ECE361 – Computer Networks

Wireshark Lab 1: HTTP

First Name: Zaheer Last Name: Hashmi

First Name: Hairan Last Name: Zheng

Group Details:

1004299056 **1004957601**

Student #: _____ Student #: _____

Mark:

	Question	Answer
1	Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?	See Fig 1
2	What languages (if any) does your browser indicate that it can accept to the server?	See Fig 2
3	What is the IP address of your computer? Of the gaia.cs.umass.edu server?	See Fig 2
4	What is the status code returned from the server to your browser?	See Fig 2
5	When was the HTML file that you are retrieving last modified at the server?	See Fig 3
6	How many bytes of content are being returned to your browser?	See Fig 4
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.	All the headers can be found
8	Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-	See Fig 5

	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?	See Fig 6
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?	See Fig 7
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.	See Fig8
12	How many HTTP GET request messages were sent by your browser?	See Fig9
13	How many data-containing TCP segments were needed to carry the single HTTP response?	See Fig10
14	What is the status code and phrase associated with the response to the HTTP GET request?	See Fig10
15	Are there any HTTP status lines in the transmitted data associated with a TCPinduced "Continuation"?	No
16	How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?	See Fig11

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.	See Fig 11
18 (optional)	What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?	
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?	

Annotated Traces

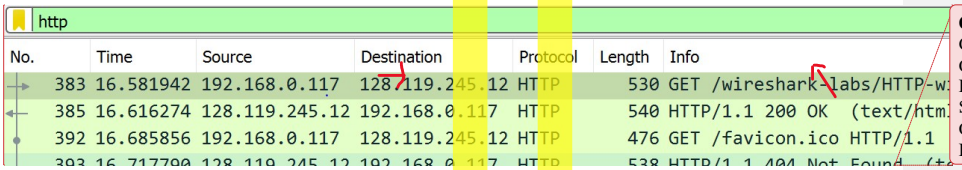


Figure 1

Commented [ZH1]: Q1:
Client HTTP version
Observe the Info field of packet No.383; We notice that the HTTP/1.1 is used by our browser to make the request.
Server HTTP version
Observe the Info filed of packet No385; We notice that HTTP/1.1 is used by the server to send the response.

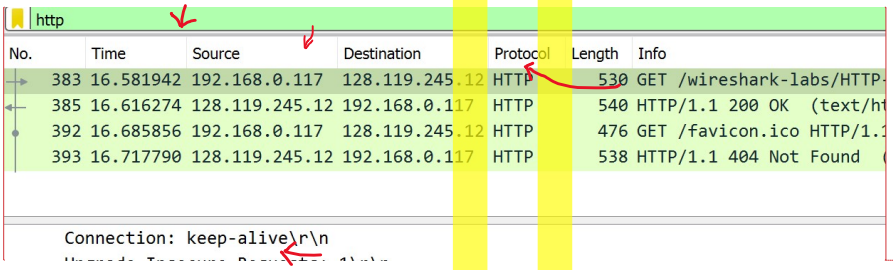


Figure 2

Commented [ZH2]: Q2:
The information for what languages are accepted by our client browser are indicated in the HTTP request. We observe by examining the wireshark HTTP layer associated with packet No.383 that our browser accepts en=US and en for languages.

Q3:
We observe that packet No.383 is that request message as evident by the Request Line under the Info column. Here we also observe our IP address under the source column: 192.168.0.117 and the server IP address under the Destination column 128.119.245.12
Q4:
Status code is found the response message sent by the server. Here we observe that packet 385 consists of the request message as indicated in its Info column. The status code here is : 200 OK

