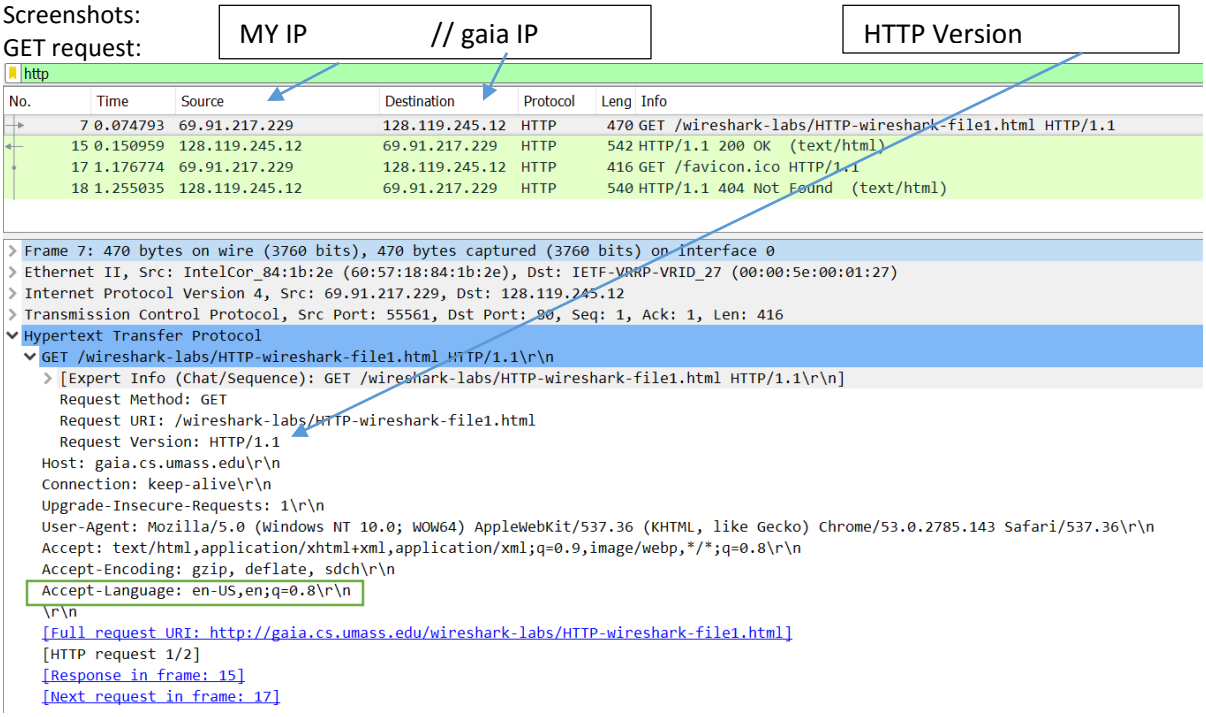
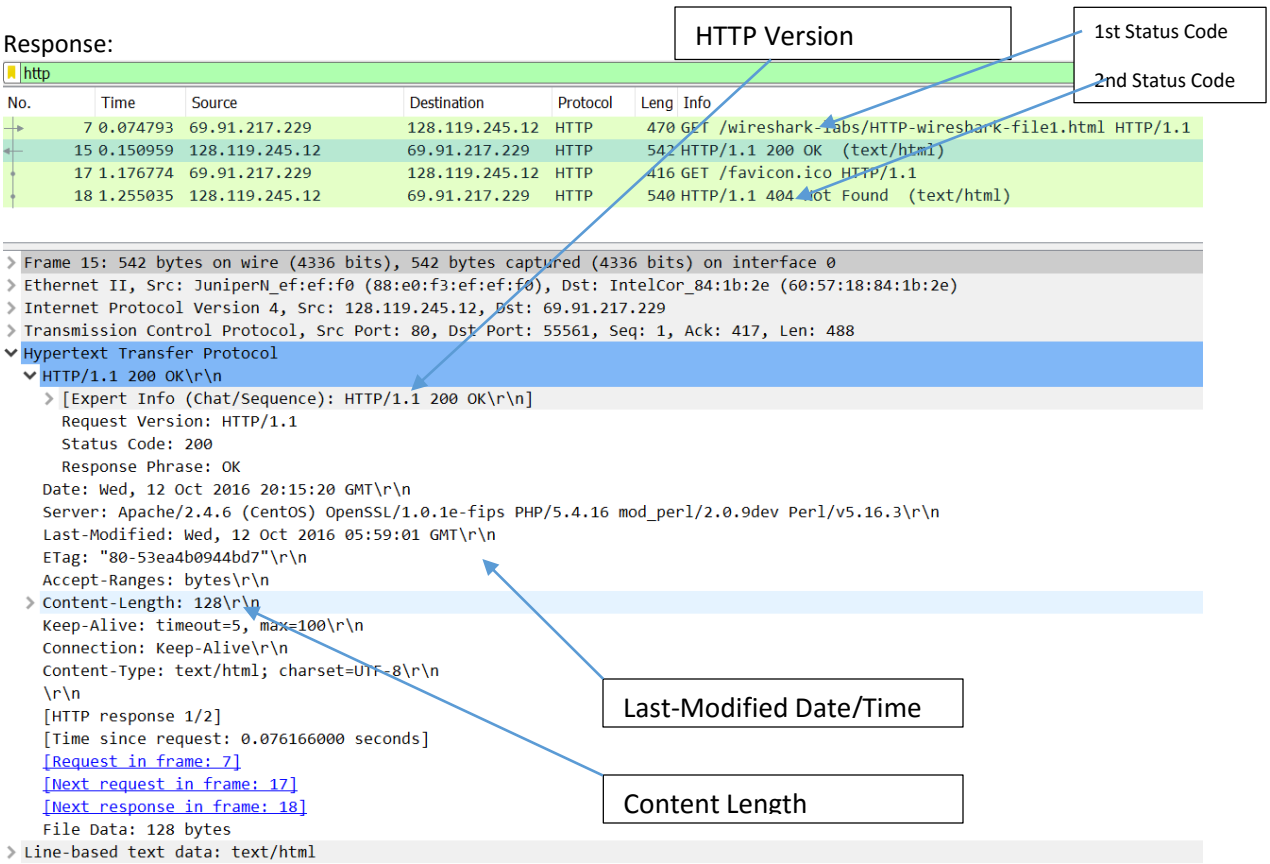
LAB 2 PART ONE

