Computer Networks Lab, Assignment 3

Suyash Gaurav

210010054

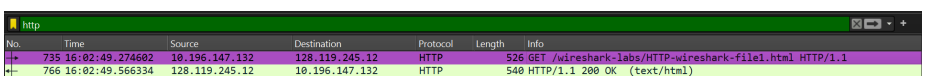
---

1 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?

HTTP Version: 1.1



http

No.	Time	Source	Destination	Protocol	Length	Info
735	16:02:49.274602	10.196.147.132	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
766	16:02:49.566334	128.119.245.12	10.196.147.132	HTTP	540	HTTP/1.1 200 OK (text/html)

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

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?

IP Address of my computer (Source IP for GET Request) → 10.196.147.132

$IPofgaia.cs.umass.eduserver(DestinationIP) \rightarrow$ 128.119.245.12

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

Status Code: 200 OK

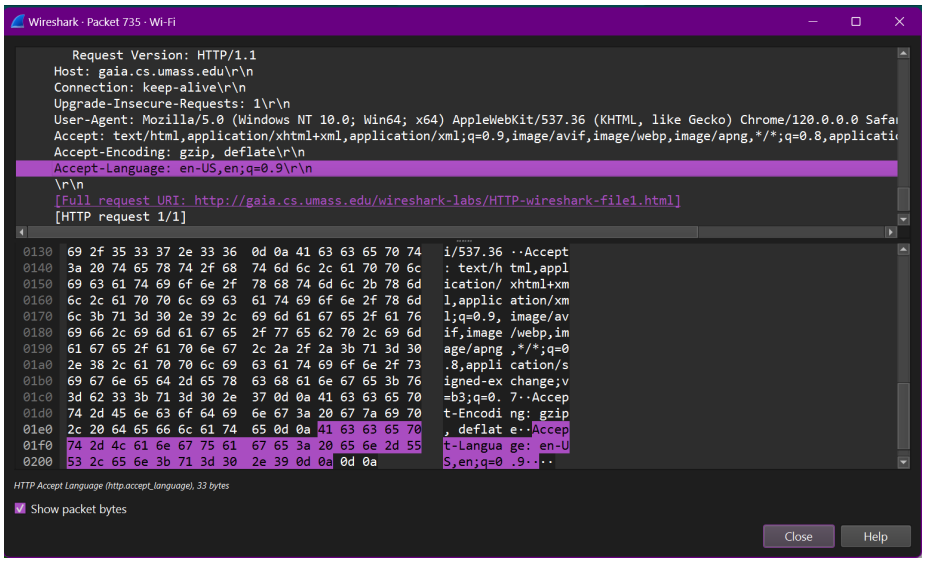


Figure 1: Q2. Accept-Language Higlighted

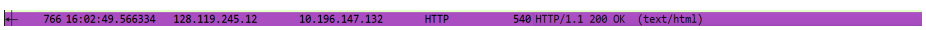


Figure 3: Q4. Status Code: 200 OK

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

Last-Modified: Tue, 16 Jan 2024 06:59:02 GMT\r \n

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

[Content length: 128 bits]

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.

No. All of the headers can be found in the raw data.

