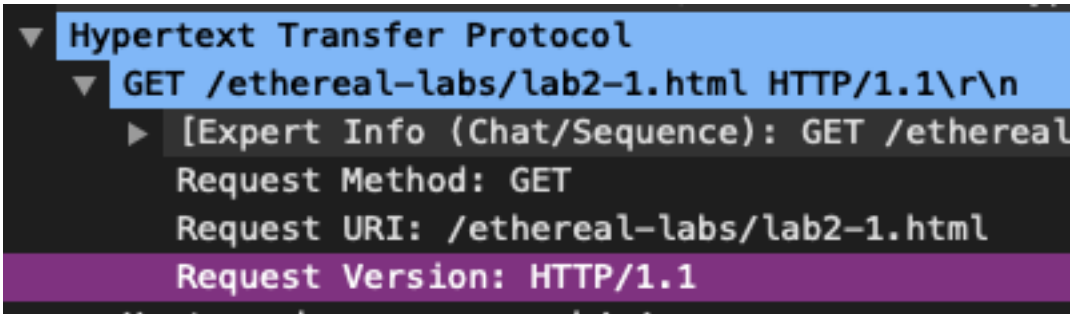
HTTP Analysis using Wireshark

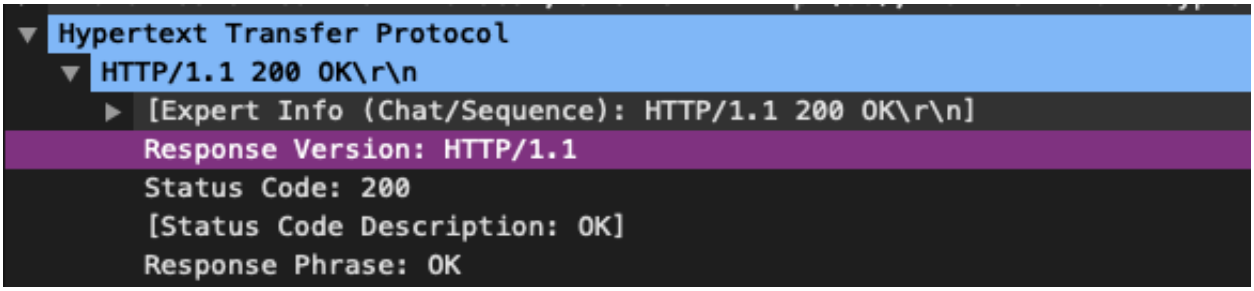
Sumaya Altamimi
442203026

Part1: The Basic HTTP GET/response interaction

Is your browser running HTTP version 1.0 or 1.1?
1.1 as shown below.



What version of HTTP is the server running?
1.1 as well.

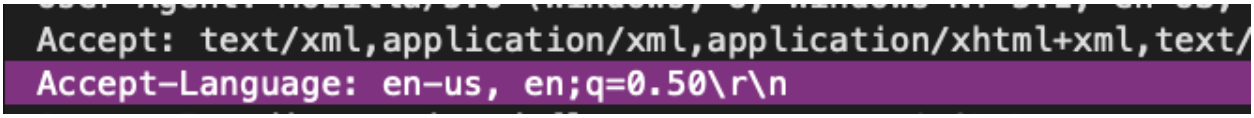


Response Version: HTTP/1.1

Response Version: HTTP/1.1

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

English language – US

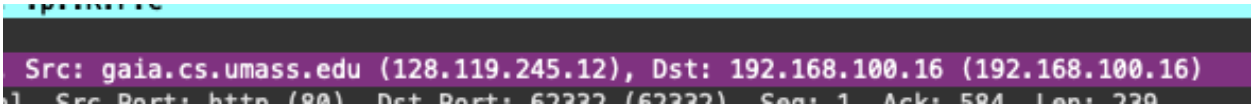


Accept-Language: en-us, en;

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

My computer: 192.168.100.16

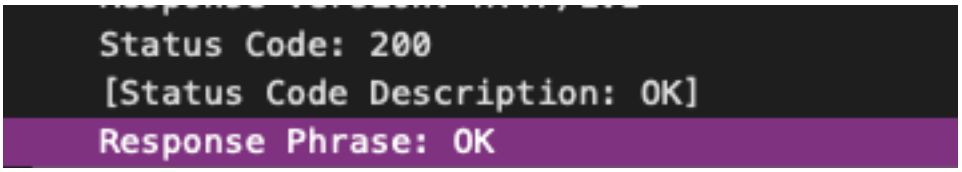
gaia.cs.umass.edu server: 128.119.245.12