Screenshots:
GET request:



Response:



Questions:

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

   My browser is running HTTP version 1.1. The server is also running HTTP version 1.1

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

   The Accept-Language part of the header indicates that it will accept en-US or US English at a quality value of 1.0 then English at a quality value of .8

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

   My computer is at: 69.91.217.229
   The gaia.cs.umass.edu is located at: 128.119.245.12

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

   The returned status code for the first request was 200 or OK

   A second request was made and the server returned a status code of 404 or Not Found

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

   The date and time indicated by the last-modified field is Wed, 12 Oct 2016 and 5:59:01 GMT

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

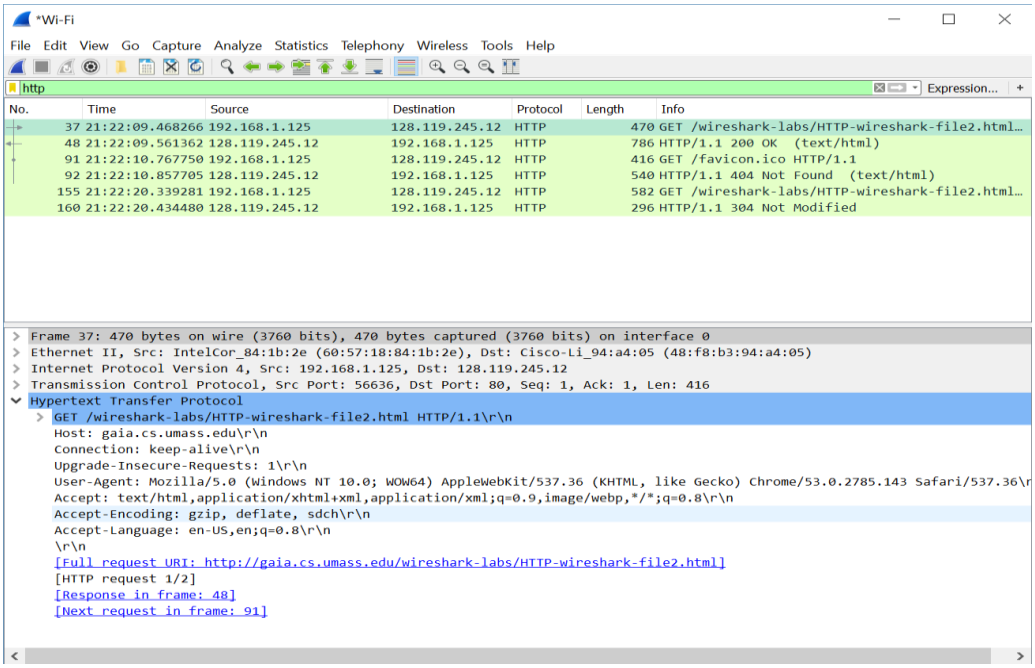
   128 Bytes are being returned to the browser

