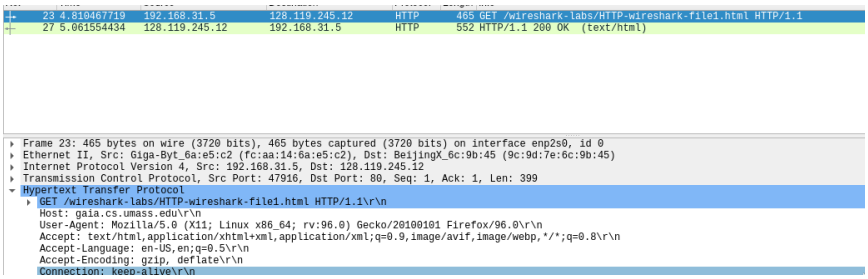
Contents

1 Basic HTTP Get Interaction

We first start the wireshark and wait for 2 minutes. Then we go to the site LINK and in the wireshark, set "http" in visual filter.

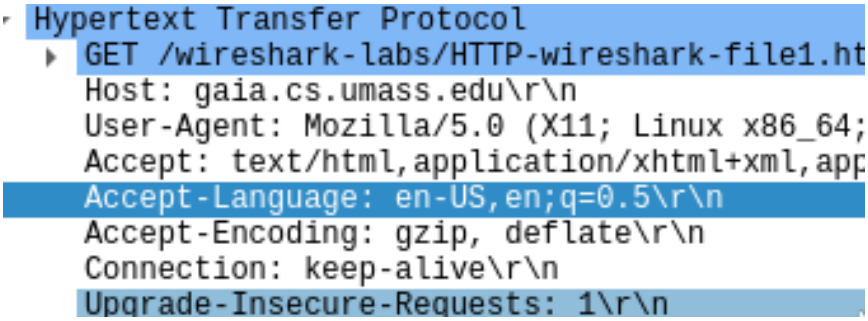
1.1 HTTP Version

HTTP 1.1
We checked the header section of the request and response message and found the same answer.



1.2 What Language can our browser accept from server?

en_{US}, meaning it accepts United States English Language only.



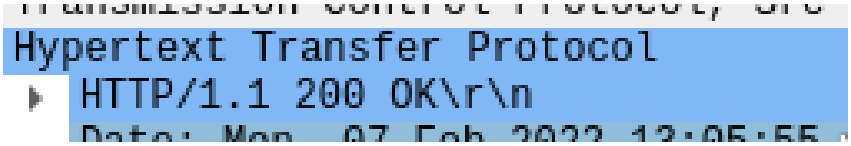
1.3 IP Address of our computer

192.168.31.5 -> Its the ip address of my computer.

	Time	Source	Destination
23	4.810467719	192.168.31.5	128.119.245.12
27	5.061554434	128.119.245.12	192.168.31.5

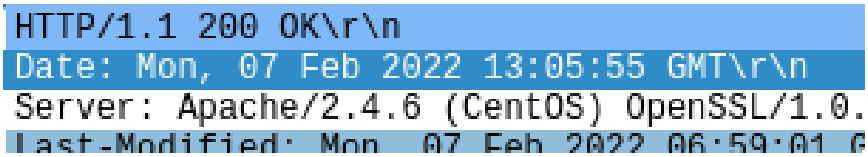
1.4 Status Code returned from Server to browser.

Server responsed `OK`.



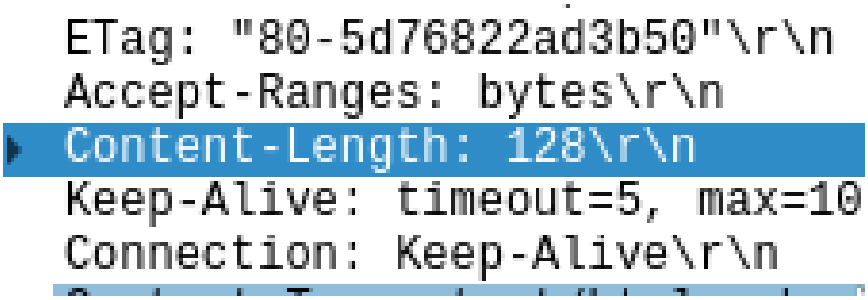
1.5 Last modified date of the html file

Current time (7 February, 2022, 7:05)
It seems it was stored in local ISP's `proxy server` as I requested for it multiple time as I forgot to clear my cache so no http requests were sniffed by wireshark.