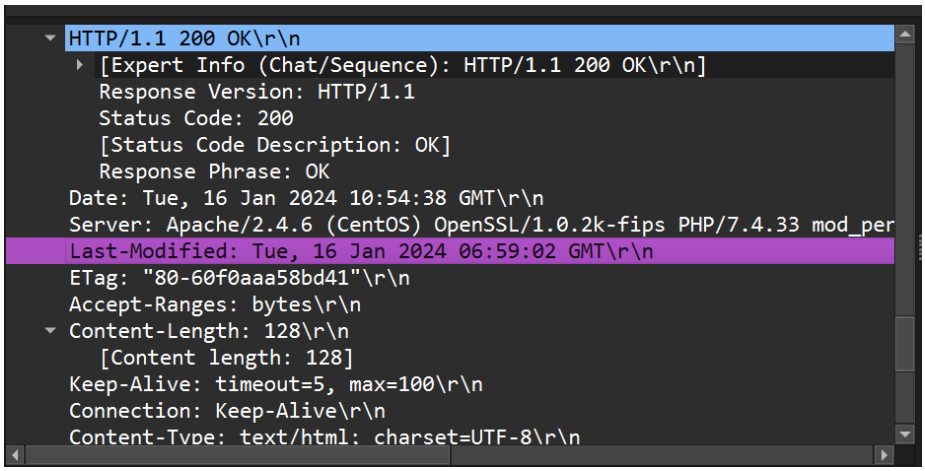


Figure 4: Q5. Last Modified

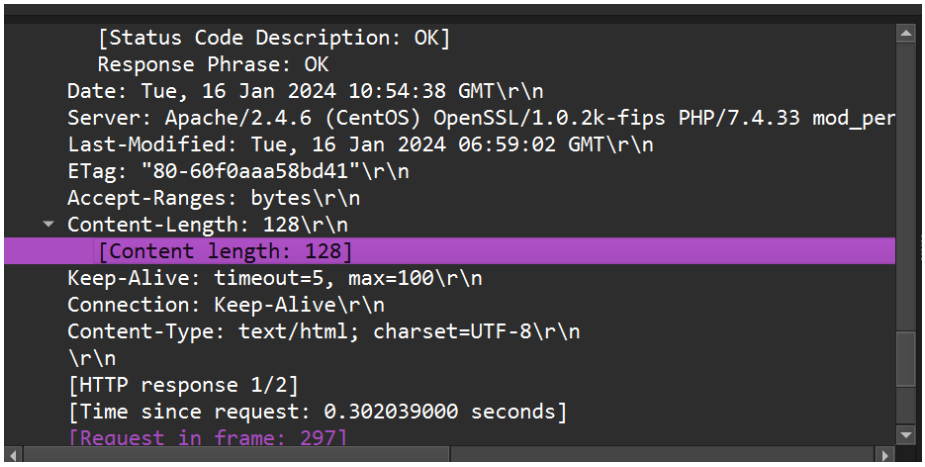


Figure 5: Q6. Content Bytes

2 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?

No. I am not able to see any "IF-MODIFIED-SINCE" line in HTTP GET.

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

Yes. I can see the content of the server response in Line-based text data: text/html (10 lines)

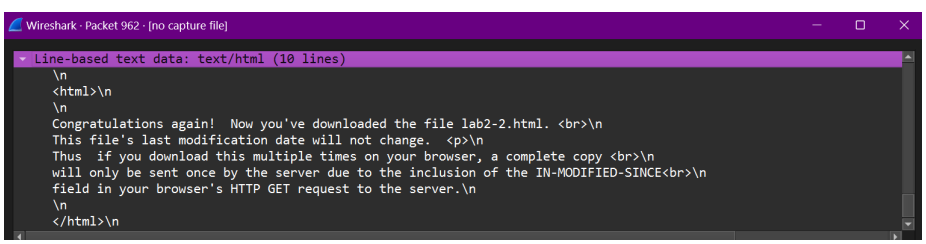


Figure 6: Q2. Line-based text data

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?

Yes. I can see "IF-MODIFIED-SINCE:" line in HTTP GET. It gives info about date and time i last accessed.

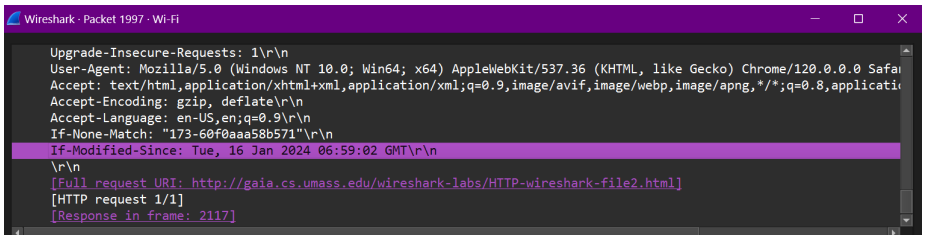


Figure 7: Q3. IF-MODIFIED-SINCE

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.

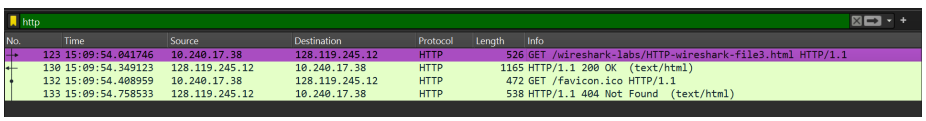
I am getting HTTP status code and phrase as **304 Not Modified** to second HTTP GET. The server did not explicitly return the contents of the file because it instructed the browser to get the content from its cache since it was not modified last.

Figure 8: Q4. HTTP status code and phrase

3 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 or Rights?

Browser sent 2 GET request messages to server as shown in the screenshot. Packet no. 123 contains GET message for the Bill of Rights.

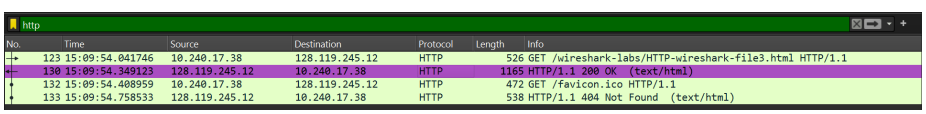


No.	Time	Source	Destination	Protocol	Length	Info
123	15:09:54.041746	10.240.17.38	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
130	15:09:54.349123	128.119.245.12	10.240.17.38	HTTP	1165	HTTP/1.1 200 OK (text/html)
132	15:09:54.408959	10.240.17.38	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
133	15:09:54.758533	128.119.245.12	10.240.17.38	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figure 9: Q1. HTTP GET request for the Bill or Rights

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

Packet No that contains status code and phrase associated with response to HTTP GET request is **130** as shown in the screenshot.



