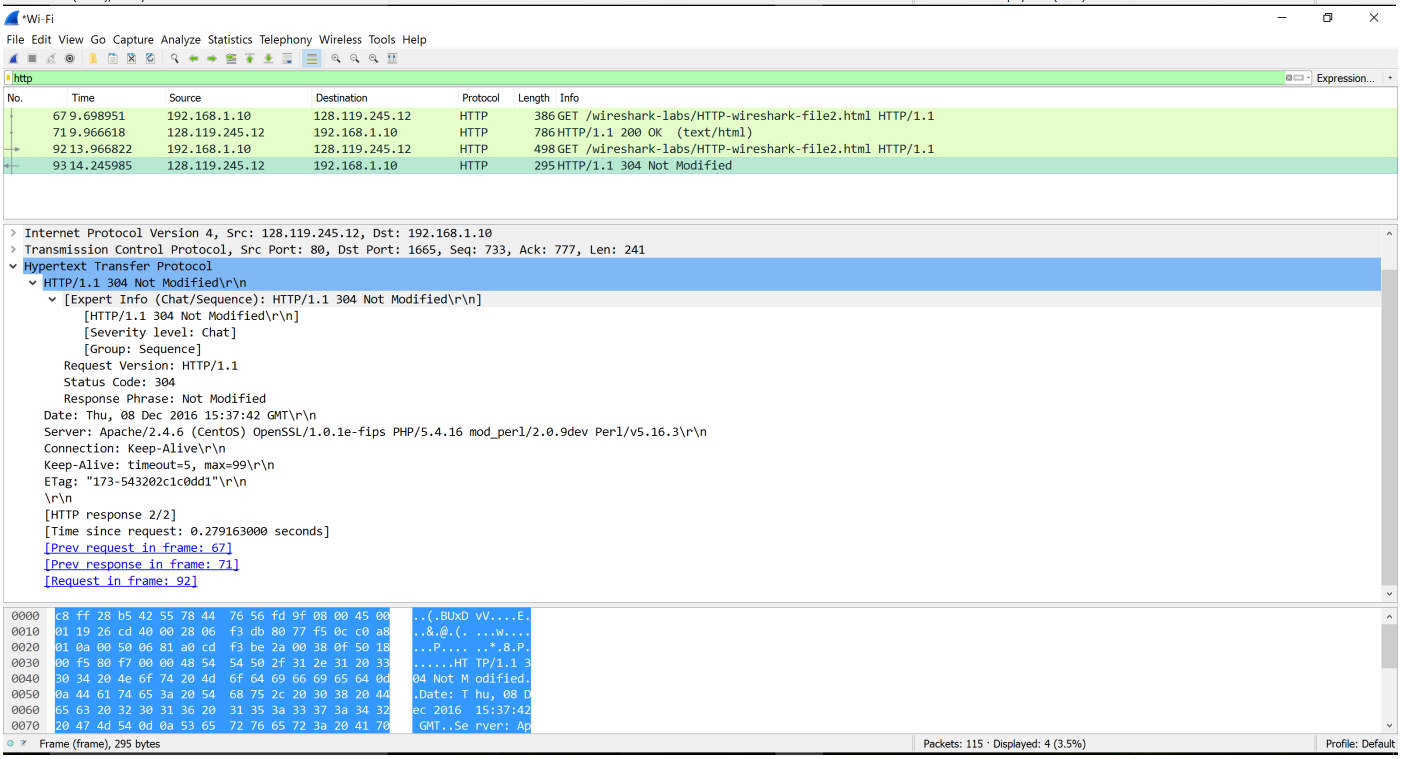
2. **What languages (if any) does your browser indicate that it can accept to the server?**
   Accept-Language: en-US,en;q=0.5\r\n
3. **What is the IP address of your computer? Of the gaia.cs.umass.edu server?**
   My computer: 192.168.1.10, gaia.cs.umass.edu:128.119.245.12
4. **What is the status code returned from the server to your browser?**
   200 OK

5. **When was the HTML file that you are retrieving last modified at the server?**
   Last-Modified: Thu, 08 Dec 2016 06:59:01 GMT\r\n
6. **How many bytes of content are being returned to your browser?**
   128
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.**
   No