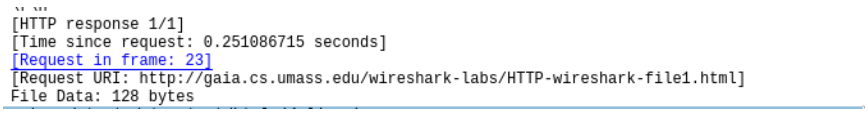
1.6 How many bytes of content are being returned to the browser?

128 Bytes.



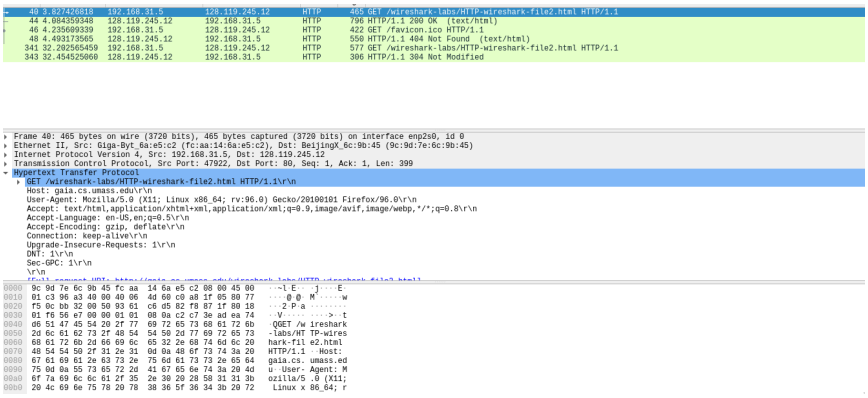
1.7 Raw Data Header and Packer Listing Window - do they differ?

Yes. The last four line in packet-listing-window were apparently extra meta data that wireshark decided to show us, We did not find this portion in raw bytes.



2 GET/Response Interaction

This is our wireshark output after we requested for the website.

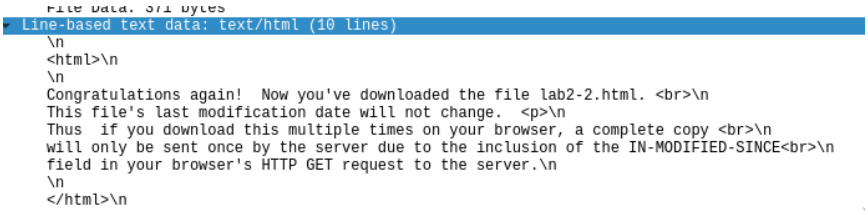


2.1 Any $\text{IF}_{\text{MODIFIEDSINCE}}$?

No. There were no $\text{IF}_{\text{MODIFIEDSINCE}}$ in the first GET message.

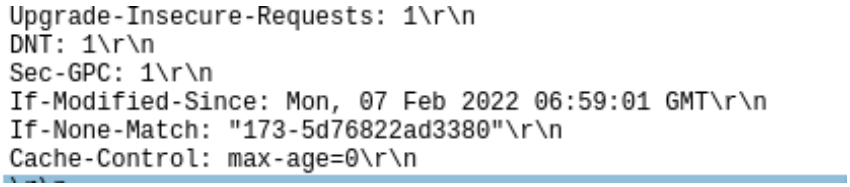
2.2 Did the server explicitly returned content file?

Yes. It did.



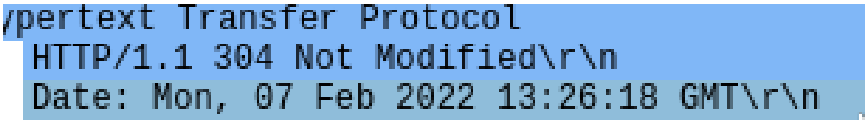
2.3 Afrer refresh, any $\text{IF}_{\text{MODIFIEDSINCE}}$?

Yes.



