ECE361 – Computer Networks

Wireshark Lab 1: HTTP

First Name: Shayshu Last Name: Nahata-Ragubance

First Name: Johnathan Last Name: Yan

Group Details:
Student #: 1005035196 Student #: 1004745476

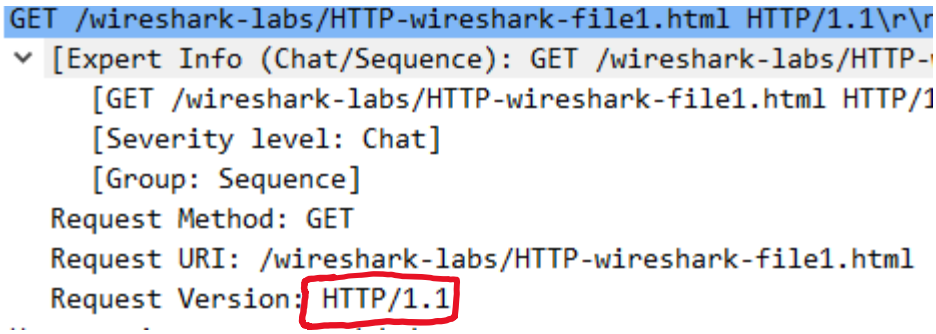
Mark:

	Question	Answer
1	Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?	Both my browser and the server are running HTTP version 1.1 See Figure 1
2	What languages (if any) does your browser indicate that it can accept to the server?	en-CA,en;q=0.9,fr-CA;q=0.8,fr;q=0.7,en-GB;q=0.6,en-US;q=0.5 So Canadian, US, and UK English and Canadian and normal French. See Figure 2
3	What is the IP address of your computer? Of the gaia.cs.umass.edu server?	My IP address is 10.0.0.230 and the server IP is 128.119.245.12 See Figure 3
4	What is the status code returned from the server to your browser?	Status code 200, meaning OK See figure 4
5	When was the HTML file that you are retrieving last modified at the server?	Sun, Jan 31, 2021 6:59:01 GMT See figure 5
6	How many bytes of content are being returned to your browser?	128 Bytes. See figure 6

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.	For example, the Connection field which is specified to be kept alive, is not shown in the packet-listing. See figure 7
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. Which is somewhat expected because the cache was cleared before doing this part. See figure 8
9	Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?	Yes, we can clearly read the entire HTML contents in the Line based text data field. It returned 10 lines of text/html (371 bytes). See figure 9
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, it contains the date it was last modified which tells the server that if the file they have has not been modified since "Sun, 31 Jan 2021" then we can use the file we have in memory. See figure 10.
11	What is the HTTP status code and phrase returned from the server in response to this second HTTP	The server returns status code 304 which means that the file has not been modified. Furthermore, the server does not send back any text/html data because we can use the data stored locally in memory instead.

	GET? Did the server explicitly return the contents of the file? Explain.	See figure 11
12	How many HTTP GET request messages were sent by your browser?	Only 1 HTTP get request was sent out. See figure 12
13	How many data-containing TCP segments were needed to carry the single HTTP response?	4 segments were needed to return the request. See figure 13.
14	What is the status code and phrase associated with the response to the HTTP GET request?	Status code 200, meaning OK. See figure 14.
15	Are there any HTTP status lines in the transmitted data associated with a TCPinduced "Continuation"?	No, the newer versions of wireshark do not use this format anymore. They just show the entire reassembled packet. See figure 15
16	How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?	3 get requests were sent. The requests were sent to: • http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html • http://gaia.cs.umass.edu/pearson.png • http://kurose.cslash.net/8E_cover_small.jpg See figure 16
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.	You can't tell for certain because there might be slight issues in the network that make it appear to be serial. However, the order in which the images were returned matches the order in which the requests were sent making me believe it was done serially. However, in practice most downloading should be done in parallel.