No.	Time	Source	Destination	Protocol	Length	Info
123	15:09:54.041746	10.240.17.38	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
130	15:09:54.349123	128.119.245.12	10.240.17.38	HTTP	1165	HTTP/1.1 200 OK (text/html)
132	15:09:54.408959	10.240.17.38	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
133	15:09:54.758533	128.119.245.12	10.240.17.38	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figure 10: Q2, Q3. Status code and phrase

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

Status code and phrase in the response 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?

Data was sent in 4 TCP segments that were needed to carry the single HTTP response and the text of the Bill of Rights.

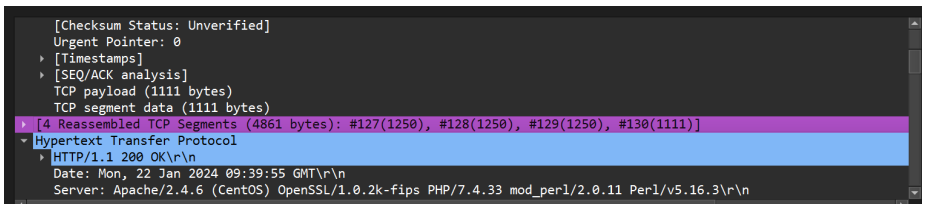


Figure 11: Q4. 4 TCP segments

---

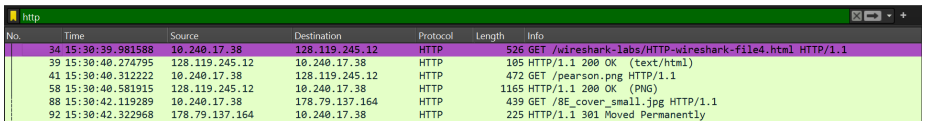
4 Part - 4 HTML Documents with Embedded Objects

---

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

My browser sent 3 HTTP GET request messages for first page contents, Logo of Pearson, and Cover of the Book.

First page address: **128.119.245.12**
Logo of Pearson: **128.119.245.12**
Cover of book: **178.79.137.164**



http

No.	Time	Source	Destination	Protocol	Length	Info
34	15:30:39.981588	10.240.17.38	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
39	15:30:40.274795	128.119.245.12	10.240.17.38	HTTP	105	HTTP/1.1 200 OK (text/html)
41	15:30:40.312222	10.240.17.38	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
58	15:30:40.581915	128.119.245.12	10.240.17.38	HTTP	1165	HTTP/1.1 200 OK (PNG)
88	15:30:42.119289	10.240.17.38	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
92	15:30:42.322968	178.79.137.164	10.240.17.38	HTTP	225	HTTP/1.1 301 Moved Permanently

Figure 12: Q1. HTTP GET request

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

Since there are separate connections for each image (gaia.cs.umass.edu and caite.cs.umass.edu), it's likely that they were downloaded in parallel. The responses for both images arrive around the same time, another indicator of parallel downloading.

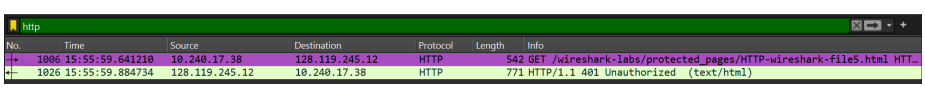
---

5 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?

Server's response is **401 Unauthorized.**



http

No.	Time	Source	Destination	Protocol	Length	Info
1006	15:55:59.641210	10.240.17.38	128.119.245.12	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTT…
1026	15:55:59.884734	128.119.245.12	10.240.17.38	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

Figure 13: Q1. server's response 401 Unauthorized

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

The new field is **Authorization** because this time we have sent a username and password to say that we are authorized to access this page.

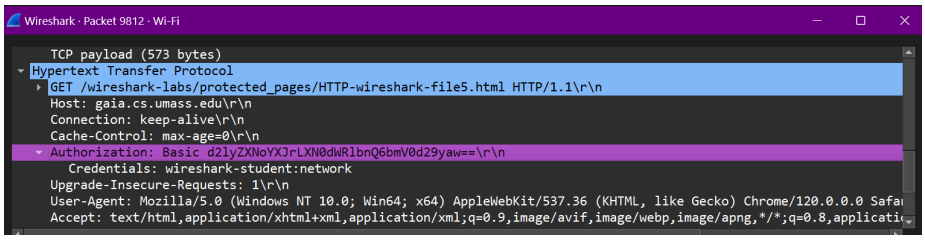


Figure 14: Q2. Authorization Field