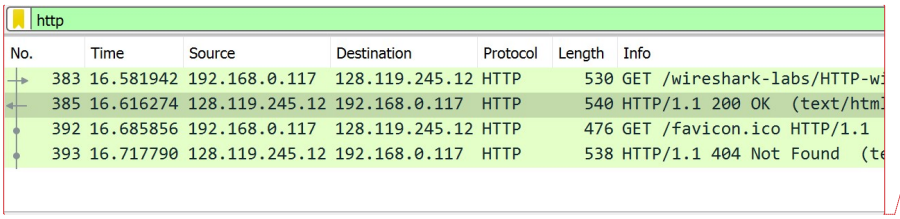


Figure 3

Commented [ZH3]: Q5:
We observe here under the HTTP layer of packet 385 that the file sent was last modified on Tue, 09 Feb 2021 06:59:01

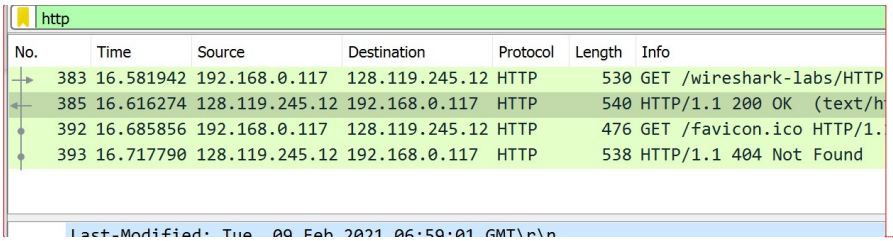


Figure 4

Commented [ZH4]: Q6:
We observe at packet No.385; request message that the size of the file received is 128bytes

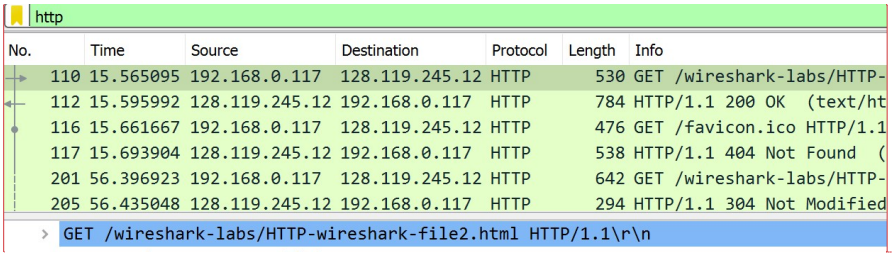


Figure 5

Commented [ZH5]: Q8:
We observe here that the first GET request message is represented by packet No.110. We observe the IF MODIFIED SINCE: line is absent in this particular request message

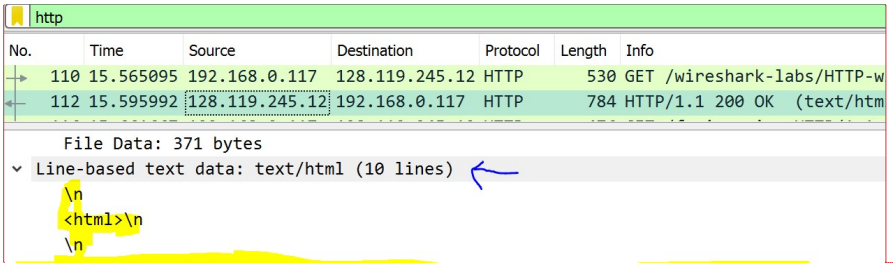


Figure 6

Commented [ZH6]: Q9:
We observe packet No. 112 here. We note that in request message the HTML file request is included

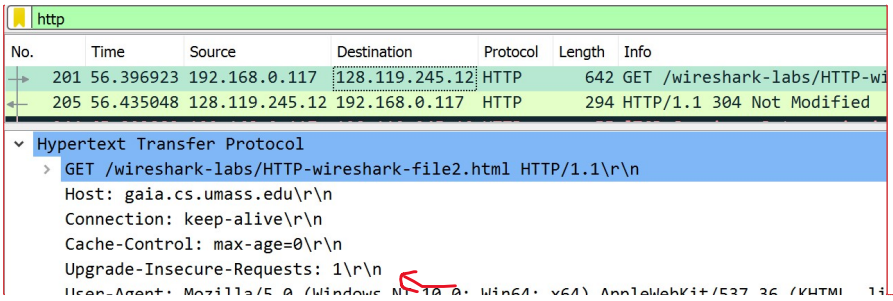


Figure 7

Commented [ZH7]: Q10:
Here we observe that the second request message (packed No. 201) does contain the IF MODIFIED SINCE: line. The date followed by this is the date server returned in the first response message.

