

CS 3873: Net-Centric Computing

Lab 1: Examining HTTP with Wireshark

Student Name: Mahmoud Moustafa

Student Number: 3648276

[Mandatory] Declaration: "I warrant that this is my own work."

Signed by Mahmoud Moustafa

[Optional] "I hereby give my permission for this work to be used (with my name and identifying information removed) for UNB Faculty of Computer Science program accreditation purposes."

Signed by _____

Report for Lab Exercise 1: Examining HTTP with Wireshark

LAB ACTIVITIES:

In this lab, we learnt how to capture packet traces with Wireshark. In particular, we used Wireshark to examine the details of the hypertext transfer protocol (HTTP).

ANSWERS TO LAB QUESTIONS:

The following gives you one example on how to draft your answer to the lab questions.

4. Based on the above trace, answer the following questions:

- a. Select the first HTTP message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer to the HTTP server. When you select the HTTP GET message, the Ethernet or Ethernet II frame, IPv4 datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. How long did it take from when the HTTP GET message was sent until the first HTTP response was received?

Answer: As seen in Fig. 1, the HTTP get message is captured 18.220895 seconds after starting Wireshark, while the first HTTP response is received at 18.260484 seconds after starting Wireshark. It took $(18.260484 - 18.220895 = 0.039589)$ seconds.

No.	Time	Source	Destination	Protocol	Length	Info
148	18.220895	192.168.2.20	128.119.245.12	HTTP	373	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
151	18.260484	128.119.245.12	192.168.2.20	HTTP	492	HTTP/1.1 200 OK (text/html)

Fig. 1. Certain HTTP GET and Response messages in the captured trace.

- b. In the trace you will find IPv4 addresses within the packets. Find an example packet in the trace where the IPv4 address associated with your machine is present. Compare this address with the IPv4 address you can find by using the following command: *ipconfig* on Windows, or *ifconfig* on MacOS or Linux. Running this command also gives a 48-bit physical address for the network interface. This is the MAC (medium access control) address (not discussed in class yet) of your machine. Can you find the MAC address of the packet in the trace? Is it the same as the physical address returned by the above command?

Answer: Yes, I can find the MAC address of the packet in the trace it is 192.168.2.20. Yes, it is the same as the physical address returned by the command above. This is shown in Fig. 2.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.140201	192.168.2.20	157.240.241.18	TCP	54	51596 → 443 [ACK] Seq=30 Ack=26 Win=512 Len=0

IPv4 Address. : 192.168.2.20

Fig.2. The IPv4 addresses

6. Examine your new trace captured in item 5 and answer the following questions:

- a) Inspect the contents of the first HTTP GET request **for the Webpage “lab1.html”** from your browser to the server³. Do you see an “If-Modified-Since” line in the HTTP GET?

Answer: No, I do not see an “If-Modified-Since” line. As shown in the Fig. 3.

1215	17.612893	192.168.2.20	131.202.244.5	HTTP	497 GET /~wsong/lab1.html HTTP/1.1
1226	17.622122	131.202.244.5	192.168.2.20	HTTP	925 HTTP/1.1 200 OK (text/html)
1243	17.692602	192.168.2.20	131.202.244.5	HTTP	435 GET /favicon.ico HTTP/1.1
1245	17.700924	131.202.244.5	192.168.2.20	HTTP	749 HTTP/1.1 200 OK (PNG)
1833	30.184219	192.168.2.20	131.202.244.5	HTTP	609 GET /~wsong/lab1.html HTTP/1.1
1837	30.188199	131.202.244.5	192.168.2.20	HTTP	281 HTTP/1.1 304 Not Modified

```
> Ethernet II, Src: IntelCor_81:ac:13 (84:5c:f3:81:ac:13), Dst: Actionte_f1:57:f0 (4c:8b:30:f1:57:f0)
> Internet Protocol Version 4, Src: 192.168.2.20, Dst: 131.202.244.5
> Transmission Control Protocol, Src Port: 53831, Dst Port: 80, Seq: 1, Ack: 1, Len: 443
< Hypertext Transfer Protocol
  < GET /~wsong/lab1.html HTTP/1.1\r\n
    Host: cs.unb.ca\r\n
    Connection: keep-alive\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/97.0.4692.99 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://cs.unb.ca/~wsong/lab1.html]
    [HTTP request 1/2]
    [Response in frame: 1226]
    [Next request in frame: 1243]
```

Fig.3. The details of the selected packet (GET ... lab1.html)

- b) Inspect the contents of the server response to the first HTTP GET request. Did the server explicitly return the contents of the file? How can you tell?

Answer: Yes, it returned the content of the file explicitly. I can tell because it is in the “Line_based text data” as shown in Fig.4.

1215	17.612893	192.168.2.20	131.202.244.5	HTTP	497 GET /~wsong/lab1.html HTTP/1.1
1226	17.622122	131.202.244.5	192.168.2.20	HTTP	925 HTTP/1.1 200 OK (text/html)
1243	17.692602	192.168.2.20	131.202.244.5	HTTP	435 GET /favicon.ico HTTP/1.1
1245	17.700924	131.202.244.5	192.168.2.20	HTTP	749 HTTP/1.1 200 OK (PNG)
1833	30.184219	192.168.2.20	131.202.244.5	HTTP	609 GET /~wsong/lab1.html HTTP/1.1
1837	30.188199	131.202.244.5	192.168.2.20	HTTP	281 HTTP/1.1 304 Not Modified

```
< Line-based text data: text/html (16 lines)
<html lang='en'>\n
<head>\n
<title>Test Webpage for Lab 1 of CS 3873</title>\n
</head>\n
\n
<body>\n
\n
This is a test webpage for the Wireshark lab that examines HTTP. <br>\n
\n
Please reload this webpage in the same tab of your browser. Do not use two separate tabs for loading this webpage. <p>\n
\n
From this lab, you are expected to check whether the webpage will be downloaded for <br>\n
multiple times to your browser. Find out the difference between the two HTTP GET messages <br>and the difference between the two HTTP response messages.\n
\n
</body>\n
</html>
```

Fig.4. The Line-based text data.

- c) Now inspect the contents of the next HTTP GET request **for the Webpage “lab1.html”** from your browser to the server4. Do you see an “If-Modified-Since:” line in the HTTP GET? If so, what information follows the “If-Modified-Since:” header?

Answer: Yes, there is an “If-Modified-Since” line. The information that follows is “Mon, 22 Jan 2018 14:06:41 GMT \r\n\r\n” the date of the last modification of file from the previous GET request. This is shown in Fig.5.

1833	30.184219	192.168.2.20	131.202.244.5	HTTP	609 GET /~wsong/lab1.html HTTP/1.1
1837	30.188199	131.202.244.5	192.168.2.20	HTTP	281 HTTP/1.1 304 Not Modified

>	Transmission Control Protocol, Src Port: 53832, Dst Port: 80, Seq: 1, Ack: 1, Len: 555
▼	Hypertext Transfer Protocol
>	GET /~wsong/lab1.html HTTP/1.1\r\n
	Host: cs.unb.ca\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/97.0.4692.99 Safari/537.36\r\n
	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
	Accept-Encoding: gzip, deflate\r\n
	Accept-Language: en-US,en;q=0.9\r\n
	If-None-Match: "21c-5635df07f6149"\r\n
	If-Modified-Since: Mon, 22 Jan 2018 14:06:41 GMT\r\n\r\n
	[Full request URI: http://cs.unb.ca/~wsong/lab1.html]
	[HTTP request 1/1]
	[Response in frame: 1837]

Fig.5. The “If-Modified-Since” line and the information that follows

- d) What is the HTTP status code and phrase returned from the server in response to this second HTTP GET for “lab1.html”? Did the server explicitly return the contents of the file? Explain.

Answer: The status code is 304. No, it did not return the contents of the file explicitly because the file has not been modified therefore, the browser retrieved it from its cache. This is shown in Fig.6. That is why we do not see a “Line_based text data” line. If it was modified, we would be able to see the contents of the file under the “Line_based text data” line.

1837	30.188199	131.202.244.5	192.168.2.20	HTTP	281 HTTP/1.1 304 Not Modified
> Frame 1837: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits) on interface \Device\NPF_{BD67C1FD-E157-42D6-9B2B-2FB4BCE6AADA}, id 0					
> Ethernet II, Src: Actionte_f1:57:f0 (4c:8b:30:f1:57:f0), Dst: IntelCor_81:ac:13 (84:5c:f3:81:ac:13)					
> Internet Protocol Version 4, Src: 131.202.244.5, Dst: 192.168.2.20					
> Transmission Control Protocol, Src Port: 80, Dst Port: 53832, Seq: 1, Ack: 556, Len: 227					
v Hypertext Transfer Protocol					
> HTTP/1.1 304 Not Modified\r\n					
Date: Tue, 01 Feb 2022 20:52:02 GMT\r\n					
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16\r\n					
Connection: Keep-Alive\r\n					
Keep-Alive: timeout=5, max=100\r\n					
ETag: "21c-5635df07f6149"\r\n					
\r\n					
[HTTP response 1/1]					
[Time since request: 0.003980000 seconds]					
[Request in frame: 1833]					
[Request URI: http://cs.unb.ca/~wsong/lab1.html]					

Fig.6. There is no a “Line_based text data” line therefore, no explicit return of file contents.