CS315 : Computer Networks Lab

Assignment 3

Sourabh Bhosale (200010004)

January 17, 2023

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?

My browser is running on HTTP version 1.1 and server is running 1.1 version of HTTP

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

en-GB(Great Britain English), en-US(US english).

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

IP address of computer : 10.196.7.63
IP address of server : 128.119.245.12

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

Status code : 200

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

Last-Modified: Mon, 16 Jan 2023 06:59:01 GMT

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

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.

No, I don't see any headers within the data that are not displayed in the packet-listing window. For all the headers there are respective bytes there inside packet-listing window.

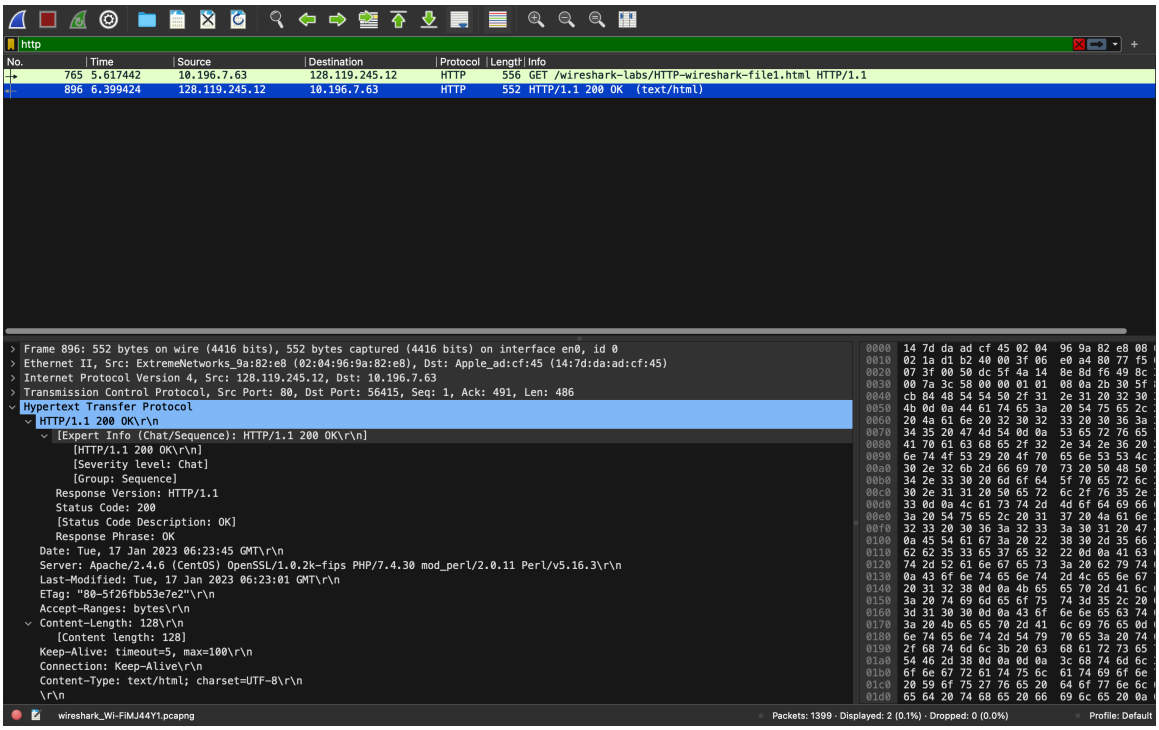


Figure 1: `Wireshark window : Part-1`

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, for the first HTTP GET request it doesn't show 'IF-MODIFIED-SINCE'.

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

Yes, it returned the contents of file. We can see that it says content length equal to 371 along with that it mentions content type also, which means that it had returned some content. It was showing the content information under the 'Line-based text data' header.

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, for the second HTTP GET request it shows 'IF-MODIFIED-SINCE'.
If-Modified-Since: Mon, 16 Jan 2023 06:59:01 GMT

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.

HTTP status code : 304
Response Phrase: Not Modified
No, it didn't return the contents of file. As no content length or content type was displayed there, which means no content is returned.