		See figure 17
18 (optional)	What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?	The returned status code is 401 meaning unauthorized. See figure 18
19 (optional)	When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?	It adds an authorization field with the username and password, converted to base 64. See figure 19



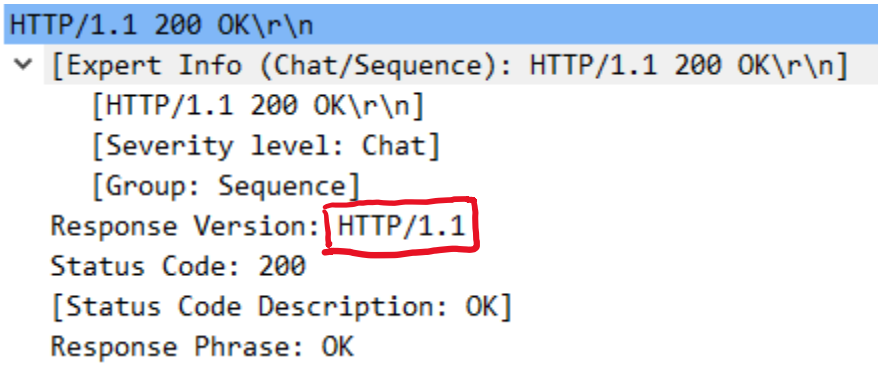


Figure 1: Question 1 HTTP version

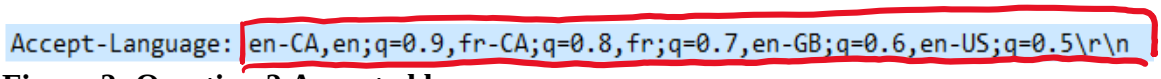


Figure 2: Question 2 Accepted language

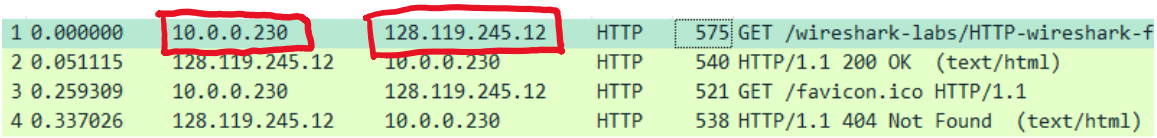


Figure 3: Question 3 IP addresses

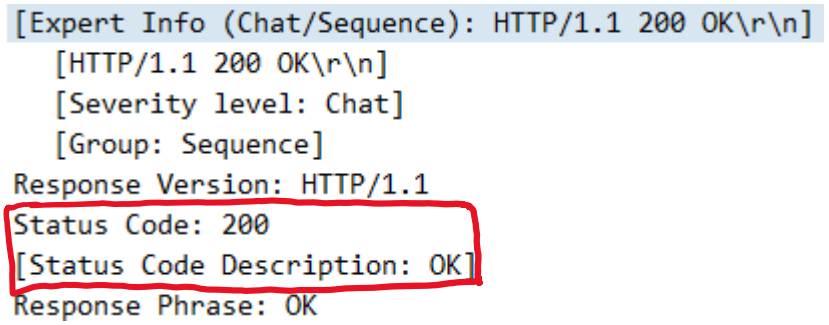


