Quinn Roemer

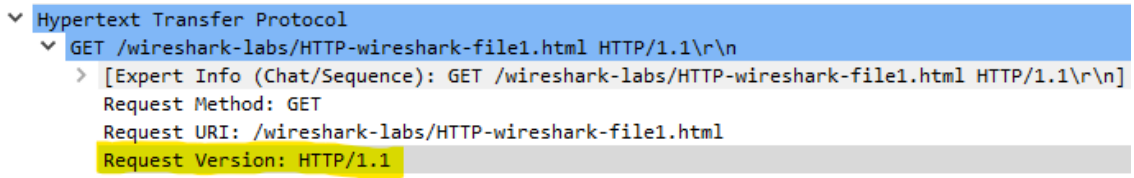
Professor Xuyu Wang

CSC 138

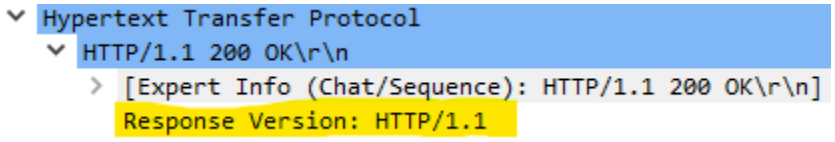
October 6, 2020

Part 1:

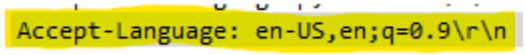
1. Is your browser running HTTP version 1.0 or 1.1? What version of the HTTP is the server running?
    - My browser is running **HTTP version 1.1.**



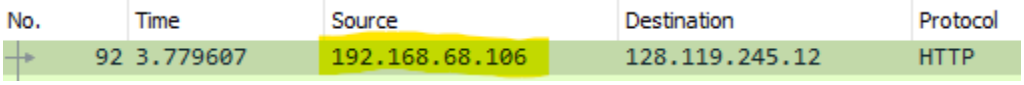
    - The server is running **HTTP version 1.1.**



2. What languages (if any) does your browser indicate that it can accept from the server?
    - My browser indicates that it can accept **English (en-US, en).**

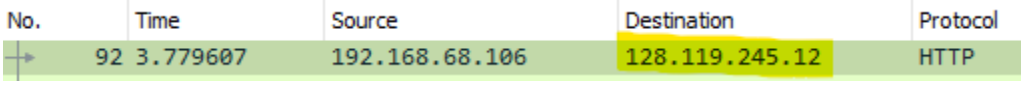


3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
    - The IP of my computer is: **192.168.68.106.**



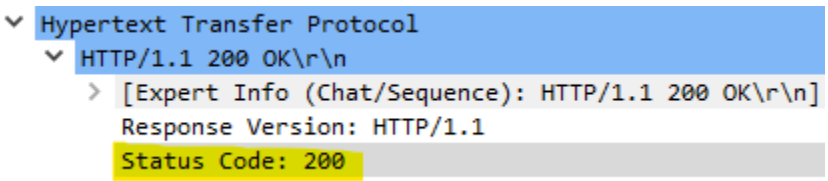
No.	Time	Source	Destination	Protocol
92	3.779607	192.168.68.106	128.119.245.12	HTTP

    - The IP of gaia.cs.umass.edu is: **128.119.245.12**

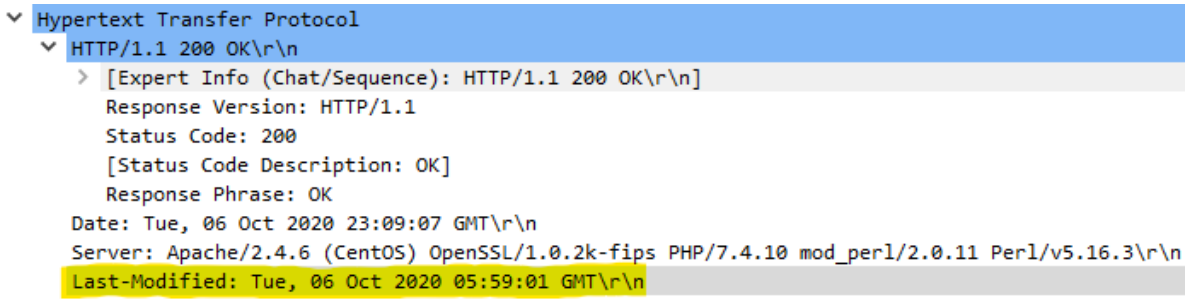


No.	Time	Source	Destination	Protocol
92	3.779607	192.168.68.106	128.119.245.12	HTTP

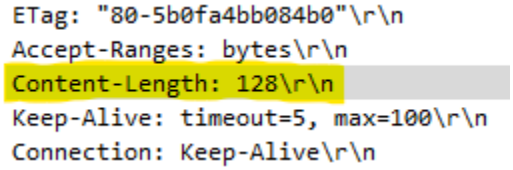
4. What was the status code returned from the server to your browser?
    - The status code returned was **200.**



5. When was the HTML file that you are retrieving last modified at the server?
    - The file was last modified: **Tue, 06 Oct 2020 05:59:01 GMT.**