Commented [ZH8R7]:

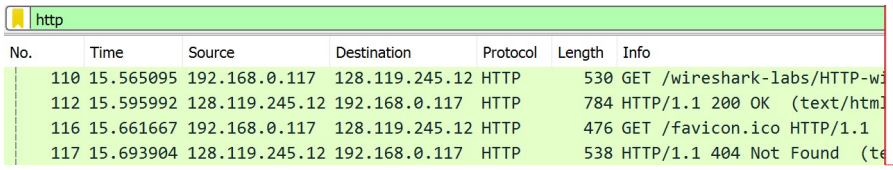


Figure 8

Commented [ZH9]: Q11:
Observing packet 205. We note in the Info column that the response message includes status code 304 with message Not Modified. Also the body does not include any files which is consistent with what we expect. We only want to retrieve file again if it had been modified since date identified in the associated request message

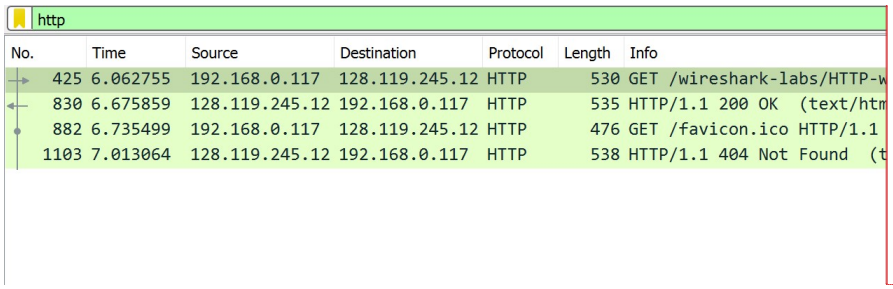


Figure 9

Commented [ZH10]: Q12:
Observing packet No.425 we notice that two HTTP request messages were sent.

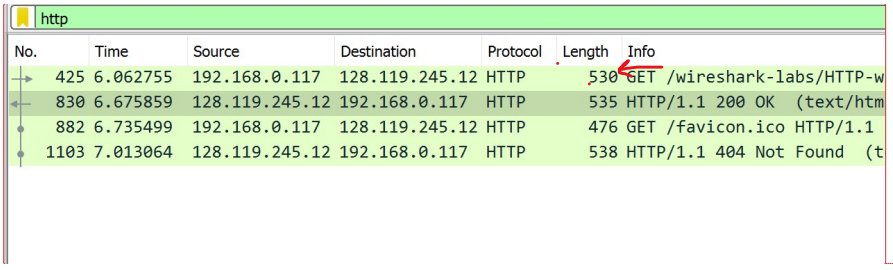
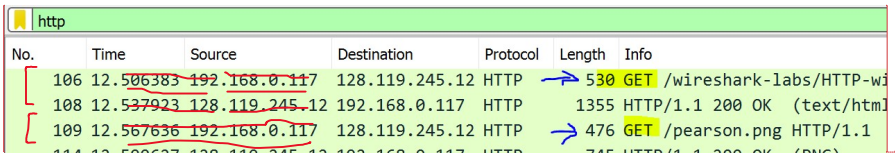


Figure 10

Commented [ZH11]: Q13:
We observe packet No. 830's TCP layer. We note that 4 TCP segments were required

Q14:
Observe Packet No.830. We note in the Info column that the stats is 200 OK.



Commented [ZH12]: Q16:
We observe packet No's: 106, 109 and 124 and look at the info column -> 3 requests are sent

Q17: We note that the requests were sent serially indicated by the different destination addresses

Figure 11