Internet Protocol Version 4, Src: gaia.cs.umass.edu (128.119.245.12), Dst: 192.168.100.16 (192.168.100.16)

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

The status code: 200 OK

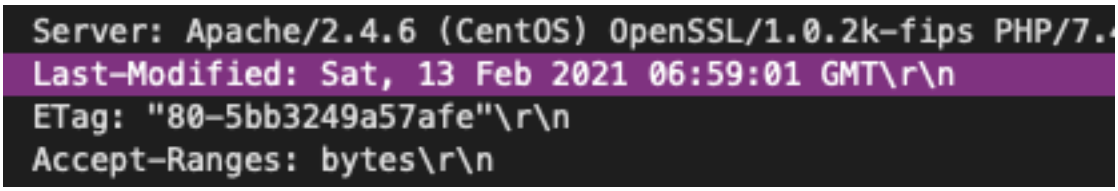


Status Code: 200

[Status Code Description: OK] Response Phrase: OK

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

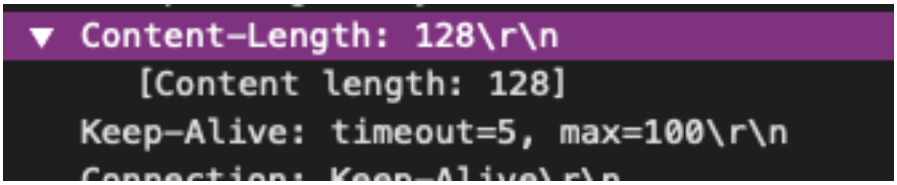
Today, one minute ago as shown below.



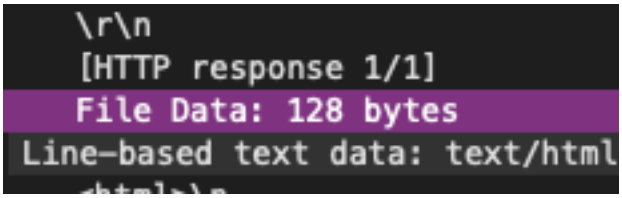
Last-Modified: Sat, 13 Feb 2021 06:59:01 GMT\r\n

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

Content Length is 128\r\n



But File Data is 128 Bytes



Content-Length: 128\r\n

[Content length: 128]

Keep-Alive: timeout=5, max=100\r\n Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n \r\n

[HTTP response 1/1]

File Data: 128 bytes

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.

Part2: The HTTP CONDITIONAL GET/response interaction

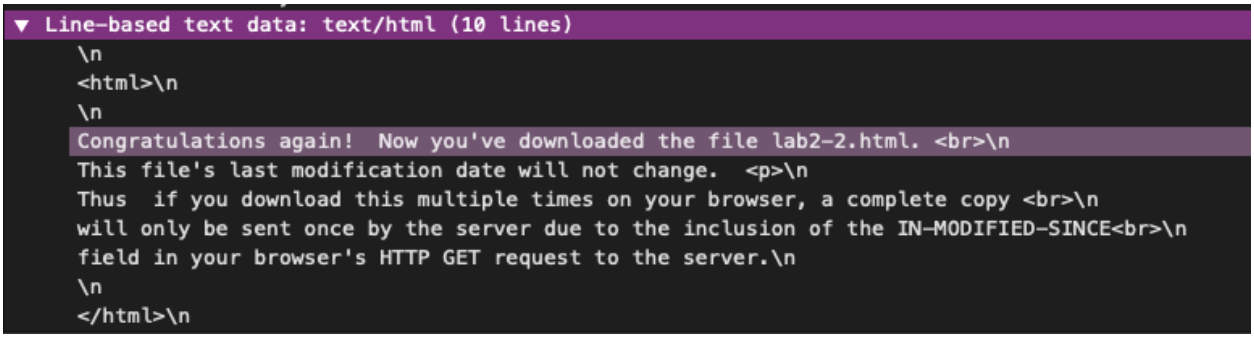
In this part and till the end of tutorial, I am going to use the captured data as describes in the assignment problem.

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.

