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

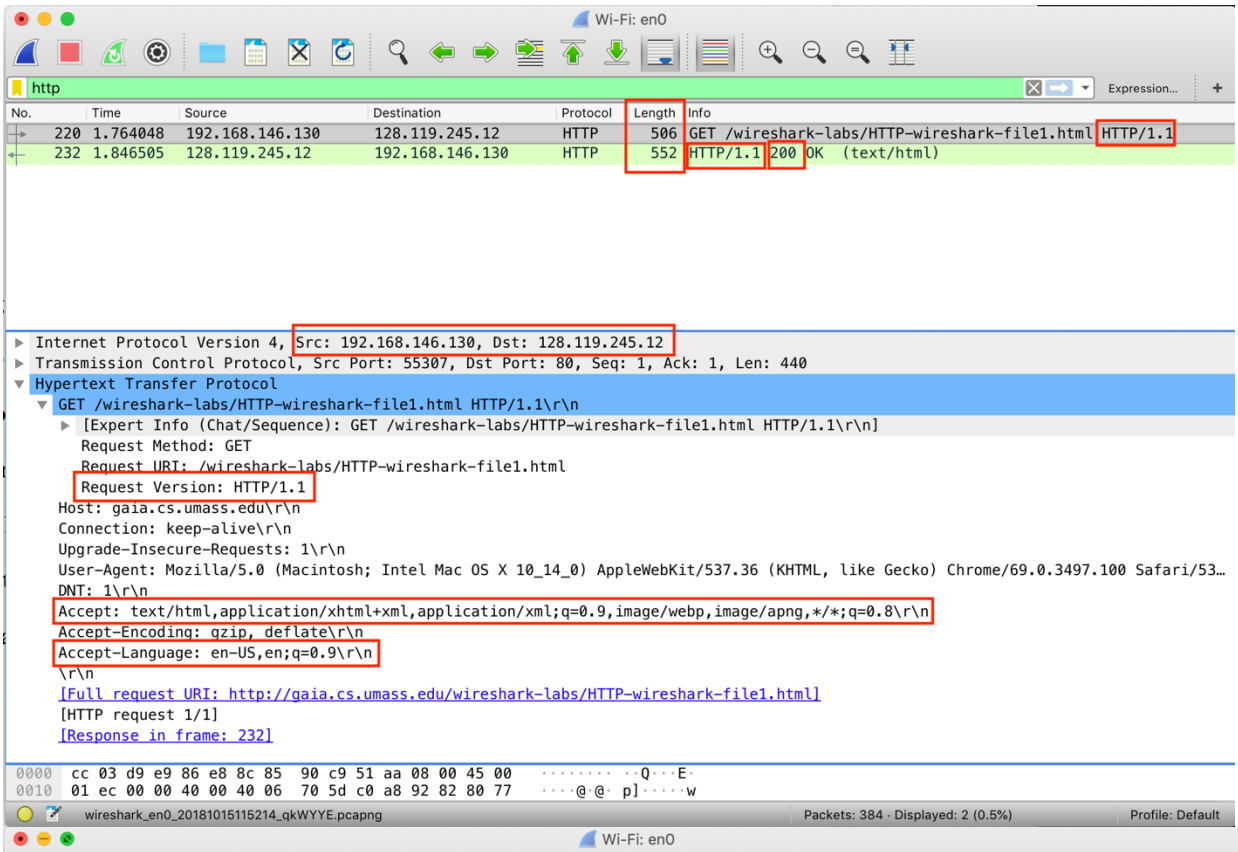
4. What is the status code returned from the server to your browser?
200