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

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

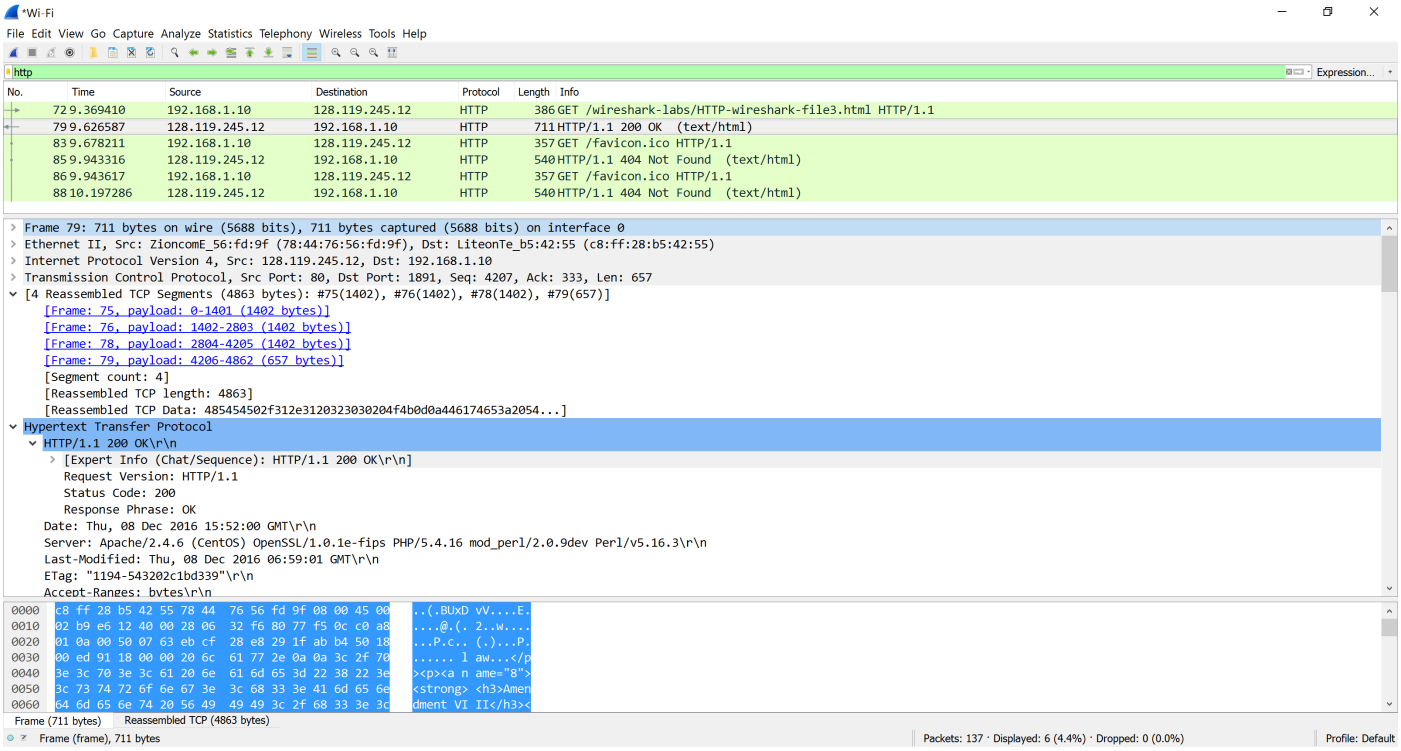
   Yes. Because of the line base text data field

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: Thu, 08 Dec 2016 06:59:01 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/1.1 304 Not Modified. The server didn't return the contents of the file since the browser loaded it from its cache.