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.**

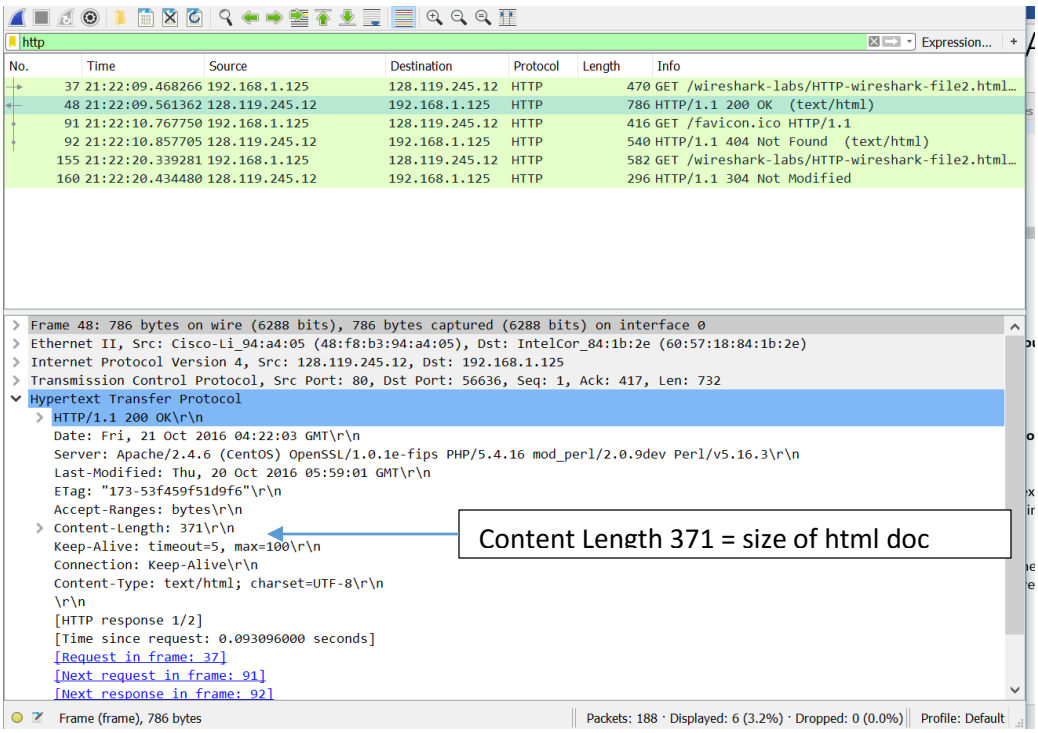
   Some of the data included in the other layers of the protocol are in the header including the acknowledgement number for the TCP and an Urgent Pointer which is also included in the TCP information.