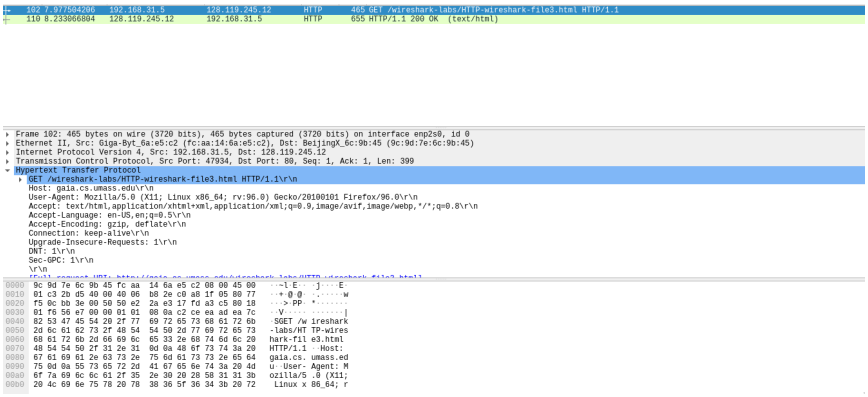
2.4 After resfresh, status code and response.

Status code: Not modified
Text Data: None.



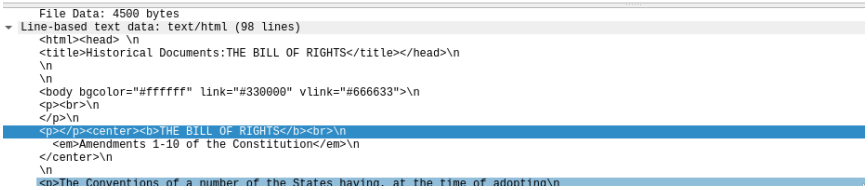
3 Long Documents

Entire output for 3rd capture is:



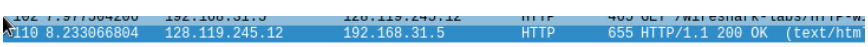
3.1 How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Only One get message.
Packet Number 102. The response message from server contains it.



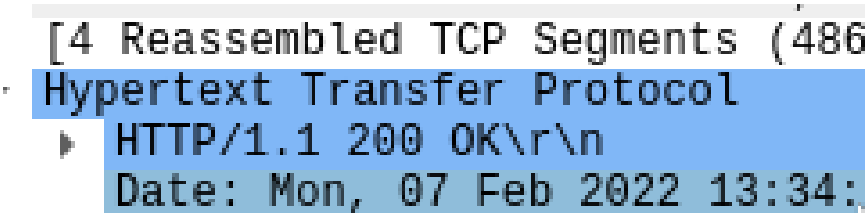
3.2 Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

packet 110.
Response: Ok.



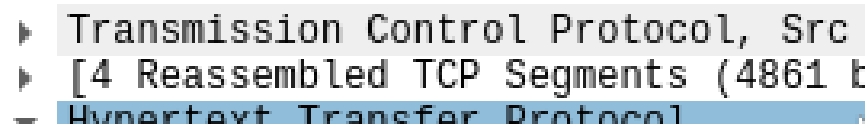
3.3 What is the status code and phrase in the response?

200 Ok.



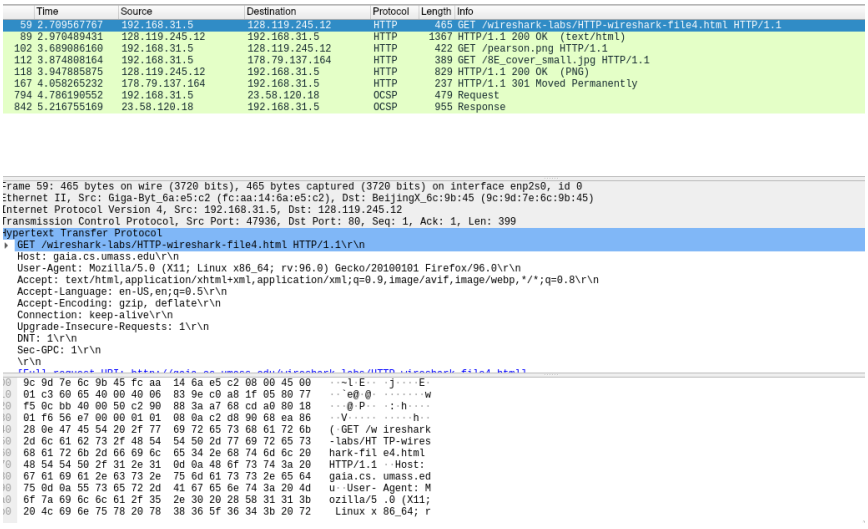
3.4 How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

