

INTERNET PROTOCOL LAB ASSIGNMENT-3

Name: Rahul Raj

Roll Number: CYS22011

Date: 22-10-2022

Analyzing HTTP request and responses using Wireshark

AIM:

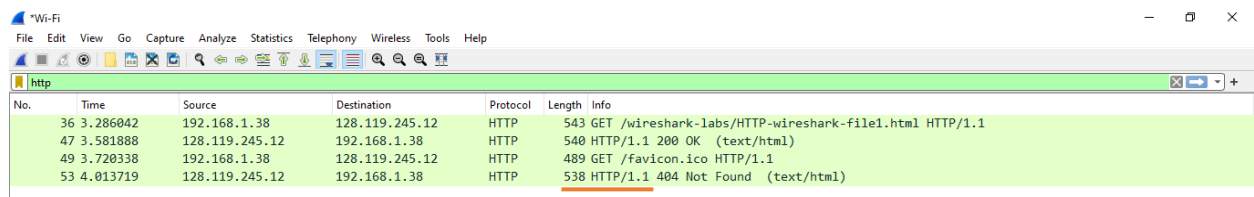
To explore the web application protocols using protocol analyzer

1)

By looking at the information in the HTTP GET and response messages, answer the following questions;

1- Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

ANS- HTTP version is 1.1



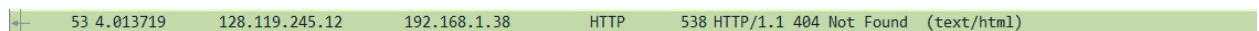
No.	Time	Source	Destination	Protocol	Length	Info
36	3.286042	192.168.1.38	128.119.245.12	HTTP	543	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
47	3.581888	128.119.245.12	192.168.1.38	HTTP	540	HTTP/1.1 200 OK (text/html)
49	3.720338	192.168.1.38	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
53	4.013719	128.119.245.12	192.168.1.38	HTTP	538	HTTP/1.1 404 Not Found (text/html)

2- What languages (if any) do your browser indicate that it can accept to the server?



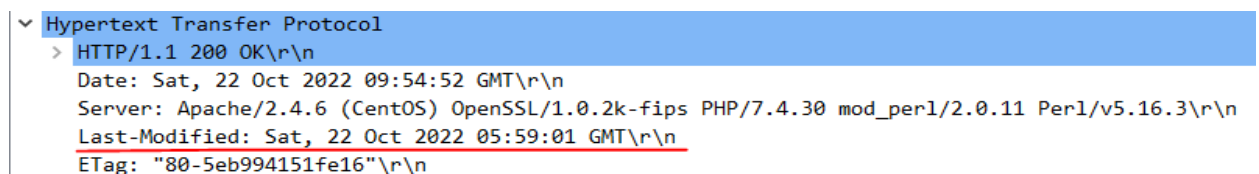
```
Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 OPR/91.0.4516.77\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
```

3- What is the status code returned from the server to your browser?



53	4.013719	128.119.245.12	192.168.1.38	HTTP	538	HTTP/1.1 404 Not Found (text/html)
----	----------	----------------	--------------	------	-----	------------------------------------

4- When was the HTML file that you are retrieving last modified at the server?



```
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Sat, 22 Oct 2022 09:54:52 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 22 Oct 2022 05:59:01 GMT\r\n
ETag: "80-5eb994151fe16"\r\n
```

5- How many bytes of content are being returned to your browser?

```
> Frame 53: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{76BEEFFB-4A0F-4E20-8886-960E1AD3EFE2}, id 0
> Ethernet II, Src: SaiNXTTe_09:03:64 (4c:ae:1c:09:03:64), Dst: LiteonTe_98:79:99 (54:8c:a0:98:79:99)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.38
> Transmission Control Protocol, Src Port: 80, Dst Port: 49306, Seq: 487, Ack: 925, Len: 484
< Hypertext Transfer Protocol
  < HTTP/1.1 404 Not Found\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
      Date: Sat, 22 Oct 2022 09:54:52 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    > Content-Length: 209\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
```

6- 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.

ANS- NO.

2) 7- 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?