PART 2

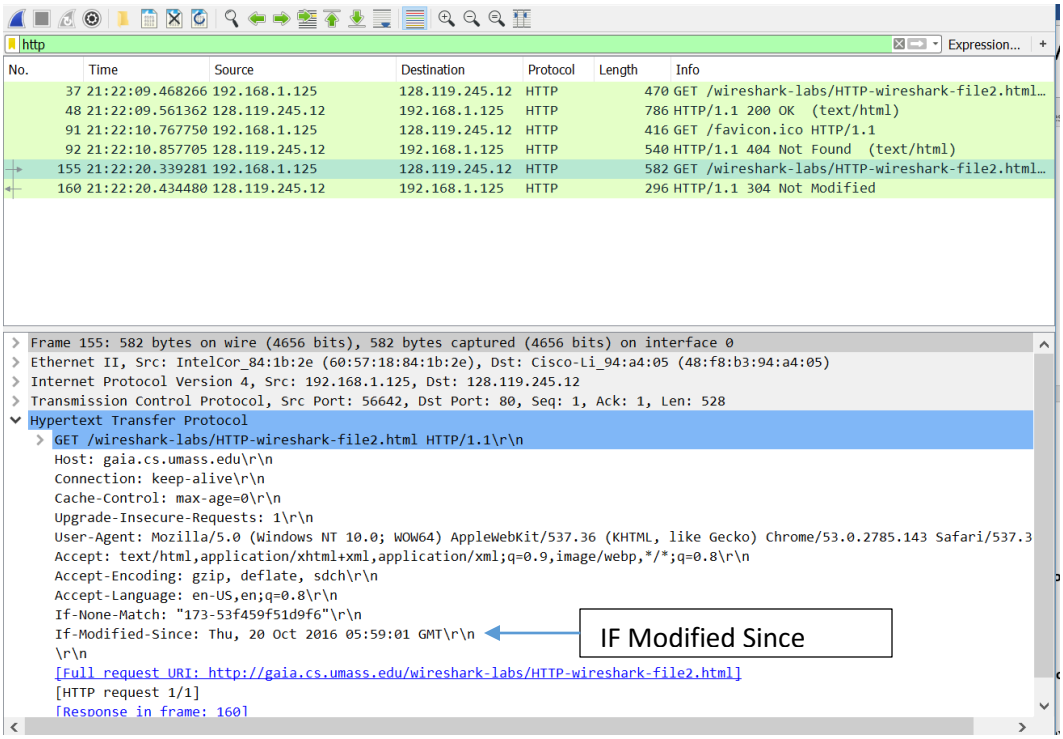
GET Request #1



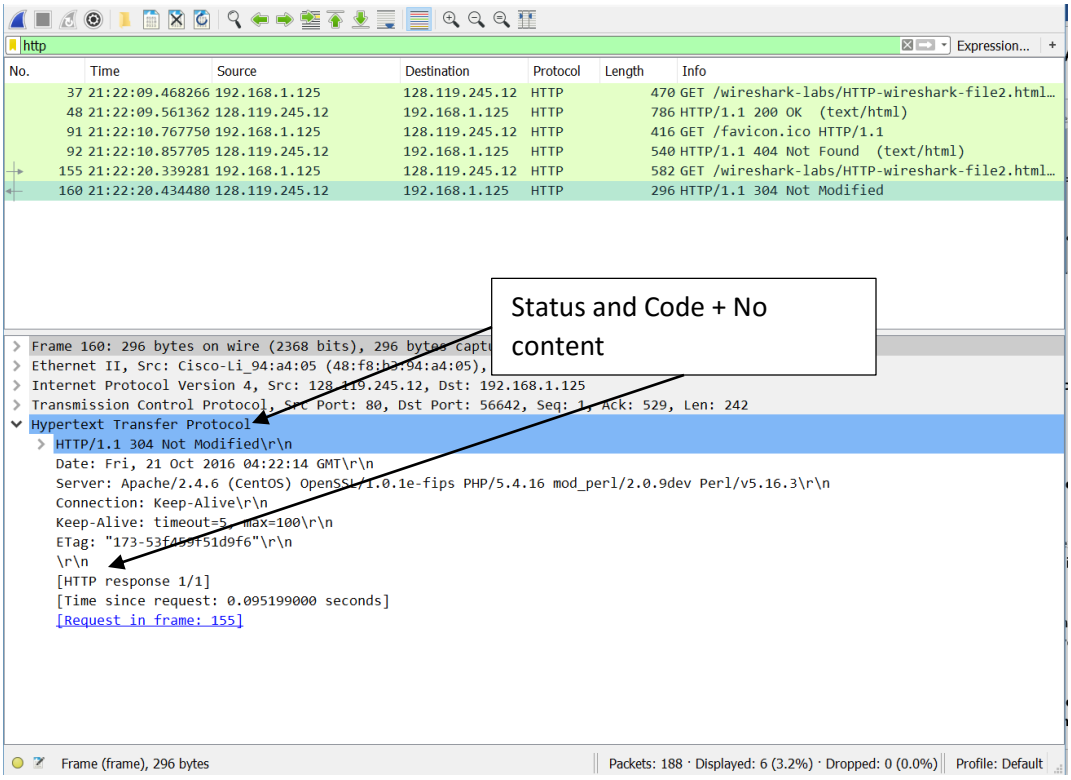
GET Response #1



GET Request #2



Response #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, it is not there.