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 sent. Packet 72

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

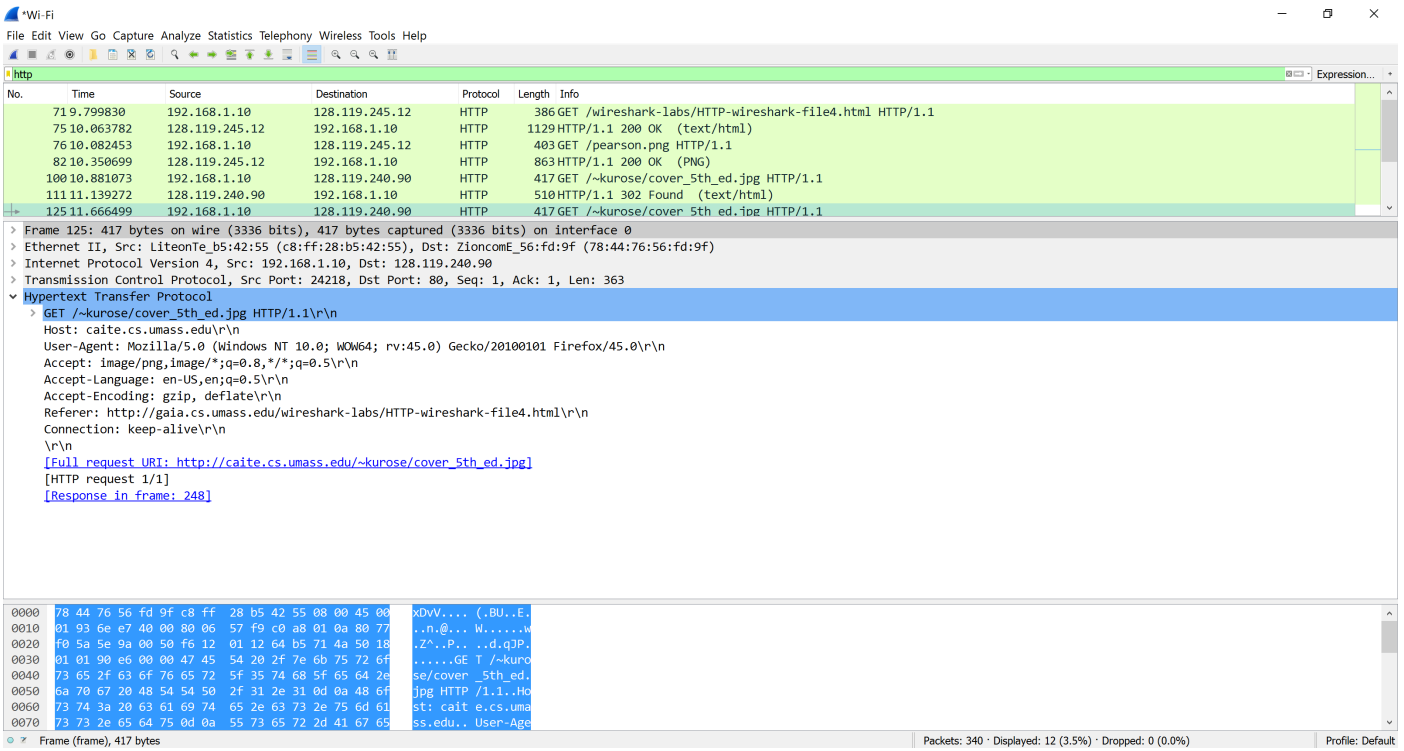
Packet 79

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

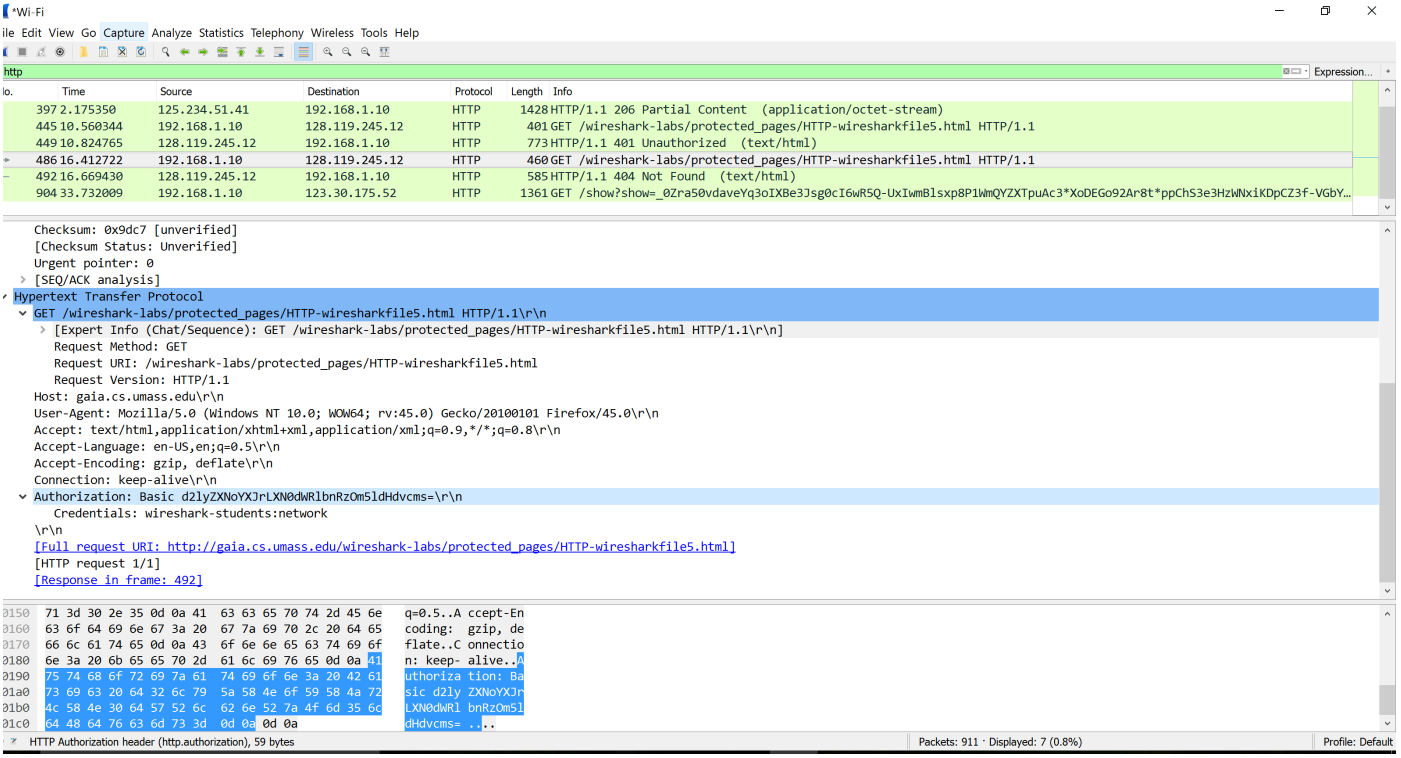


16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

4. Initial page: 128.119.245.12, Pearson's logo: 128.119.245.12, Cover 5th ed:128.119.240.90, 128.119.240.90

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.

Yes, by checking the TCP ports we can see if our files were downloaded serially or in parallel.



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 HTTP GET includes the Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n