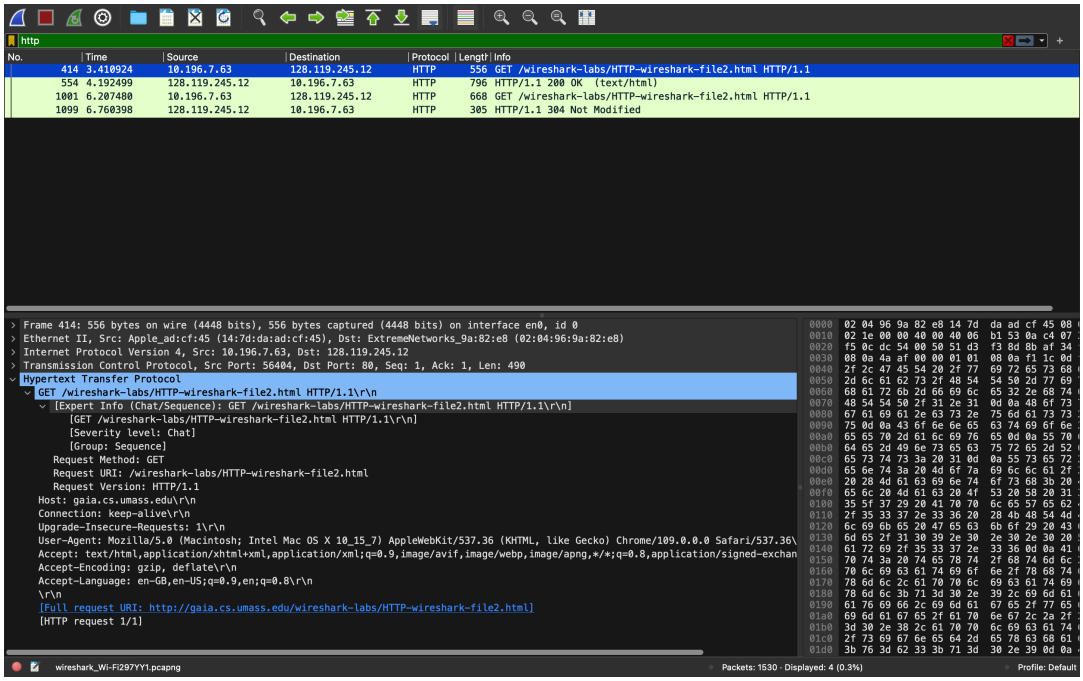


Figure 2: `Wireshark window : Part-2`

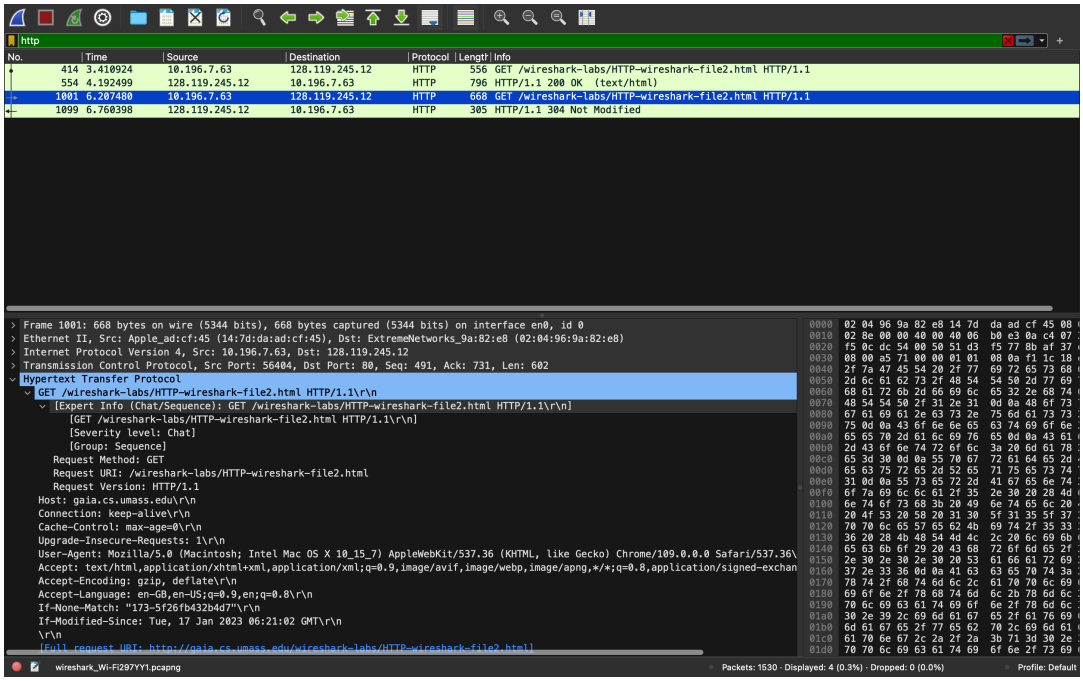


Figure 3: `Wireshark window : Part-2`

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?