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

   In the header it declares the content length being 371, which is the exact length of the text/html file. Meaning the server did not send anything extra beyond the file and the information in the response header.

   In the response header however there's an extra field called Etag which is sent back to the server in the second HTTP GET response, meaning it was likely sent by the server and saved by the client.

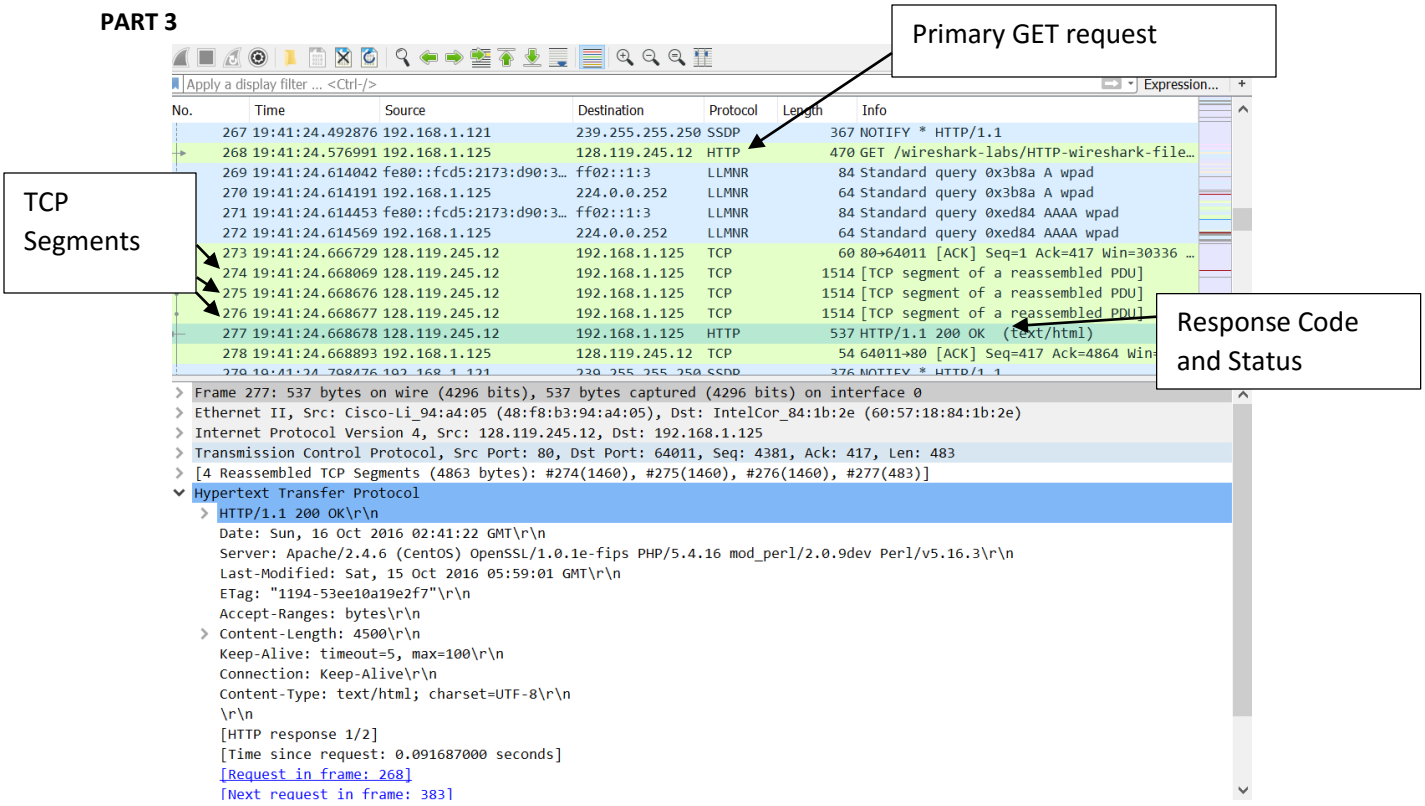
10. **Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?**

    The IF-MODIFIED-SINCE header is followed by the date Sat, 15 Oct 2016 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.**

    The HTTP Status code and phrase returned by the response to the second GET request is Status code: 304 with Response Phrase: Not Modified. The server does not return the contents of the file because it determined sending the contents of the file is unnecessary as the file had not been modified since it was previously sent. The ETag is sent again though.

