

CS315: Assignment-2

Name: Shahil Patel

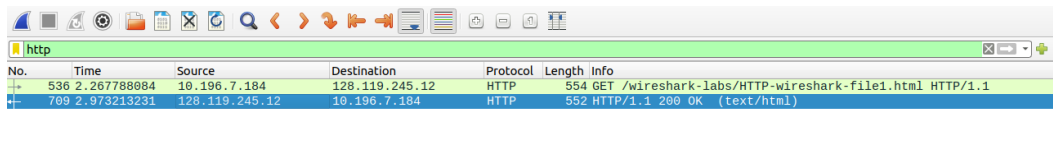
Roll No.: 200010039

Part-1: The Basic HTTP GET/response interaction

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

Ans: Browser is running HTTP version: **1.1**, Server is running HTTP version: **1.1**

Screenshot:



No.	Time	Source	Destination	Protocol	Length	Info
536	2.267788084	10.196.7.184	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
709	2.973213231	128.119.245.12	10.196.7.184	HTTP	552	HTTP/1.1 200 OK (text/html)

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

Ans: **en-US,en;q=0.5**

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

Ans: IP address of my computer is: **10.196.7.184**

IP address of *gaia.cs.umass.edu* server: **128.119.245.12**

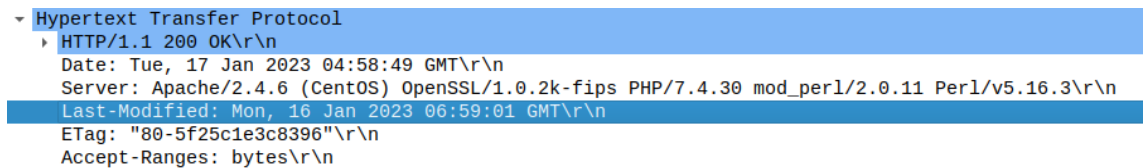
4. What is the status code returned from the server to your browser?

Ans: Status code returned from the server to your browser: **200 OK**

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

Ans: Last Modified: **Mon, 16 Jan 2023 06:59:01 GMT\r\n**

Screenshot:



```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Tue, 17 Jan 2023 04:58:49 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: Mon, 16 Jan 2023 06:59:01 GMT\r\n
    ETag: "80-5f25c1e3c8396"\r\n
    Accept-Ranges: bytes\r\n

```

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

Ans: **128 bytes** of content is being returned to my browser.

Screenshot:

```
[HTTP response 1/1]
[Time since request: 0.705425147 seconds]
[Request in frame: 536]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
▼ Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
```

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, we don't see any headers within data that are not displayed in the packet-listing window but displayed in packet content window.

Part-2 The HTTP CONDITIONAL GET/response interaction

1. 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, I don't see an "IF-MODIFIED-SINCE" line in the HTTP GET on inspecting the contents of the first HTTP GET request from my browser to the server.

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

Ans: Yes the server explicitly returns the contents of the files. We can verify from the line which shows the amount of file data transferred in bytes which are **371 bytes**

Screenshot:

```
File Data: 371 bytes
▼ Line-based text data: text/html (10 lines)
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

3. 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?

Ans: Yes we see an "IF-MODIFIED-SINCE" line in the HTTP GET. The information gives the date of the last modification which in our case is: **MON, 16 Jan 2023 06:59:01 GMT\r\n**.

4. 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.

Ans: status code and phrase returned from the server: **304 Not Modified**.

The server did not explicitly return the content of the file, because we have already fetched the file from the server previously and the *file data is already stored in the browser's cache*.

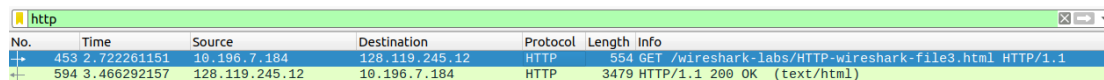
Part-3 Retrieving Long Documents

1. 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: Browser sent **1** HTTP GET request message

The packet number in the trace that contains the GET Message for the *Bill of rights* is: **453**

Screenshot:



No.	Time	Source	Destination	Protocol	Length	Info
453	2.722261151	10.196.7.184	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
594	3.466292157	128.119.245.12	10.196.7.184	HTTP	3479	HTTP/1.1 200 OK (text/html)

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

Ans: The packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request is: **594**

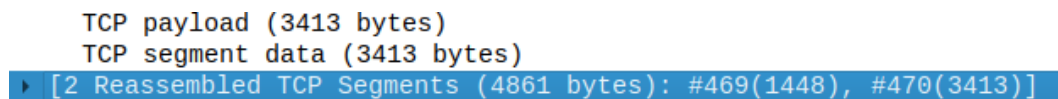
3. What is the status code and phrase in the response?

Ans: status code and phrase is: **200 OK**.

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

Ans: **2** data-containing TCP segments were needed to carry the single HTTP response and to the text of The Bill of Rights.

Screenshot:



TCP payload (3413 bytes)
TCP segment data (3413 bytes)
[2 Reassembled TCP Segments (4861 bytes): #469(1448), #470(3413)]

Part-4 HTML Documents with Embedded Objects

1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Ans: **3** HTTP GET requests were sent by my browser.

The addresses to which the GET requests were sent are:

- a. **128.119.245.12**
- b. **128.119.245.12**
- c. **178.79.137.164**

2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Ans: The images are loaded in **serial** fashion as the timestamps are sequential. At a time only one request is sent for the HTTP GET.

Part-5: HTTP Authentication

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

Ans: For the initial HTTP GET message from my browser the server's response is: **401 Unauthorized**.

Screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
334	3.115470366	10.196.7.184	128.119.245.12	HTTP	570	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html ...
392	3.999301958	128.119.245.12	10.196.7.184	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
996	14.973164009	10.196.7.184	35.232.111.17	HTTP	153	GET / HTTP/1.1
1114	15.695725102	35.232.111.17	10.196.7.184	HTTP	214	HTTP/1.1 204 No Content
2790	45.587624524	10.196.7.184	128.119.245.12	HTTP	629	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html ...
2803	47.004455230	128.119.245.12	10.196.7.184	HTTP	556	HTTP/1.1 200 OK (text/html)

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

Ans: The new field included in the 2nd HTTP GET message is:

Field: **Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n**
Credentials: wireshark-students:network

Screenshot:

Cache-Control: max-age=0 ...
▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Credentials: wireshark-students:network