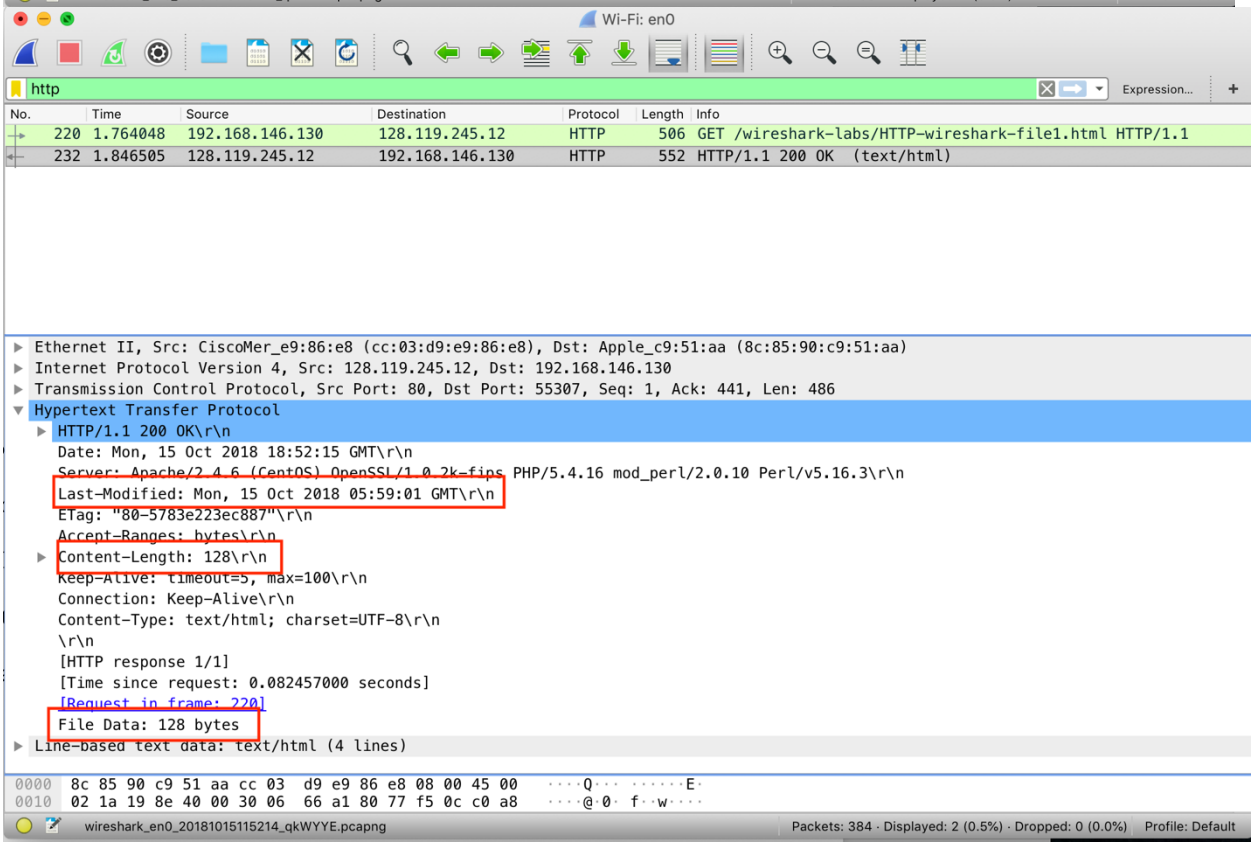
5. When was the HTML file that you are retrieving last modified at the server?
Monday, October 15, 2018 05:59:01 GMT