Figure 4: Question 4 Sever response code

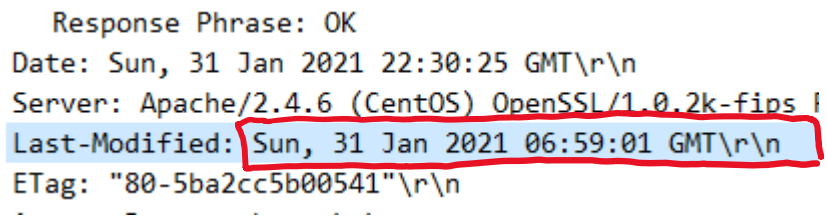


Figure 5: Question 5 Last modified

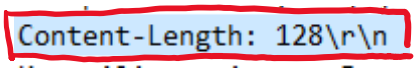


Figure 6: Question 6 size of file returned

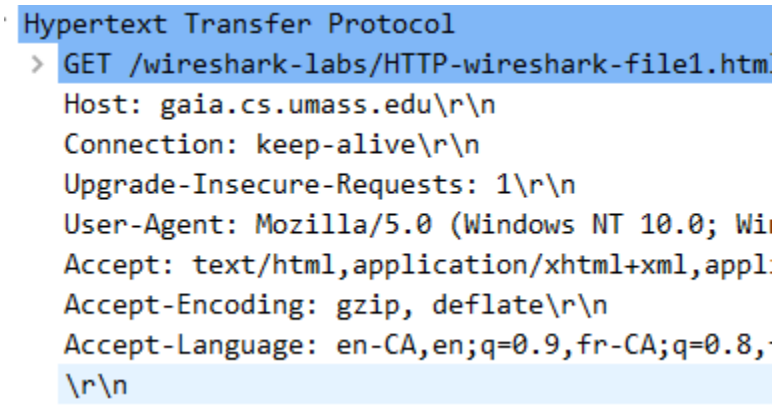


Figure 7: Question 7 connection keep alive

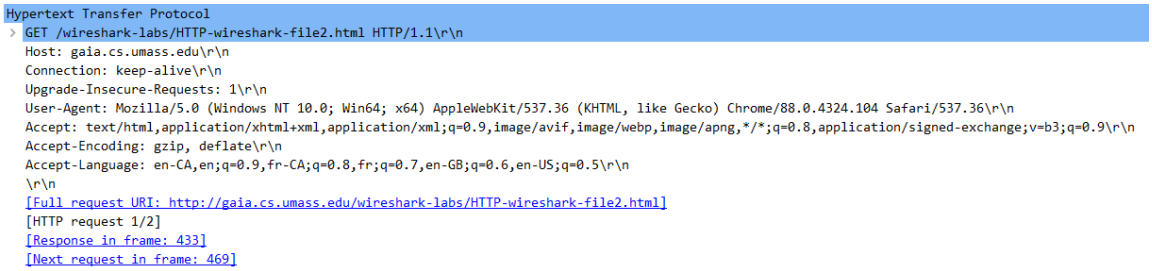


Figure 8: Question 8 If modified since

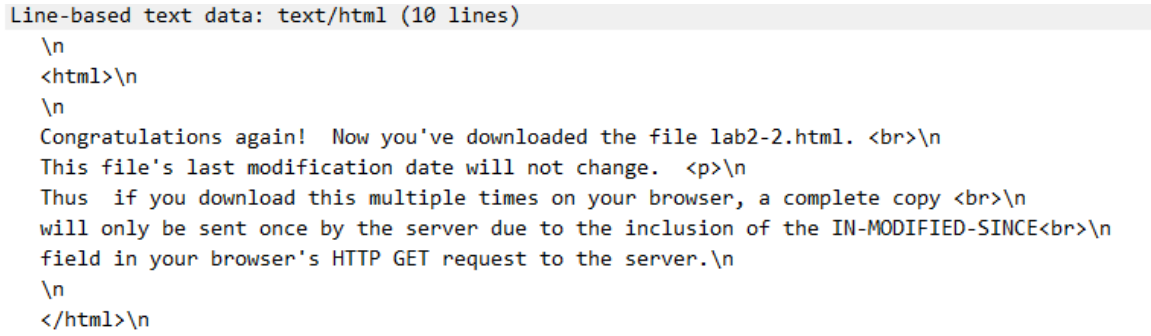


Figure 9: Question 9 File contents

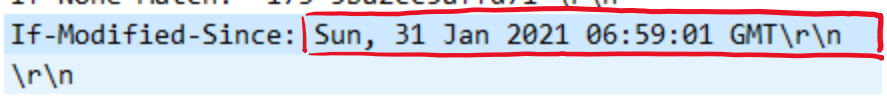


Figure 10: Question 10 second HTTP get request

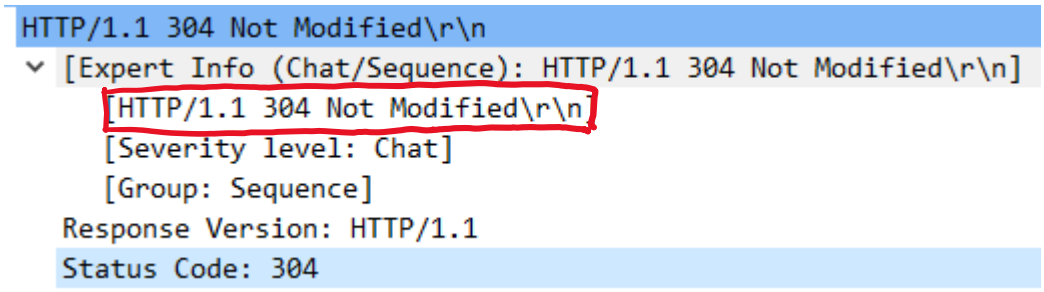