PART 3



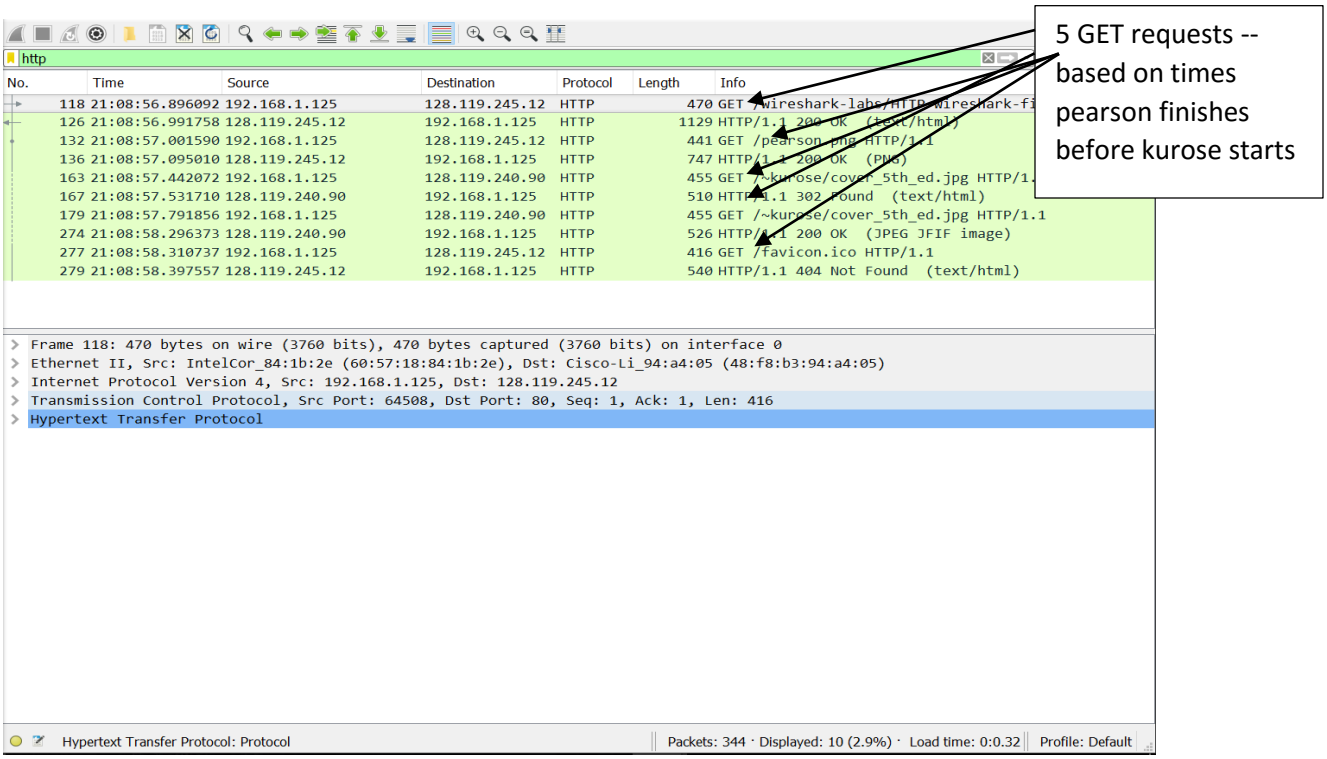
12. **How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?**
    My browser sent two GET requests, packet numbers 268 and 383. Packet number 268, the first one, contains the GET message for the bill of rights. The second request is requesting the /favicon.ico, which gets a 404 Not found response.

13. **Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**
    Packet Number 277 has the code and phrase associated with the response.

