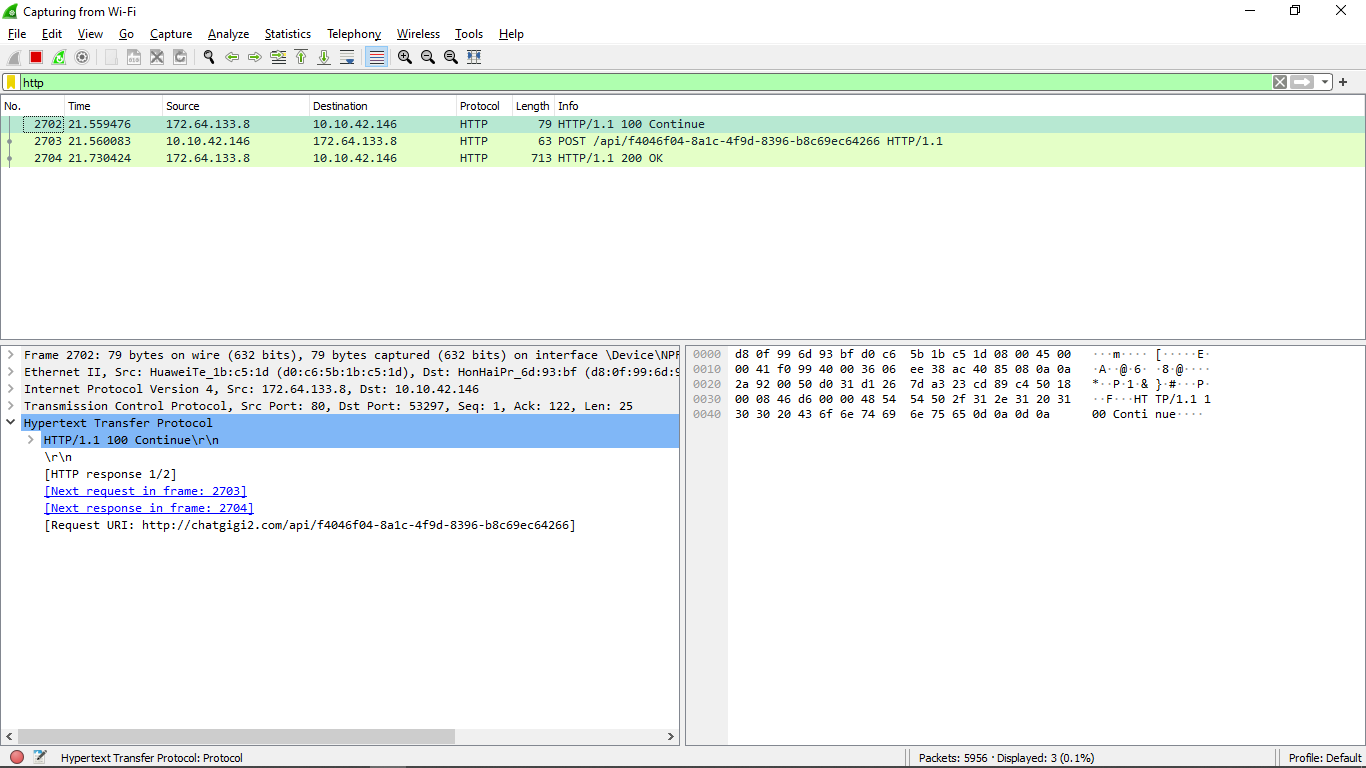
Name: Fatima Sohail Shaukat

Roll # 2020-CE-37

Task 1:



4.