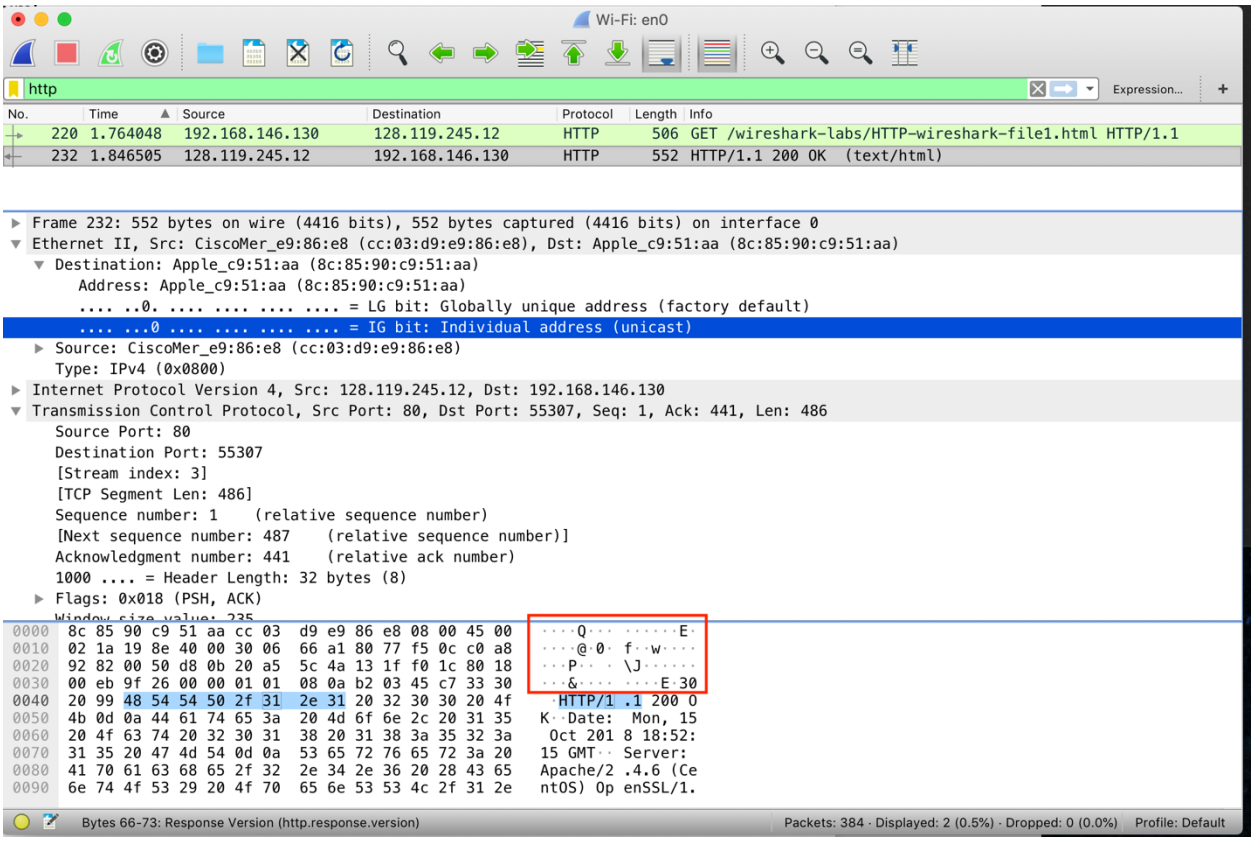
6. How many bytes of content are being returned to your browser?
552 bytes are returned in the 200 status code request.
For content, it shows that file data is **128 bytes.**

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)


Wi-Fi: en0
http
Expression...
No. Time Source Destination Protocol Length Info
220 1.764048 192.168.146.130 128.119.245.12 HTTP 506 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
232 1.846505 128.119.245.12 192.168.146.130 HTTP 552 HTTP/1.1 200 OK (text/html)
Internet Protocol Version 4, Src: 192.168.146.130, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55307, Dst Port: 80, Seq: 1, Ack: 1, Len: 440
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/53…
DNT: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 232]
0000 cc 03 d9 e9 86 e8 8c 85 90 c9 51 aa 08 00 45 00
0010 01 ec 00 00 40 00 40 06 70 5d c0 a8 92 82 80 77
wireshark_en0_20181015115214_qkWYYE.pcapng
Packets: 384 · Displayed: 2 (0.5%)
Profile: Default


Wi-Fi: en0
http
Expression...
No. Time Source Destination Protocol Length Info
220 1.764048 192.168.146.130 128.119.245.12 HTTP 506 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
232 1.846505 128.119.245.12 192.168.146.130 HTTP 552 HTTP/1.1 200 OK (text/html)
Ethernet II, Src: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8), Dst: Apple_c9:51:aa (8c:85:90:c9:51:aa)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.146.130
Transmission Control Protocol, Src Port: 80, Dst Port: 55307, Seq: 1, Ack: 441, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 15 Oct 2018 18:52:15 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Mon, 15 Oct 2018 05:59:01 GMT\r\n
ETag: "80-5783e223ec887"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.082457000 seconds]
[Request in frame: 220]
File Data: 128 bytes
Line-based text data: text/html (4 lines)
0000 8c 85 90 c9 51 aa cc 03 d9 e9 86 e8 08 00 45 00
0010 02 1a 19 8e 40 00 30 06 66 a1 80 77 f5 0c c0 a8
wireshark_en0_20181015115214_qkWYYE.pcapng
Packets: 384 · Displayed: 2 (0.5%) · Dropped: 0 (0.0%)
Profile: Default