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

Yes. As shown below:



Line-based text data: text/html (10 lines)

\n

<html>\n

\n

Congratulations again! Now you've downloaded the file lab2-2.html.
\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
\n

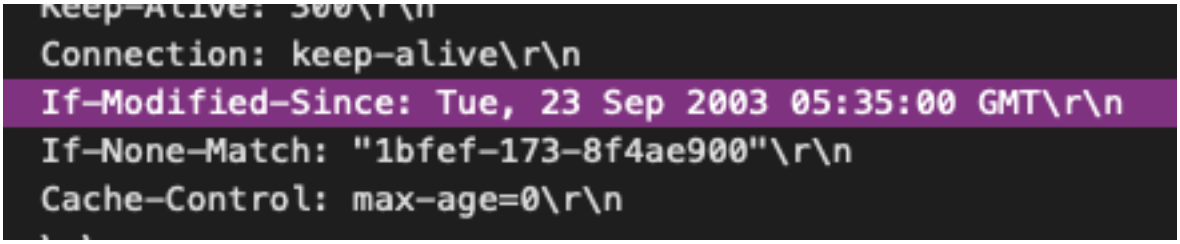
will only be sent once by the server due to the inclusion field in your browser's HTTP GET request to the server.\n \n

</html>\n

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?

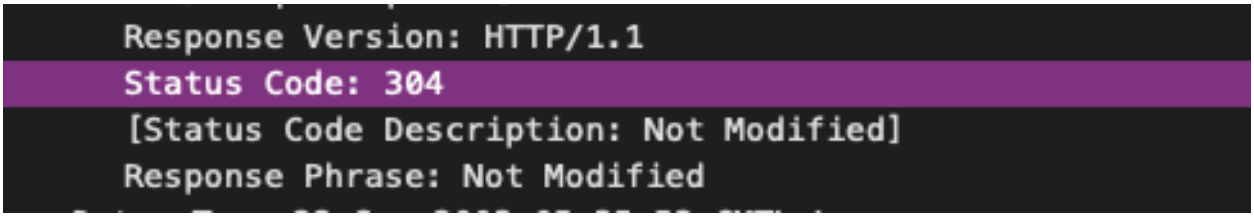
Yes. The time and date data modified after the last update/request. As shown:



If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n

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.

No. The status code is 304. The phrase is Not modified as shown below. Explanation: The second time I refresh the page only and there is no need to get the page again from the server. So, it is already stored in the cache.



304 Not Modified

Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)

Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23

36:23)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)

Transmission Control Protocol, Src Port: http (80), Dst Port: 4247 (4247), Seq: 686, Ack:

1116, Len: 189

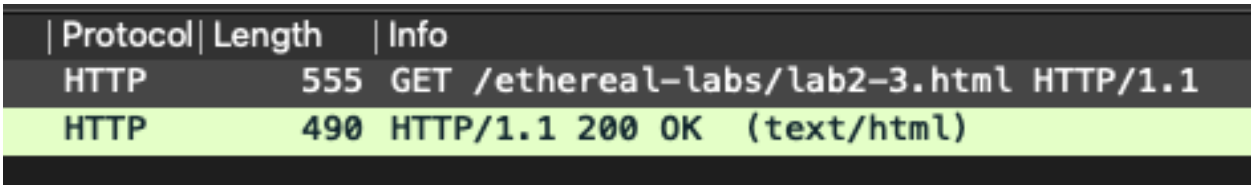
Hypertext Transfer Protocol

No. HTTP/1.1 304 Not Modified\r\n

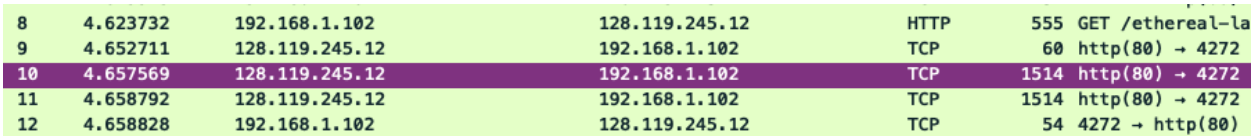
Part3: Retrieving Long Documents

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"?

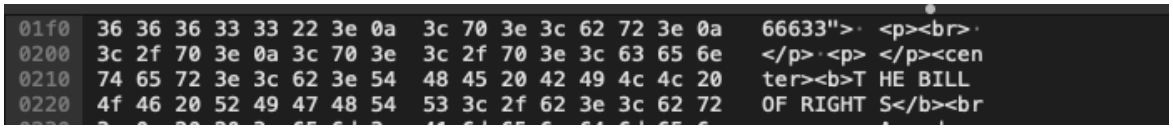
Only one request message as shown below. The packet number is 8.