Only 1 HTTP GET request message was send by my browser. Packet number : 917

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

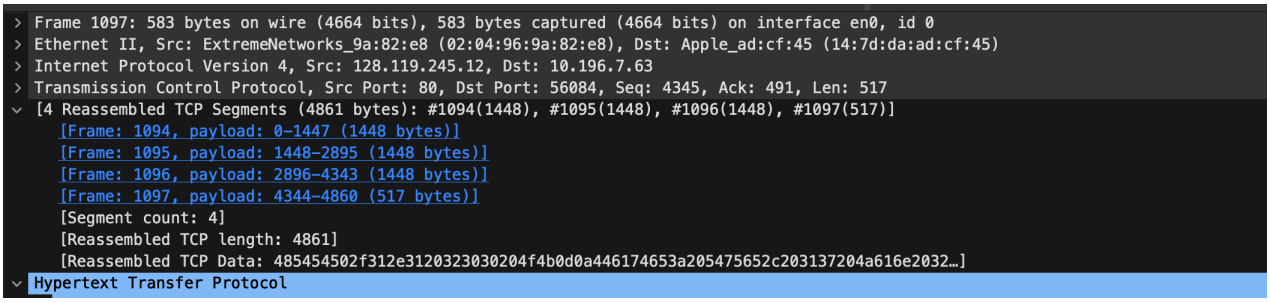
Packet number : 1097

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

Status Code: 200
Response Phrase: OK

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

4 Reassembled TCP Segments (4861 bytes).