C :\Users\DELL\A ppData\Local\Temp\wireshark\_Wi-Fi3ZX6Z1.pcapng 45891 total packets, 12 shown

No. Time Source Destination Protocol Length Info

3851 27.752273 172.64.133.8 10.10.42.146 HTTP 80 HTTP/1.1 100 Continue

Frame 3851: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF\_{338D6C75-6A2E-46E1-AFBE-B928AC832714},

id 0

Ethernet II, Src: HuaweiTe\_1b:c5:1d (d0:c6:5b:1b:c5:1d), Dst: HonHaiPr\_6d:93:bf (d8:0f:99:6d:93:bf)

Internet Protocol Version 4, Src: 172.64.133.8, Dst: 10.10.42.146

Transmission Control Protocol, Src Port: 80, Dst Port: 53297, Seq: 1, Ack: 122, Len: 25

Hypertext Transfer Protocol

HTTP/1.1 100 Continue\r\n

\r\n

[HTTP response 1/8]

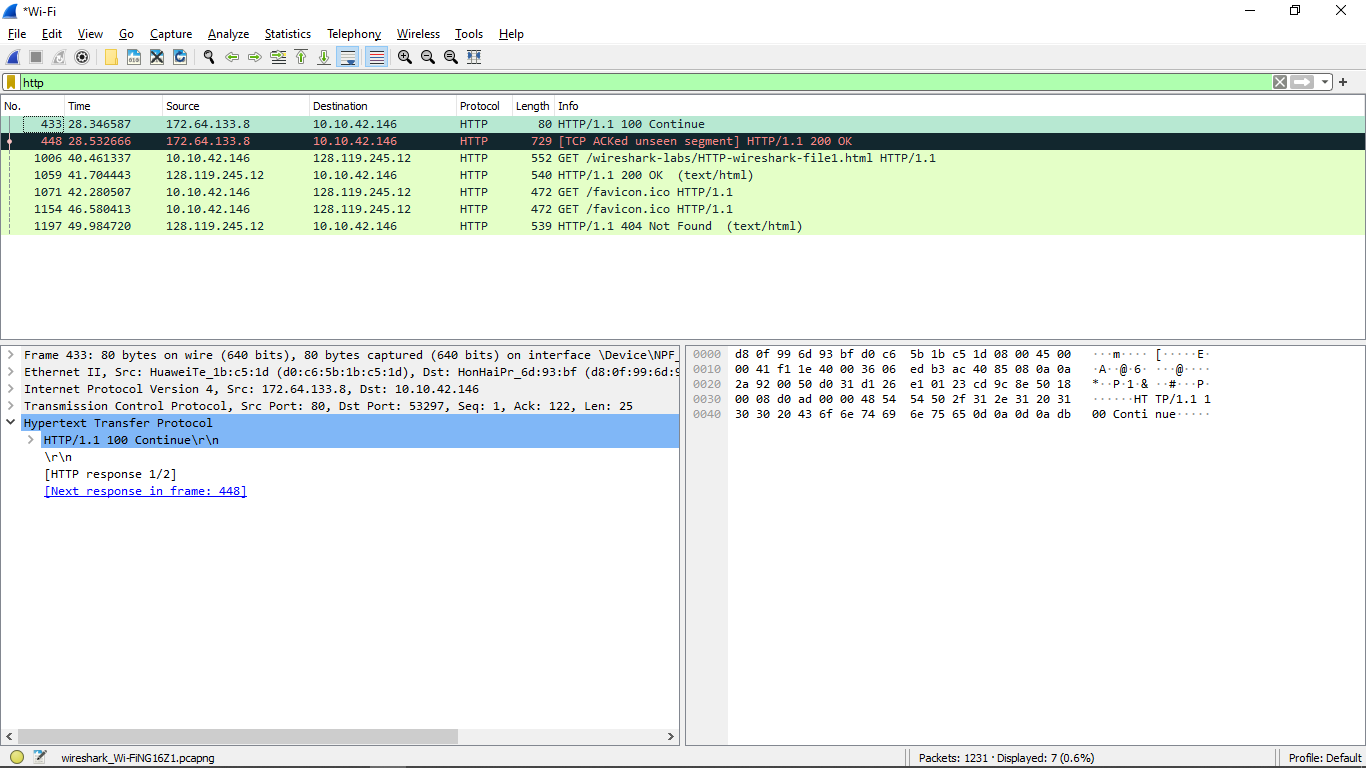
[Next request in frame: 3853]

[Next response in frame: 4054]

[Request URI: <http://chatgigi2.com/api/1b5f0607-515b-4f6e-a9e6-2862f6e38beb>]

**Section 1:**





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

My browser and the HTTP server are both running version 1.1.