14. **What is the status code and phrase in the response?**
    The status is 200 and the phrase is OK.

15. **How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?**
    There were three TCP responses sent of length 1514 each.

PART 4



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

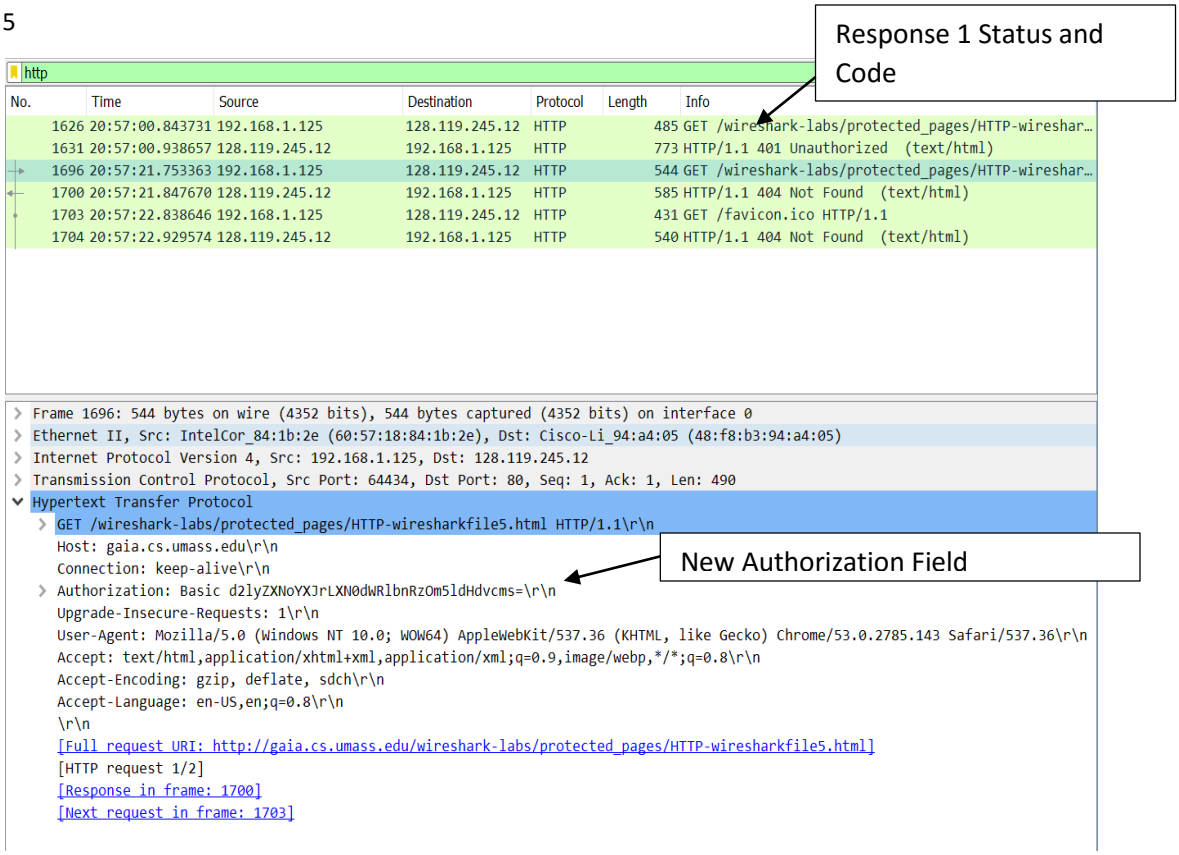
    There were a total of 5 GET requests sent from my browser.

    No. 118 gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
    No. 132 gaia.cs.umass.edu/pearson.png
    No. 163 manic.cs.umass.edu/~kurose/cover_5th_ed.jpg
    No. 179 caite.cs.umass.edu/~kurose/cover_5th_ed.jpg
    No. 279 gaia.cs.umass.edu/favicon.ico

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 two images were downloaded serially. You can tell it's done serially by the sequence of events. The second GET request is not made until the first response is received and the image is sent, meaning they are not happening at the same time as they would if the images were downloaded in parallel.

PART 5



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 in packet 1631 is a 401 status code with the 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?

There is a new field labeled Authorization in the second request followed by an alphanumeric phrase in Base64 format.