ANS- NO

No.	Time	Source	Destination	Protocol	Length	Info
861	2.766578	192.168.1.38	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1066	3.057426	128.119.245.12	192.168.1.38	HTTP	784	HTTP/1.1 200 OK (text/html)
1069	3.150598	192.168.1.38	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
1196	3.439878	128.119.245.12	192.168.1.38	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1368	5.746985	192.168.1.38	128.119.245.12	HTTP	645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1370	6.042051	128.119.245.12	192.168.1.38	HTTP	293	HTTP/1.1 304 Not Modified

```
> Transmission Control Protocol, Src Port: 52889, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
< Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 Edg/106.0.1370.47\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
```

8- Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

ANS- YES, Destination address = source address should be same

<html>

Congratulations again! Now you've downloaded the file lab2-2.html.

This file's last modification date will not change. <p>

Thus if you download this multiple times on your browser, a complete copy
 will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
 field in your browser's HTTP GET request to the server.

</html>

9- 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? What information follows the “IF-MODIFIEDSINCE:” header?

ANS- Yes, it contains – “Sat, 22 oct 2022 05:59:01 GMT\r\n”

861	2.766578	192.168.1.38	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1066	3.057426	128.119.245.12	192.168.1.38	HTTP	784	HTTP/1.1 200 OK (text/html)
1069	3.150598	192.168.1.38	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
1196	3.439878	128.119.245.12	192.168.1.38	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1368	5.746985	192.168.1.38	128.119.245.12	HTTP	645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1370	6.042051	128.119.245.12	192.168.1.38	HTTP	293	HTTP/1.1 304 Not Modified


```

> Ethernet II, Src: LiteonTe_98:79:99 (54:8c:a0:98:79:99), Dst: SaiNXTe_09:03:64 (4c:ae:1c:09:03:64)
> Internet Protocol Version 4, Src: 192.168.1.38, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52889, Dst Port: 80, Seq: 905, Ack: 1215, Len: 591
> 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/106.0.0.0 Safari/537.36 Edg/106.0.1370.47\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: "173-5eb994151f25e"\r\n
    If-Modified-Since: Sat, 22 Oct 2022 05:59:01 GMT\r\n
  \r\n

```

10- 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 file’s contents? Explain.

Length	Info
533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
784	HTTP/1.1 200 OK (text/html)
479	GET /favicon.ico HTTP/1.1
538	HTTP/1.1 404 Not Found (text/html)
645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
293	HTTP/1.1 304 Not Modified

3)

11- 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?

ANS- One HTTP GET request, first packet in the trace contains the GET message.

No.	Time	Source	Destination	Protocol	Length	Info
21	0.292442	192.168.1.38	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
46	0.590391	128.119.245.12	192.168.1.38	HTTP	565	HTTP/1.1 200 OK (text/html)

12- Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

46	0.590391	128.119.245.12	192.168.1.38	HTTP	565	HTTP/1.1 200 OK (text/html)
----	----------	----------------	--------------	------	-----	-----------------------------

13- What is the status code and phrase in the response?

ANS- Status code – 200, phrase – Ok

46	0.590391	128.119.245.12	192.168.1.38	HTTP	565	HTTP/1.1 200 OK (text/html)
----	----------	----------------	--------------	------	-----	-----------------------------

14- How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

ANS- We have 3 TCP segments.

42	0.580720	128.119.245.12	192.168.1.38	TCP	1504	80 → 58126 [ACK] Seq=1 Ack=480 Win=30720 Len=1450 [TCP segment of a reassembled PDU]
43	0.580720	128.119.245.12	192.168.1.38	TCP	1504	80 → 58126 [ACK] Seq=1451 Ack=480 Win=30720 Len=1450 [TCP segment of a reassembled PDU]
44	0.580833	192.168.1.38	128.119.245.12	TCP	54	58126 → 80 [ACK] Seq=480 Ack=2901 Win=131840 Len=0
45	0.581079	128.119.245.12	192.168.1.38	TCP	1504	80 → 58126 [PSH, ACK] Seq=2901 Ack=480 Win=30720 Len=1450 [TCP segment of a reassembled PDU]
46	0.590391	128.119.245.12	192.168.1.38	HTTP	565	HTTP/1.1 200 OK (text/html)

4)

15- What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

ANS- Status code 401, phrase - Unauthorized

No.	Time	Source	Destination	Protocol	Length	Info
14	6.717291	192.168.1.38	128.119.245.12	HTTP	541	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
20	7.004465	128.119.245.12	192.168.1.38	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

16- When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

ANS- For first get request we won't have any authorization header

```
GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

But whereas for second get we have Authorization

```
GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic V2lyZXNoYXJrLXN0dWRlbnQ6bmV0d29yaw==
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

RESULT

Thus, explored the web application protocols using protocol analyzer successfully.