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

Language is English



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

IP address of my computer is 10.10.42.146 and that of Destination is 128.119.245.12



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

Status Code: 200



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

****

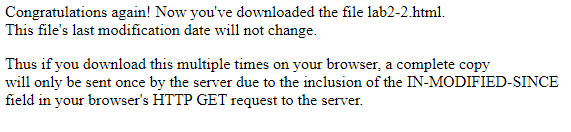
1. **How many bytes of content are being returned to your browser?**

**[Content length: 128]**

1. **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.**

**I do not see any different headings between the two windows**

**Task 3:**

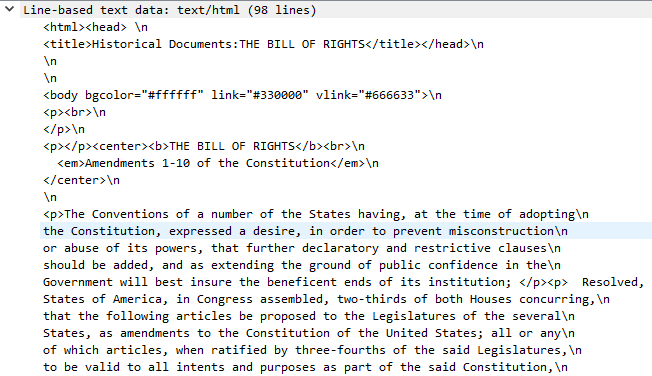
****

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?**

**If-Modified-Since: Tue, 07 Feb 2023 06:47:02 GMT\r\n**

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

**The server did explicitly return the contents of the file. Wireshark includes a section titled “Line-Based Text Data” which shows what the server sent back to my browser which is specifically what the website showed when I brought it up on my browser.**

****

1. **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?**

**There is no second HTTP GET.**

1. **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.**

**The HTTP status code is “304: Not Modified”**

**The server did not return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.**

**Task 4:**

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?**

My browser only sent 1 HTTP GET request to the server. The Packet that contained the GET message was packet number 2195.

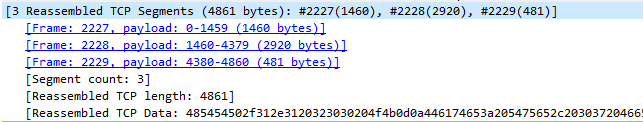
1. **Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**

**The packet that contains the status code and phrase which the server sent in response to the GET message was packet number 2229.**

1. **What is the status code and phrase in the response?**

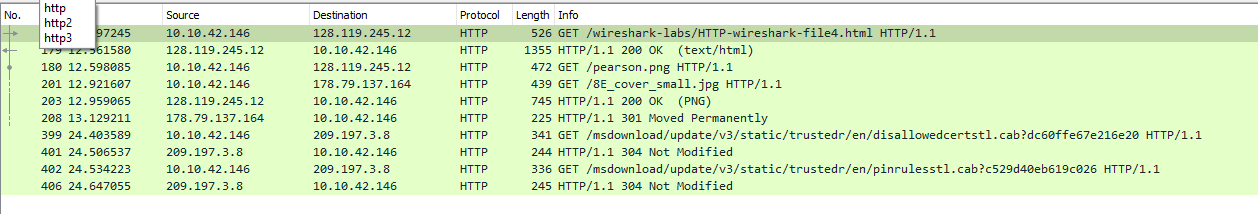
**The code and phrase in the response was 200 OK.**

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

**The data was sent in 3 TCP segments to the browser, then reassembled.**

**Task 4:**

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

****

**My browser sent 5 http GET message requests of the following:**

* **Pearson Logo**
* **Cover Page**
* **The initial page**
* **2 download requests**

**Initial Page address: 128.119.245.12**

**Pearson Logo: 128.119.245.12**

**Cover Page: 178.79.137.164**

**Downloads: 209.197.3.8**

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

**The two images are downloaded serially.**

****

**Task 5:**

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

**The servers intial response was “401 Unauthorized”**

****

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

**The new field that is now included is the authorization field. This is included because we sent the server a username and password along with our request stating that we were authorized to receive the page.**

****