Figure 11: Question 11 server status code response

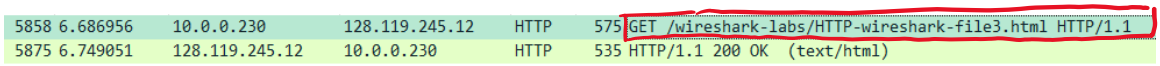


Figure 12: Question 12 Number of GET requests sent

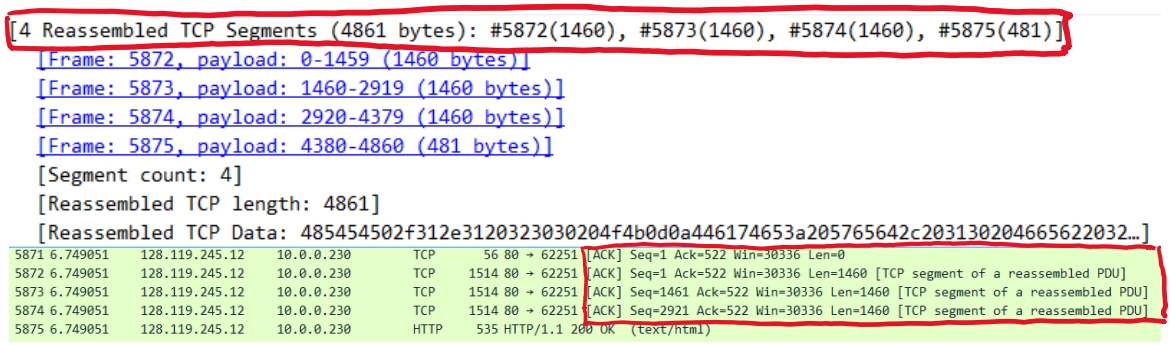


Figure 13: Question 13 Number of TCP segments

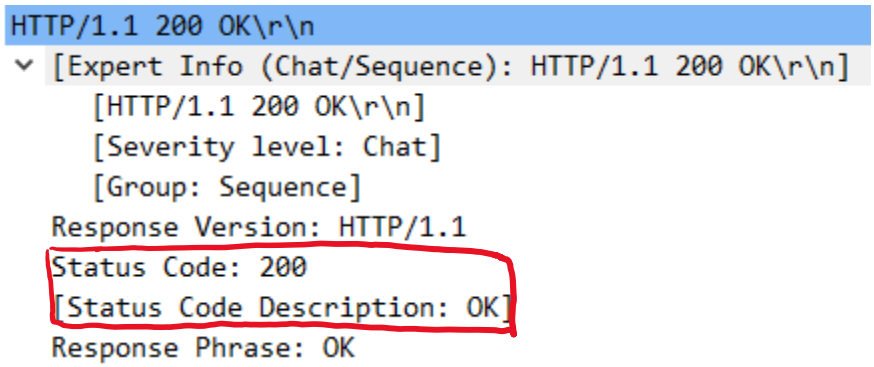


Figure 14: Question 14 Server status response to large file

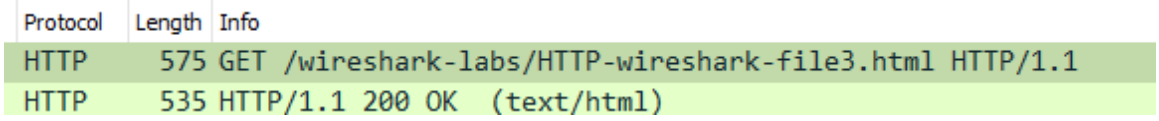


Figure 15: Question 15 HTTP Continuation

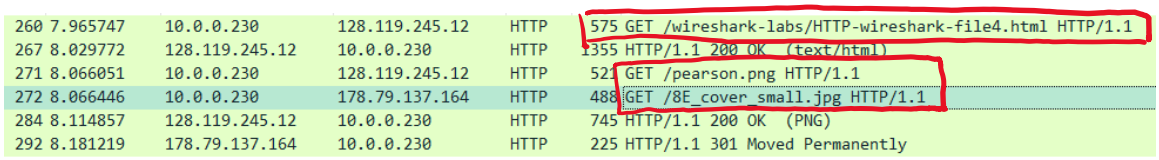
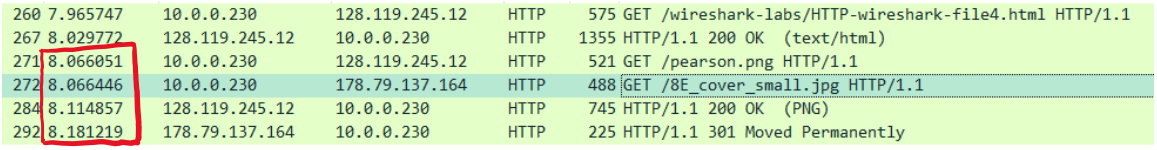


Figure 16: Question 16 Get requests sent



260	7.965747	10.0.0.230	128.119.245.12	HTTP	575	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
