

# 21CY681 - INTERNET PROTOCOL LAB - III

Name: Surya S Nair

Register Number: CB.EN.P2CYS22007

Date: 20th October 2022

Assignment Topic: To use wireshark and analyse various HTTP packets and protocols

1. Is your browser running HTTP version 1.0 or 1.1?

```
299 2022/293 15:25:10.833469 192.168.170.120 128.119.245.12 HTTP 479 GET /favicon.ico HTTP/1.1
```

What version of HTTP is the server running?

```
331 2022/293 15:25:11.140864 128.119.245.12 192.168.170.120 HTTP 539 HTTP/1.1 404 Not Found (text/html)
```

Ans : Browser is running on HTTP version 1.1 and the server has version 1.1.

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

Ans : en-US

```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
.
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Ans : My IP address is 192.168.170.120 and the server is 128.119.245.12

```
192.168.170.120
128.119.245.12
```

4. What is the status code returned from the server to your browser?

Ans : Status code: 404 Not Found

```
331 2022/293 15:25:11.140864 128.119.245.12 192.168.170.120 HTTP 539 HTTP/1.1 404 Not Found (text/html)
```

5. When was the HTML file that you are retrieving last modified at the server?

Ans :

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod\_perl/2.0.11 Perl/v5.16.3  
Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT

6. How many bytes of content are being returned to your browser?

Ans :

Accept-Ranges: bytes  
Content-Length: 128

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.

Ans : No

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?

Ans : No

sub2\_http.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Time	No.	Source	Destination	Protocol	Length	Info
2022/293 15:59:...	35	192.168.170.120	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2022/293 15:59:...	39	128.119.245.12	192.168.170.120	HTTP	784	HTTP/1.1 200 OK (text/html)
2022/293 15:59:...	942	192.168.170.120	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2022/293 15:59:...	1256	192.168.170.120	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2022/293 15:59:...	1546	128.119.245.12	192.168.170.120	HTTP	294	HTTP/1.1 304 Not Modified
2022/293 15:59:...	2114	128.119.245.12	192.168.170.120	HTTP	784	HTTP/1.1 200 OK (text/html)
2022/293 15:59:...	3015	192.168.170.120	128.119.245.12	HTTP	645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2022/293 15:59:...	3033	128.119.245.12	192.168.170.120	HTTP	293	HTTP/1.1 304 Not Modified

Internet Protocol Version 4, Src: 192.168.170.120, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 56782, Dst Port: 80, Seq: 351111111, Win: 65535, Len: 0

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4660.53 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n

0000 5e 9d 6a af 47 1a 28 39 26 63 33 5b 08 00 45 00 ^-j-G-(9  
0010 02 00 a7 f1 40 00 80 06 70 61 c0 a8 aa 78 80 77 ....@..  
0020 f5 0c dd ce 00 50 63 84 c0 ac 44 aa ed 6e 50 18 ....Pc..  
0030 01 02 ff 72 00 00 47 45 54 20 2f 77 69 72 65 73 ....r..GE  
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab  
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 iredshark  
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP  
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia  
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu..C  
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep-  
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I

Hypertext Transfer Protocol: Protocol

Packets: 3046 - Displayed: 8 (0.3%)

Profile: Default

```

> Internet Protocol Version 4, Src: 192.168.170.120, Dst: 128.119.
> Transmission Control Protocol, Src Port: 56782, Dst Port: 80, Se
v 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n

```

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

Ans :

```
<html>
```

```

Congratulations again! Now you've downloaded the file lab2-2.html. <br>
This file's last modification date will not change. <p>
Thus if you download this multiple times on your browser, a complete copy <br>
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
field in your browser's HTTP GET request to the server.

```

```
</html>
```

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? What information follows the “IF-MODIFIED SINCE:” header?

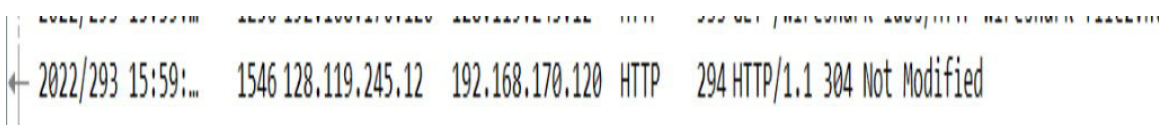
Ans : Yes

```

Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5eb71059bd74a"\r\n
If-Modified-Since: Thu, 20 Oct 2022 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTT
[HTTP request 1/1]
[Response in frame: 1546]

```

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 file's contents? Explain.

Ans :  2022/293 15:59:1... 1546 128.119.245.12 192.168.170.120 HTTP 294 HTTP/1.1 304 Not Modified

No the server didn't explicitly return the file's contents.

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?

Ans :

```

533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
835 HTTP/1.1 200 OK (text/html)
479 GET /favicon.ico HTTP/1.1

```

1 st Packet

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

Ans :

```

1100 2022/293 10:46:22.281367 192.168.121.59 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1259 2022/293 10:46:25.363281 128.119.245.12 192.168.121.59 HTTP 835 HTTP/1.1 200 OK (text/html)

```

1 st Packet

14. What is the status code and phrase in the response?

Ans :Status Code: 200

Phrase: Ok

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

Ans :

```
1255 2022/293 10:46:25.360249 128.119.245.12 192.168.121.59 TCP 1414 80 → 52678 [ACK] Seq=1 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
1256 2022/293 10:46:25.360294 128.119.245.12 192.168.121.59 TCP 1414 80 → 52678 [ACK] Seq=1361 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
1257 2022/293 10:46:25.360463 192.168.121.59 128.119.245.12 TCP 54 52678 → 80 [ACK] Seq=480 Ack=2721 Win=66560 Len=0
1258 2022/293 10:46:25.362219 128.119.245.12 192.168.121.59 TCP 1414 80 → 52678 [ACK] Seq=2721 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
```

3 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

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

Ans :

```
37 2022/293 11:19:22.763598 128.119.245.12 192.168.170.120 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)
```

Status code: 401

Phrase: Unauthorized

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

Ans :

```
Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm8=
```

The new field is included in the HTTP GET message is Authorization.