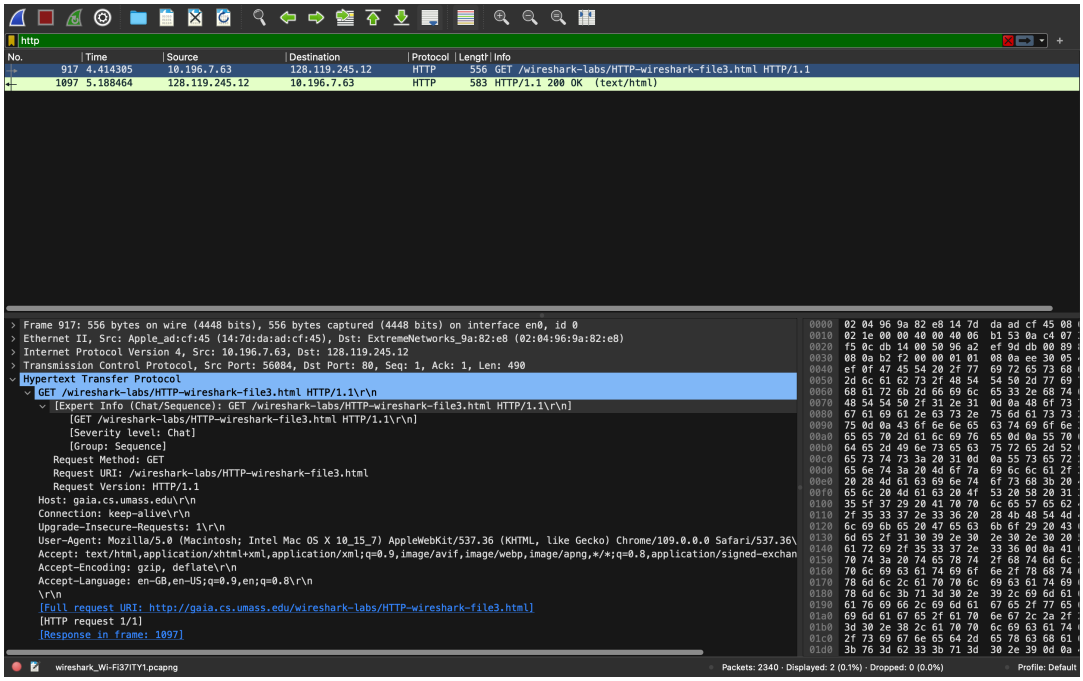


Figure 4: `Wireshark window : Part-3`

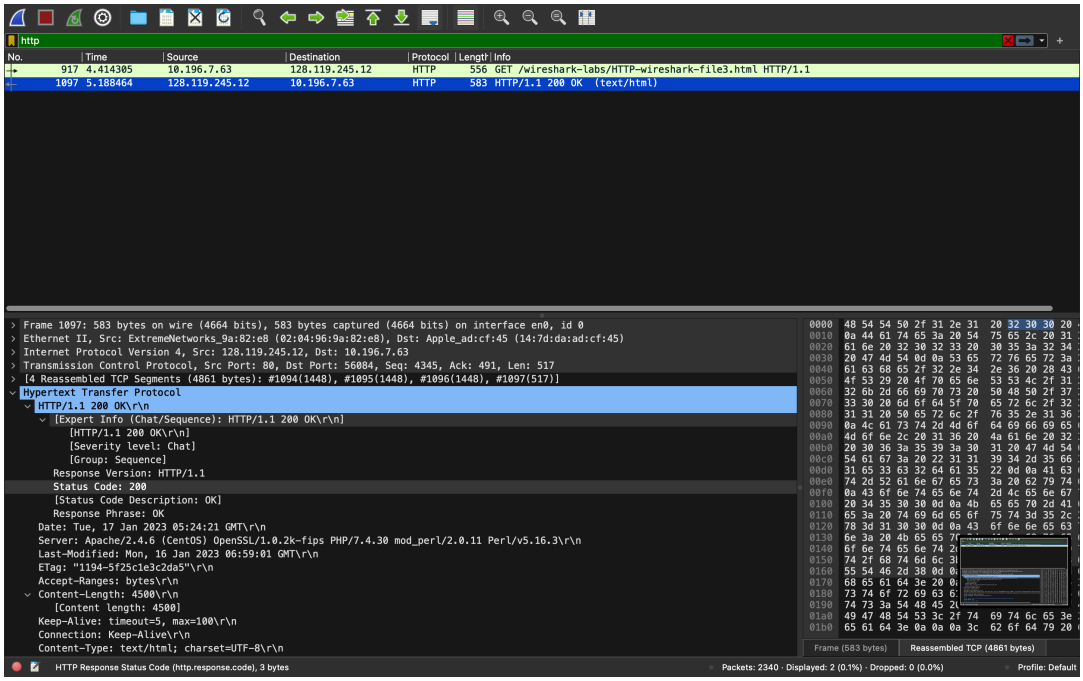


Figure 5: `Wireshark window : Part-3`

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?

3 HTTP GET request messages were send by my browser.
The internet addresses for the GET requests were 128.119.245.12, 128.119.245.12, 178.79.137.164 respectively.