6. How many bytes of content are being returned to your browser?
    - The server returned **128 bytes.**

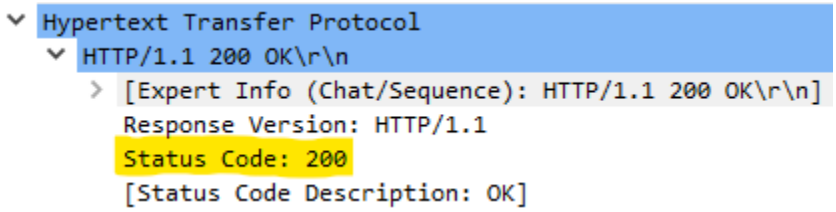


7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
    - No, I do not see any headers that appear in packet content window that do not appear in the packet-list.

Part 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?
    - The first file does not contain an **"IF-MODIFIED-SINCE"** line since this file is not cached.

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
    - Yes, the server responded with a status code 200, meaning the response contains the contents of the file.



- This can be verified by examining the response packet, which holds the contents of the HTML file.

```
Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you seen an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?
    - Yes, the line exists, the information that follows is **Tue, 06 Oct 2020 05:59:01 GMT.**

```
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5b0fa4bb07cdf"\r\n
If-Modified-Since: Tue, 06 Oct 2020 05:59:01 GMT\r\n
\r\n
```

11. What is the HTTP status code and phrase returned from the server in response to the second HTTP GET? Did the server explicitly return the contents of the file? Explain?
    - The status code returned is **304**, which means the file has **not been modified**. As a result, the packet contains no information about the contents of the file.

```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
  Date: Tue, 06 Oct 2020 23:48:13 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=99\r\n
  ETag: "173-5b0fa4bb07cdf"\r\n
```

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 of Rights?
    - My browser sent a **single GET request** to the server and the packet number in the trace was **42**

No.	Time	Source	Destination	Protocol	Length	Info
42	1.133963	192.168.68.106	128.119.245.12	HTTP	543	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    - Packet number **57** contains the status code and phrase associated with the HTTP GET request.

```
▾ [4 Reassembled TCP Segments (4861 bytes): #57(1460), #58(1460), #59(1460)
    [Frame: 57, payload: 0-1459 (1460 bytes)]
    [Frame: 58, payload: 1460-2919 (1460 bytes)]
    [Frame: 59, payload: 2920-4379 (1460 bytes)]
    [Frame: 60, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    › [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 57  65 64 2c 20 30 37 20 4f   ·Date: W ed, 07 O
0020  63 74 20 32 30 32 30 20  30 30 3a 30 34 3a 35 33   ct 2020  00:04:53
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  31 30 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   10 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   ·Last-Mo dified:
00a0  54 75 65 2c 20 30 36 20  4f 63 74 20 32 30 32 30   Tue, 06  Oct 2020
00b0  20 30 35 3a 35 39 3a 30  31 20 47 4d 54 0d 0a 45    05:59:0 1 GMT··E
```

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

```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    › [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      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?
    - A total of **four segments** were necessary.

```
[4 Reassembled TCP Segments (4861 bytes): #57(1460), #58(1460), #59(1460), #60(481)]
    [Frame: 57, payload: 0-1459 (1460 bytes)]
    [Frame: 58, payload: 1460-2919 (1460 bytes)]
    [Frame: 59, payload: 2920-4379 (1460 bytes)]
    [Frame: 60, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057…]
```

Part 4:

16. How many HTTP GET request messages did your browser send? To which internet addresses were these GET requests sent?
    - My browser sent a total of three HTTP GET requests to the same address, **128.119.245.12.**

No.	Time	Source	Destination	Protocol	Length	Info
46	3.185368	192.168.68.106	128.119.245.12	HTTP	543	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
55	3.315382	128.119.245.12	192.168.68.106	HTTP	1127	HTTP/1.1 200 OK (text/html)
59	3.351473	192.168.68.106	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
73	3.462567	128.119.245.12	192.168.68.106	HTTP	745	HTTP/1.1 200 OK (PNG)
86	3.619000	192.168.68.106	128.119.245.12	HTTP	489	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
755	4.014893	128.119.245.12	192.168.68.106	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

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.
    - They are downloaded **serially** as the request for the second image does not begin until after the first image is received. This can be seen in the image below:

No.	Time	Source	Destination	Protocol	Length	Info
46	3.185368	192.168.68.106	128.119.245.12	HTTP	543	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
55	3.315382	128.119.245.12	192.168.68.106	HTTP	1127	HTTP/1.1 200 OK (text/html)
59	3.351473	192.168.68.106	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
73	3.462567	128.119.245.12	192.168.68.106	HTTP	745	HTTP/1.1 200 OK (PNG)
86	3.619000	192.168.68.106	128.119.245.12	HTTP	489	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
755	4.014893	128.119.245.12	192.168.68.106	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

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 status code is **401** with the phrase **Unauthorized**.

```
Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
        Response Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Unauthorized
```

19. When the browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
    - The GET message now holds the **authorization field** which contains the username and password that was entered.