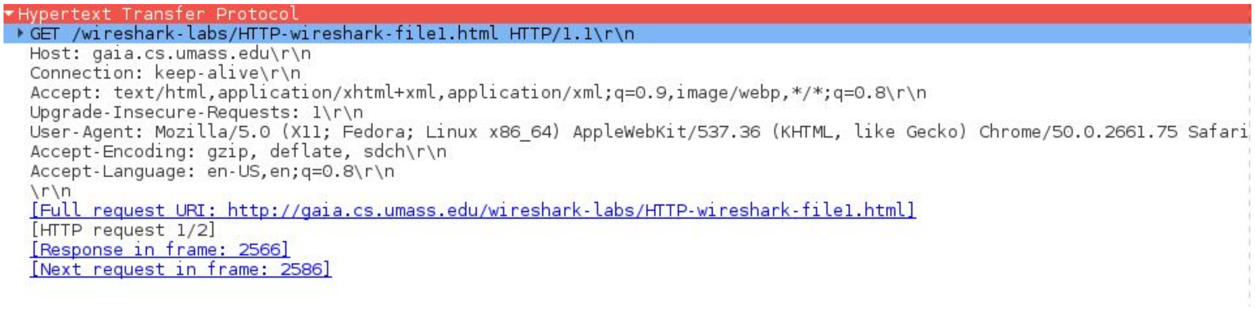
Kevin Stine
Lab 2 - HTTP

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 and the server is also running version 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?
   The browser can accept text/html, application/xhtml+xml, application/xml, and image/webp



```
▾Hypertext Transfer Protocol
 ▸ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
   Host: gaia.cs.umass.edu\r\n
   Connection: keep-alive\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
   Upgrade-Insecure-Requests: 1\r\n
   User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.75 Safari
   Accept-Encoding: gzip, deflate, sdch\r\n
   Accept-Language: en-US,en;q=0.8\r\n
   \r\n
   [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
   [HTTP request 1/2]
   [Response in frame: 2566]
   [Next request in frame: 2586]
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   My IP address is 10.0.0.6 and the server is 128.119.245.12

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

5. When was the HTML file that you are retrieving last modified at the server?
   It was last modified at Tuesday, April 19th at 5:59 GMT, which I believe is the time I accessed it

6. How many bytes of content are being returned to your browser?
   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?
   By inspecting the raw data, I'm able to see the html tags as well as all the newline characters

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?
   I do not see an if modified since line in the HTTP GET

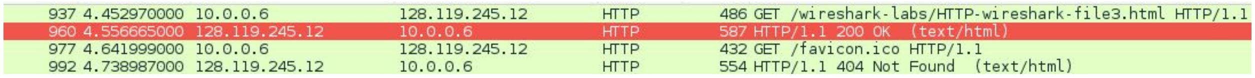
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   The server did explicitly return the contents of the file, since it has the section for line-based text data and it displays everything that the page had on it.

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 there is an if-modified-since line which says “If-modified-Since: Tue, 19 Apr 2015 05:59:02 GMT”

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 server did not explicitly return the contents of the file and it returned a not modified status code. It did not attach the section for line-based text data, since it hadn’t been modified so it didn’t need to be updated.

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 only sent one HTTP GET request for the file, and another one for the

favicon.



```
 937 4.452970000 10.0.0.6        128.119.245.12  HTTP   486 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 960 4.556665000 128.119.245.12  10.0.0.6        HTTP   587 HTTP/1.1 200 OK  (text/html)
 977 4.641999000 10.0.0.6        128.119.245.12  HTTP   432 GET /favicon.ico HTTP/1.1
 992 4.738987000 128.119.245.12  10.0.0.6        HTTP   554 HTTP/1.1 404 Not Found  (text/html)
```

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    I received the status code OK after requesting to get the file and also says 4 reassembled TCP segments

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

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

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET request sent?
    My browser sent out four GET requests not including the GET for the favicon. They were sent to 128.119.245.12, 23.39.21.76, 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?
    One of the images was moved permanently, however I believe that they would be downloading in parallel since it's just grabbing the bytes from each picture.

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
    The server's response was 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?
    There are a few new fields which are added such as last-modified, ETag, and accept ranges