4 TCP segments.



4 Documents with Embeded Objects

The capture for this part is:



No.	Time	Source	Destination	Protocol	Length	Info
59	2.709567767	192.168.31.5	128.119.245.12	HTTP	465	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
89	2.970489431	128.119.245.12	192.168.31.5	HTTP	1367	HTTP/1.1 200 OK (text/html)
102	3.689086160	192.168.31.5	128.119.245.12	HTTP	422	GET /pearson.png HTTP/1.1
112	3.874808164	192.168.31.5	178.79.137.164	HTTP	389	GET /8E_cover_small.jpg HTTP/1.1
118	3.947885875	128.119.245.12	192.168.31.5	HTTP	829	HTTP/1.1 200 OK (PNG)
167	4.058265232	178.79.137.164	192.168.31.5	HTTP	237	HTTP/1.1 301 Moved Permanently
794	4.786190552	192.168.31.5	23.58.120.18	OCSP	479	Request
842	5.216755169	23.58.120.18	192.168.31.5	OCSP	955	Response

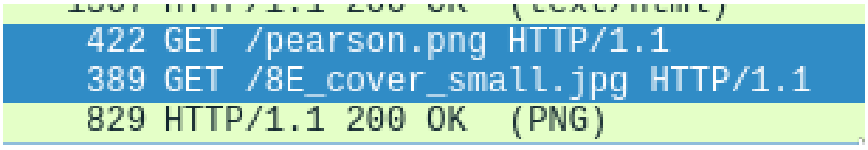
4.1 Number of GET requests and Where were they sent?

3 GET messages. They were sent to:

- 128.119.245.12
- 128.119.245.12
- 178.79.137.164

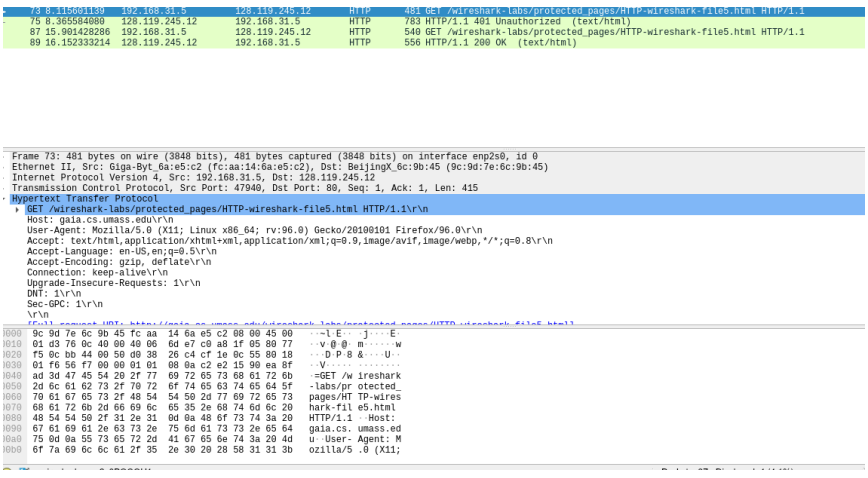
4.2 Images downloaded Serially or parallely?

Parallely. Because the GET requests for both of them were sent first and then we eventually got the response messages for the image GET requests.



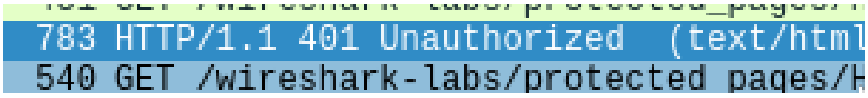
5 HTTP Authentication

The total capture for this section is:



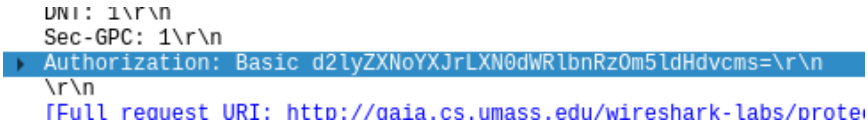
5.1 Server's Response to Initial GET Request

Status Code: 401
Phrase: Unauthorized



5.2 When sending the GET request for the second time, what new field was included?

Authorization was the new field.
It carries the very basic encrypted form of our username and password.



6 About Me

Abhijit Paul
BSSE 1201

Institute of Information & Technology
University of Dhaka