Section 2

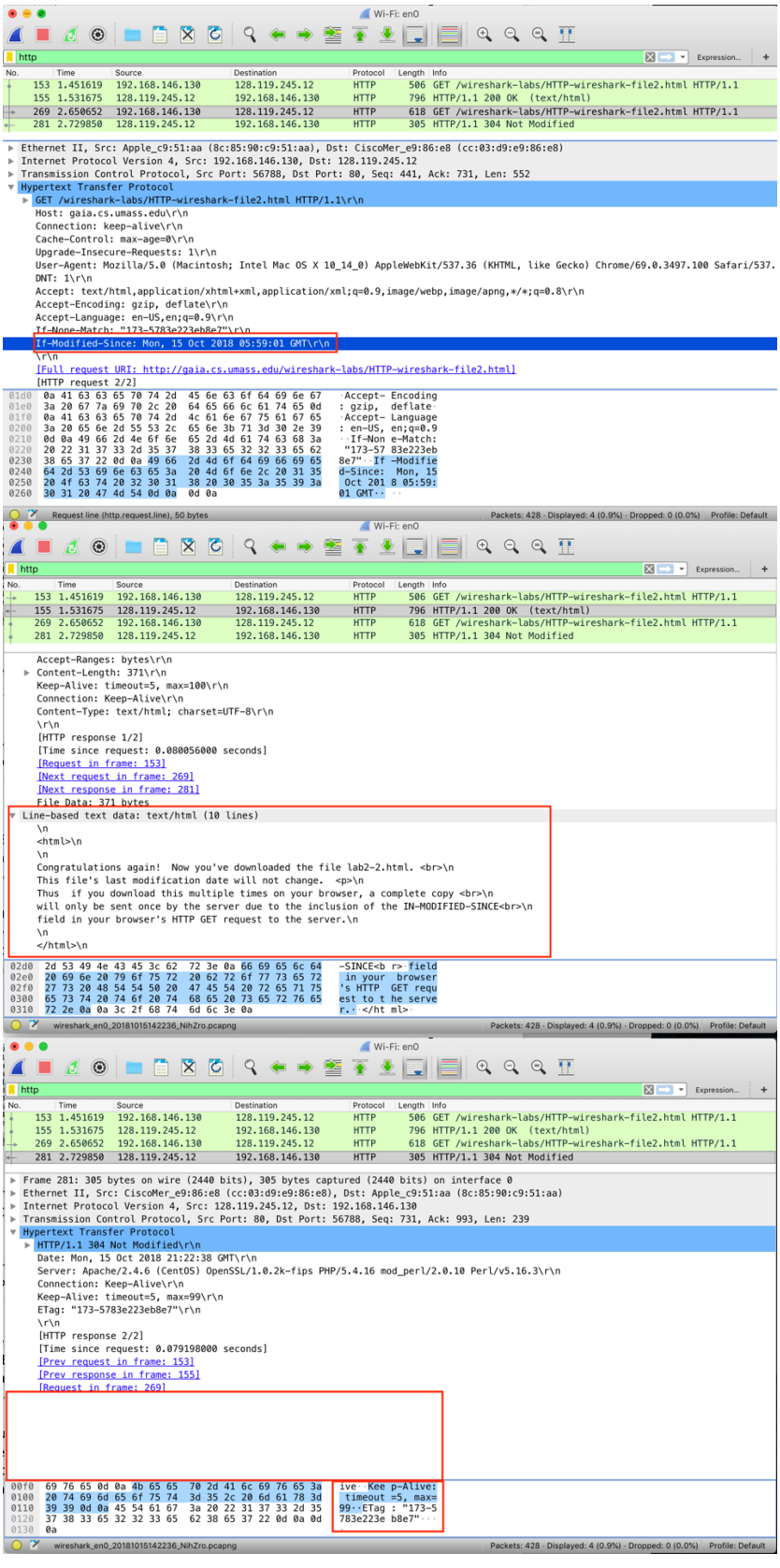
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
No, not in the first HTTP GET request.