267	8.029772	128.119.245.12	10.0.0.230	HTTP	1355	HTTP/1.1 200 OK (text/html)
271	8.066051	10.0.0.230	128.119.245.12	HTTP	521	GET /pearson.png HTTP/1.1
272	8.066446	10.0.0.230	178.79.137.164	HTTP	488	GET /8E_cover_small.jpg HTTP/1.1
284	8.114857	128.119.245.12	10.0.0.230	HTTP	745	HTTP/1.1 200 OK (PNG)
292	8.181219	178.79.137.164	10.0.0.230	HTTP	225	HTTP/1.1 301 Moved Permanently

Figure 17: Question 17 parallel or serial

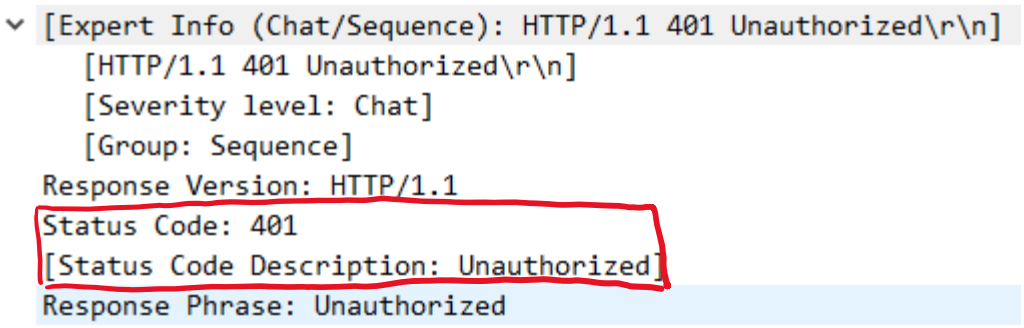


Figure 18: Question 18 unauthorized GET request

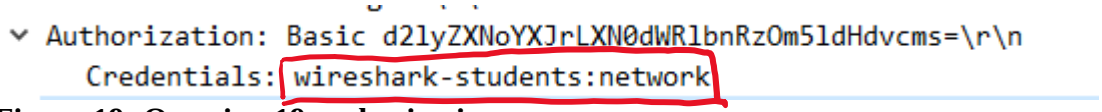


Figure 19: Question 19 authorization