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

They were downloaded from the two websites in parallel as we see two web servers here:
1. 128.119.245.12 - for downloading pearson.png image (logo image)
2. 178.79.137.164 - for downloading cover page image

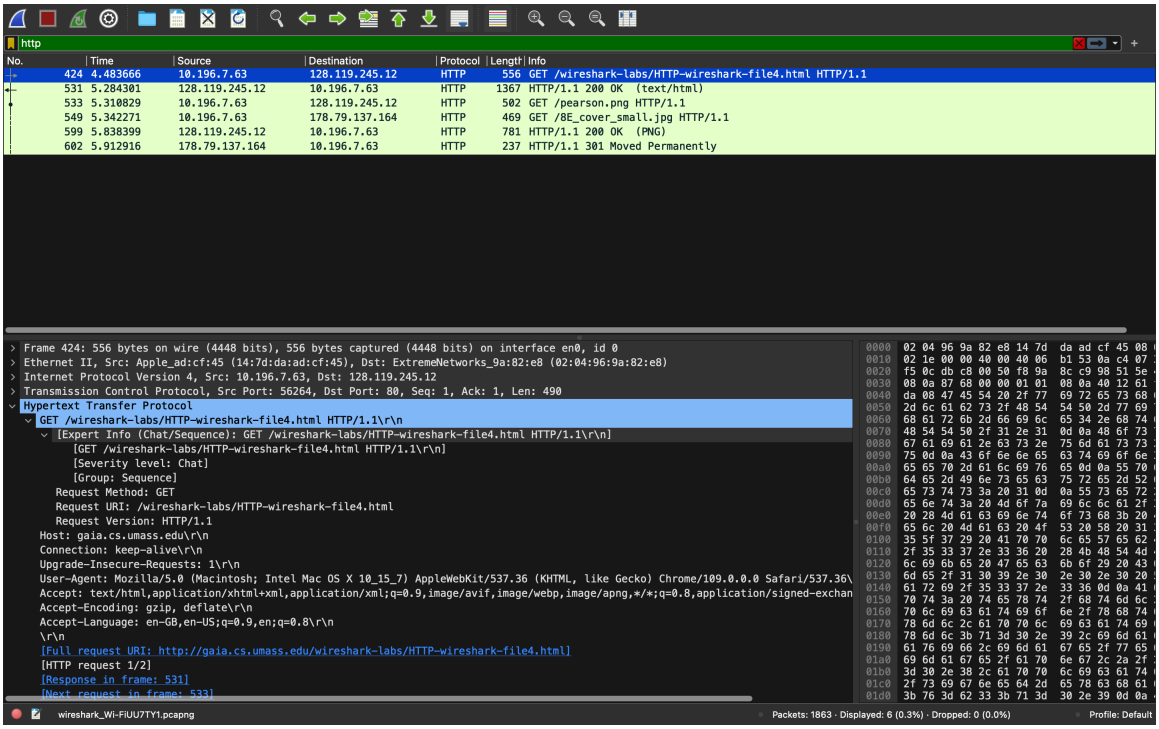


Figure 6: `Wireshark window : Part-4`

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?

Status Code: 401
Response Phrase: 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 `Authorization` was included for the second HTTP GET message which has description as mentioned in the following image.

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 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-exchan
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
```

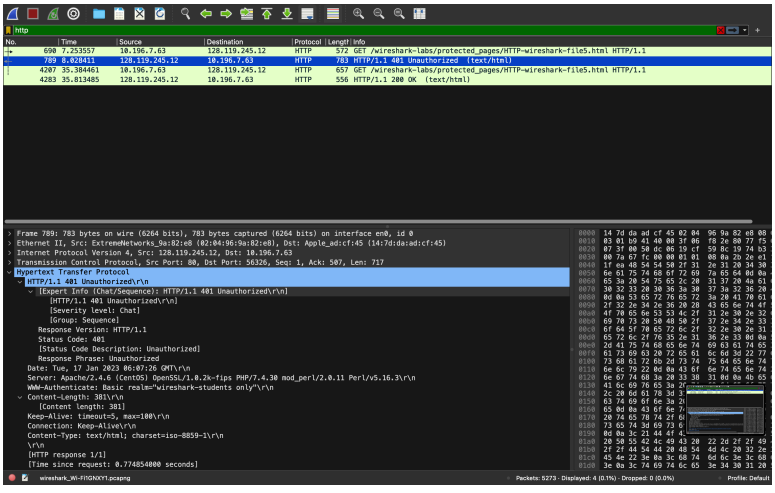


Figure 7: `Wireshark window : Part-5`