

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

No.	Time	Source	Destination	Protocol	Length	Info
383	16.581942	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-labs/ HTTP/1.1
385	16.616274	128.119.245.12	192.168.0.117	HTTP	540	HTTP/1.1 200 OK (text/html)
392	16.685856	192.168.0.117	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
393	16.717790	128.119.245.12	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found

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 field of packet No.385; We notice that HTTP/1.1 is used by the server to send the response.

No.	Time	Source	Destination	Protocol	Length	Info
383	16.581942	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-labs/ HTTP/1.1
385	16.616274	128.119.245.12	192.168.0.117	HTTP	540	HTTP/1.1 200 OK (text/html)
392	16.685856	192.168.0.117	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
393	16.717790	128.119.245.12	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found

Connection: keep-alive\r\n

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

No.	Time	Source	Destination	Protocol	Length	Info
383	16.581942	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-w
385	16.616274	128.119.245.12	192.168.0.117	HTTP	540	HTTP/1.1 200 OK (text/htm
392	16.685856	192.168.0.117	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
393	16.717790	128.119.245.12	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found (te

Figure 3

No.	Time	Source	Destination	Protocol	Length	Info
383	16.581942	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP
385	16.616274	128.119.245.12	192.168.0.117	HTTP	540	HTTP/1.1 200 OK (text/h
392	16.685856	192.168.0.117	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.
393	16.717790	128.119.245.12	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found

Last-Modified: Tue, 09 Feb 2021 06:59:01 GMT\r\n

Figure 4

No.	Time	Source	Destination	Protocol	Length	Info
110	15.565095	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-
112	15.595992	128.119.245.12	192.168.0.117	HTTP	784	HTTP/1.1 200 OK (text/ht
116	15.661667	192.168.0.117	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
117	15.693904	128.119.245.12	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found (
201	56.396923	192.168.0.117	128.119.245.12	HTTP	642	GET /wireshark-labs/HTTP-
205	56.435048	128.119.245.12	192.168.0.117	HTTP	294	HTTP/1.1 304 Not Modified

> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

Figure 5

No.	Time	Source	Destination	Protocol	Length	Info
110	15.565095	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-w
112	15.595992	128.119.245.12	192.168.0.117	HTTP	784	HTTP/1.1 200 OK (text/htm

File Data: 371 bytes

Line-based text data: text/html (10 lines)

```

\r\n
<html>\r\n
\r\n

```

Figure 6

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

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

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

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

No.	Time	Source	Destination	Protocol	Length	Info
201	56.396923	192.168.0.117	128.119.245.12	HTTP	642	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
205	56.435048	128.119.245.12	192.168.0.117	HTTP	294	HTTP/1.1 304 Not Modified

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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3183.87 Safari/537.36

Figure 7

No.	Time	Source	Destination	Protocol	Length	Info
110	15.565095	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
112	15.595992	128.119.245.12	192.168.0.117	HTTP	784	HTTP/1.1 200 OK (text/html)
116	15.661667	192.168.0.117	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
117	15.693904	128.119.245.12	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figure 8

No.	Time	Source	Destination	Protocol	Length	Info
425	6.062755	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
830	6.675859	128.119.245.12	192.168.0.117	HTTP	535	HTTP/1.1 200 OK (text/html)
882	6.735499	192.168.0.117	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
1103	7.013064	128.119.245.12	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figure 9

No.	Time	Source	Destination	Protocol	Length	Info
425	6.062755	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
830	6.675859	128.119.245.12	192.168.0.117	HTTP	535	HTTP/1.1 200 OK (text/html)
882	6.735499	192.168.0.117	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
1103	7.013064	128.119.245.12	192.168.0.117	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figure 10

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]:

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

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

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 status is 200 OK.

http						
No.	Time	Source	Destination	Protocol	Length	Info
106	12.506383	192.168.0.117	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wi
108	12.537923	128.119.245.12	192.168.0.117	HTTP	1355	HTTP/1.1 200 OK (text/htm
109	12.567636	192.168.0.117	128.119.245.12	HTTP	476	GET /pearson.png HTTP/1.1

Figure 11

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