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)


Wi-Fi: en0
http
No. Time Source Destination Protocol Length Info
153 1.451619 192.168.146.130 128.119.245.12 HTTP 506 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
155 1.531675 128.119.245.12 192.168.146.130 HTTP 796 HTTP/1.1 200 OK (text/html)
269 2.650652 192.168.146.130 128.119.245.12 HTTP 618 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
281 2.729850 128.119.245.12 192.168.146.130 HTTP 305 HTTP/1.1 304 Not Modified
Ethernet II, Src: Apple_c9:51:aa (8c:85:90:c9:51:aa), Dst: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
Internet Protocol Version 4, Src: 192.168.146.130, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56788, Dst Port: 80, Seq: 441, Ack: 731, Len: 552
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.
DNT: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5783e223eb8e7"\r\n
If-Modified-Since: Mon, 15 Oct 2018 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]
Request line (http.request.line), 50 bytes
Packets: 428 · Displayed: 4 (0.9%) · Dropped: 0 (0.0%) Profile: Default
Wi-Fi: en0
http
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.080056000 seconds]
[Request in frame: 153]
[Next request in frame: 269]
[Next response in frame: 281]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html.
\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
\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
wireshark_en0_20181015142236_NihZro.pcapng
Packets: 428 · Displayed: 4 (0.9%) · Dropped: 0 (0.0%) Profile: Default
Wi-Fi: en0
http
Frame 281: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0
Ethernet II, Src: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8), Dst: Apple_c9:51:aa (8c:85:90:c9:51:aa)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.146.130
Transmission Control Protocol, Src Port: 80, Dst Port: 56788, Seq: 731, Ack: 993, Len: 239
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Date: Mon, 15 Oct 2018 21:22:38 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-5783e223eb8e7"\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.079198000 seconds]
[Prev request in frame: 153]
[Prev response in frame: 155]
[Request in frame: 269]
wireshark_en0_20181015142236_NihZro.pcapng
Packets: 428 · Displayed: 4 (0.9%) · Dropped: 0 (0.0%) Profile: Default

Section 3

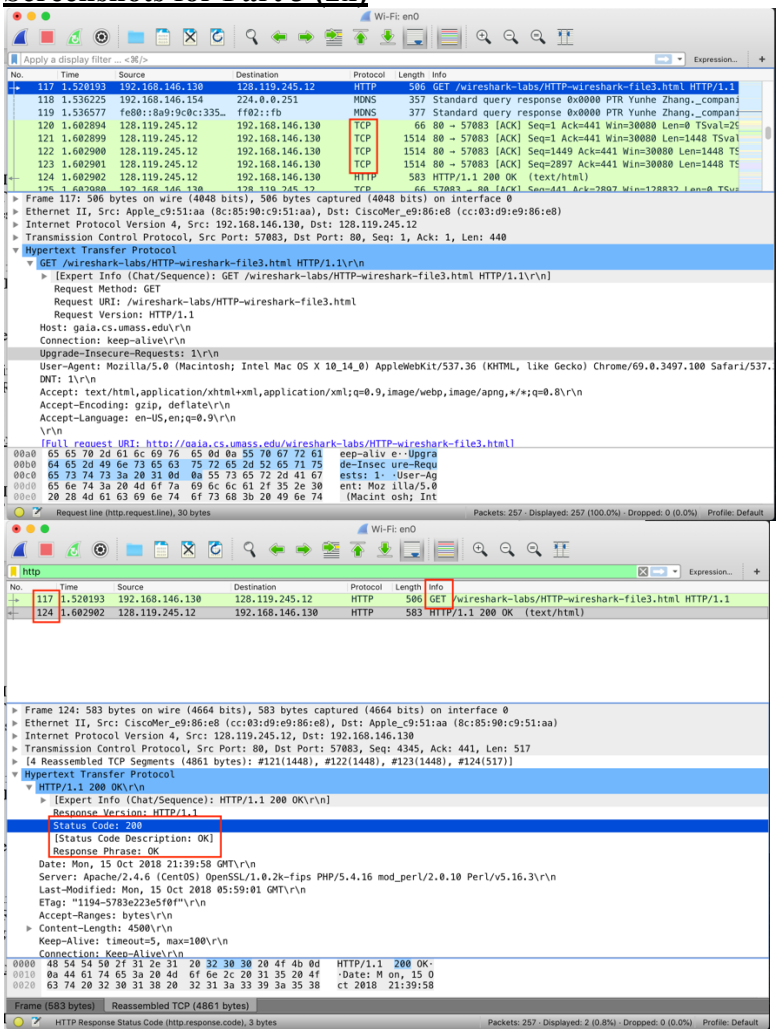
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
1x HTTP GET request messages
Packet Number 117

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)

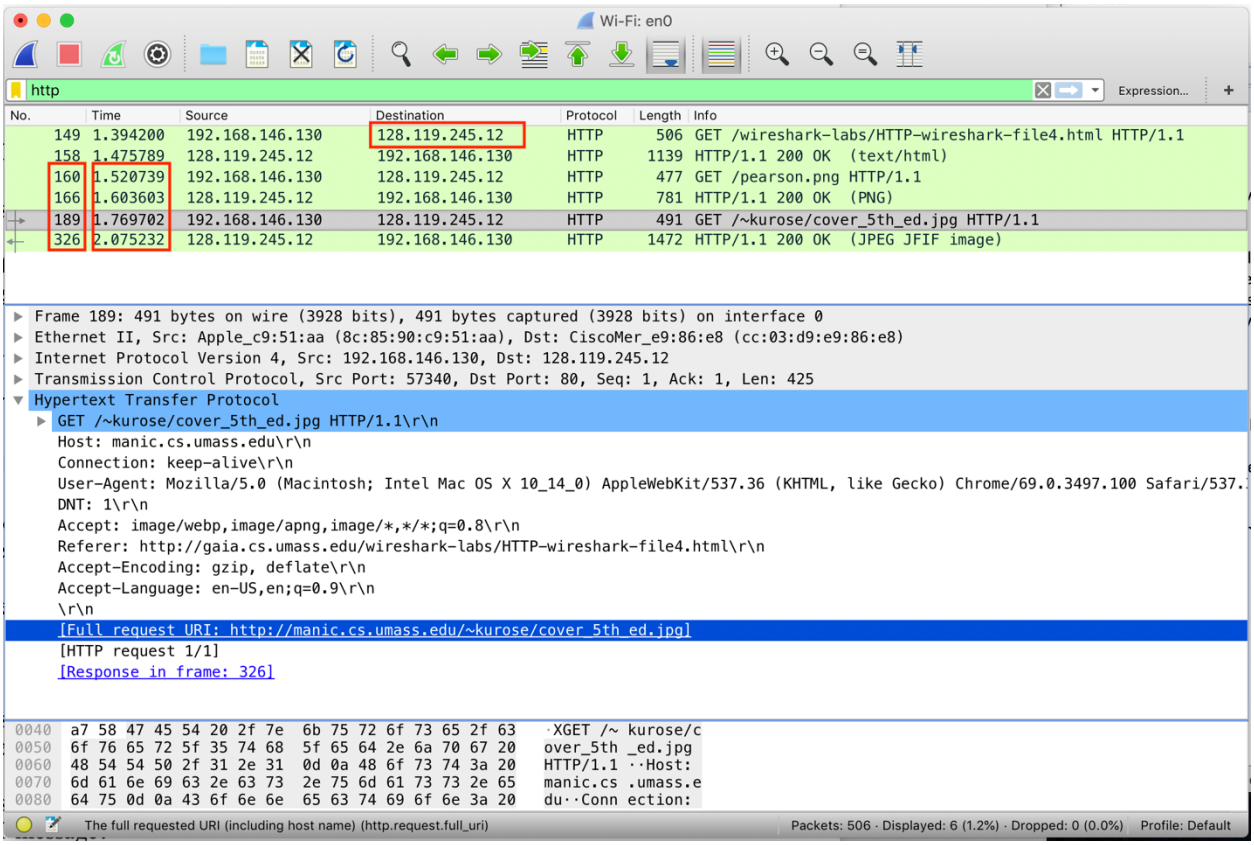
b) All 3 were going to the IP Address: 128.119.245.12

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)