The first part of the message (The Bill of Rights) is handled by the second TCP segment (or packet number 10 in our case) as shown below. After clicking in the second TCP packet for details:

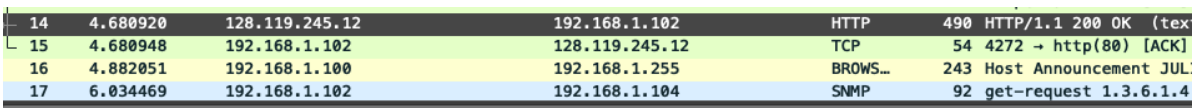


The part of the message shown below:



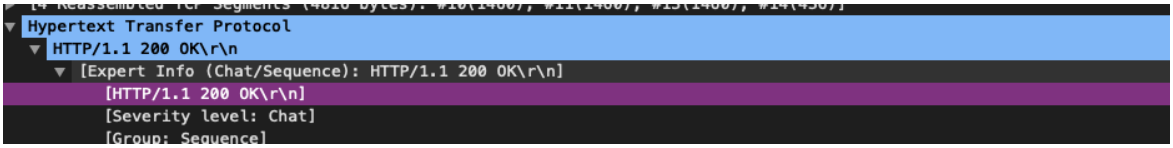
Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Packet number 14 contains the HTTP response status code and phrase.



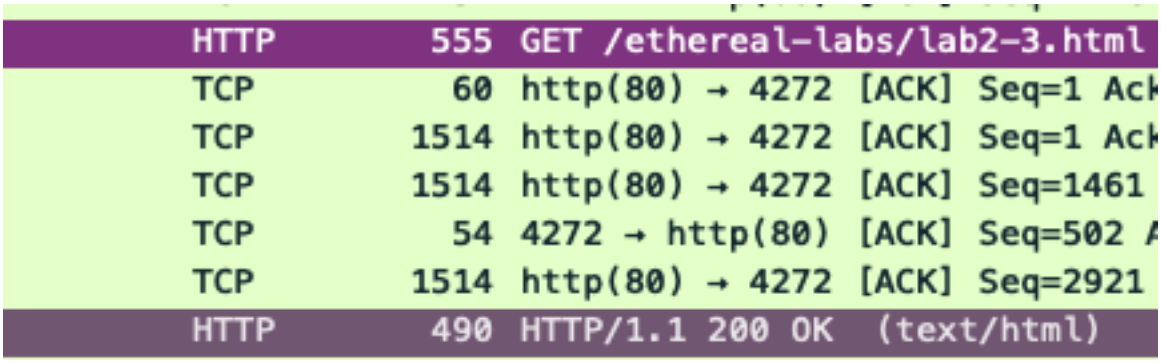
What is the status code and phrase in the response?

200 OK.



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

5 TCP segments were needed to handle all the text of Bill of Rights as shown below.



Part4: HTML Documents with Embedded Objects

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

There are three GET messages from my browser.

These are sent to 128.119.245.12, 165.193.123.218, and to 134.241.6.82 as shown below.

Source	Destination
192.168.1.102	128.119.245.12
128.119.245.12	192.168.1.102
192.168.1.102	165.193.123.218
192.168.1.102	134.241.6.82
165.193.123.218	192.168.1.102
134.241.6.82	192.168.1.102

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

First, from downloading the page visually I noticed that the first image is displayed before the second one.

Second, from Wireshark we can see the time of the requests and responses are serial as shown:

Time
7.236929
7.260813
7.305485
7.308803
7.333054
7.589877

Finally, if we remove the HTTP filter in Wireshark, we can see that multiple TCP segments before and after the HTTP request and response.

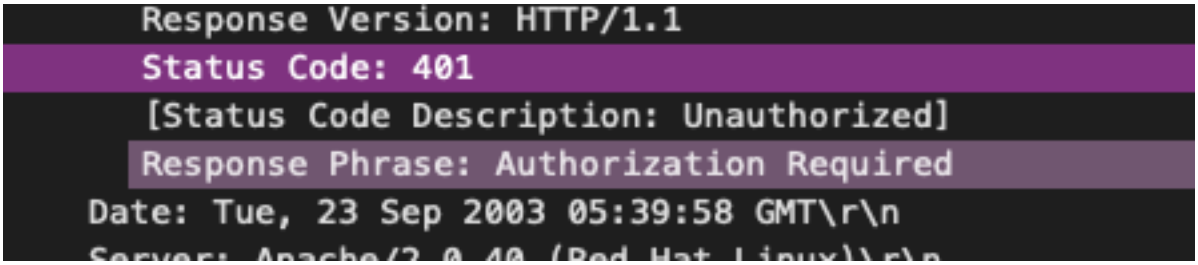
Which means they are not downloaded in parallel. The two images are downloaded serially.

Part5: HTTP Authentication

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: Authorization Required



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

Authorization. As shown: