Ayush Singh Rathore
AP21110010570

Mobile & wireless Security

LAB-2 Assignment

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

Ans: Version 1.1

```
Hypertext Transfer Protocol
    GET /connecttest.txt HTTP/1.1\r\n
    Connection: Close\r\n
    User-Agent: Microsoft NCSI\r\n
    Host: www.msftconnecttest.com\r\n
    \r\n
    [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
    [HTTP request 1/1]
    [Response in frame: 813]
```

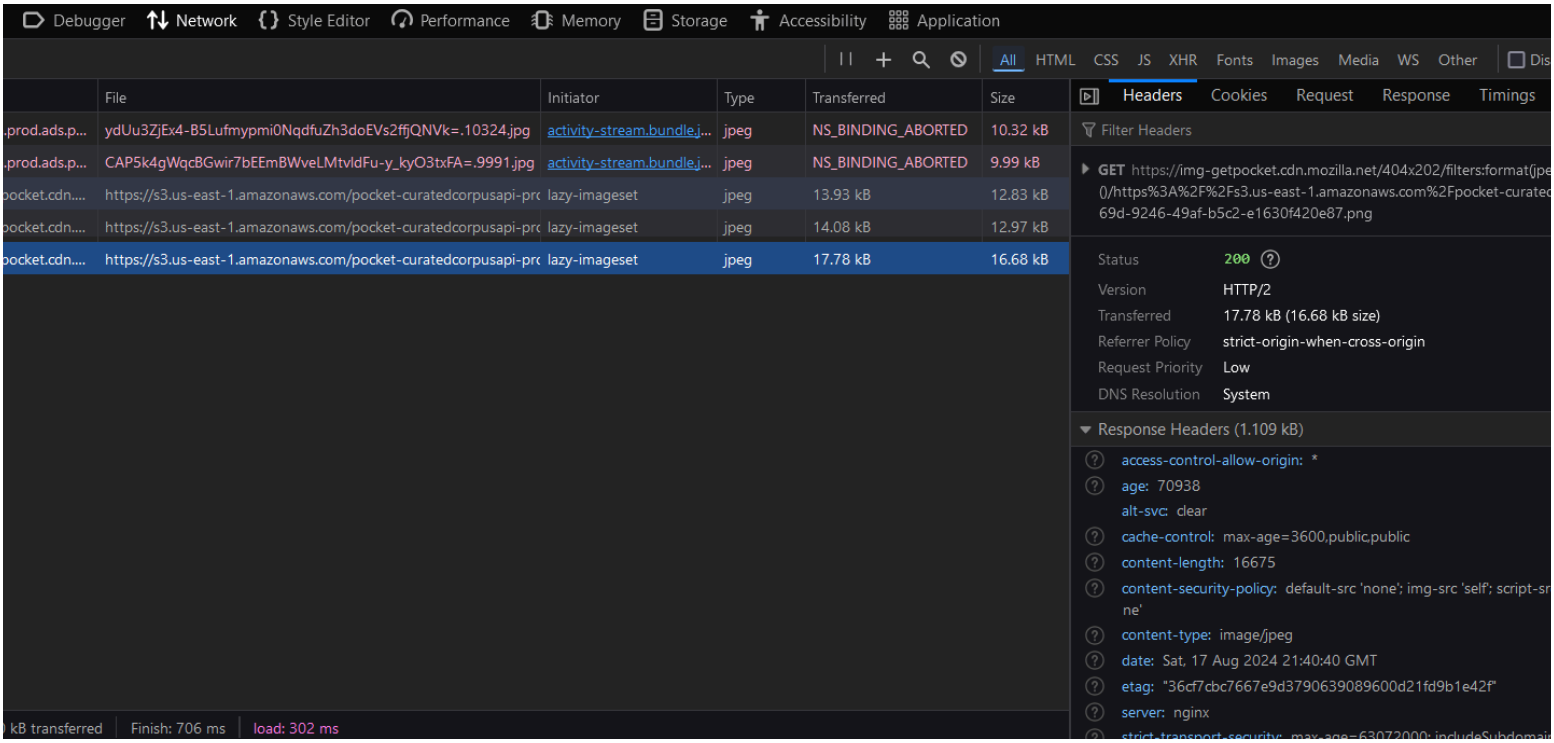
2. What languages (if any) does your browser indicate that it can accept to the server?

Ans: Accept-Language: en-US,en;q=0.5

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

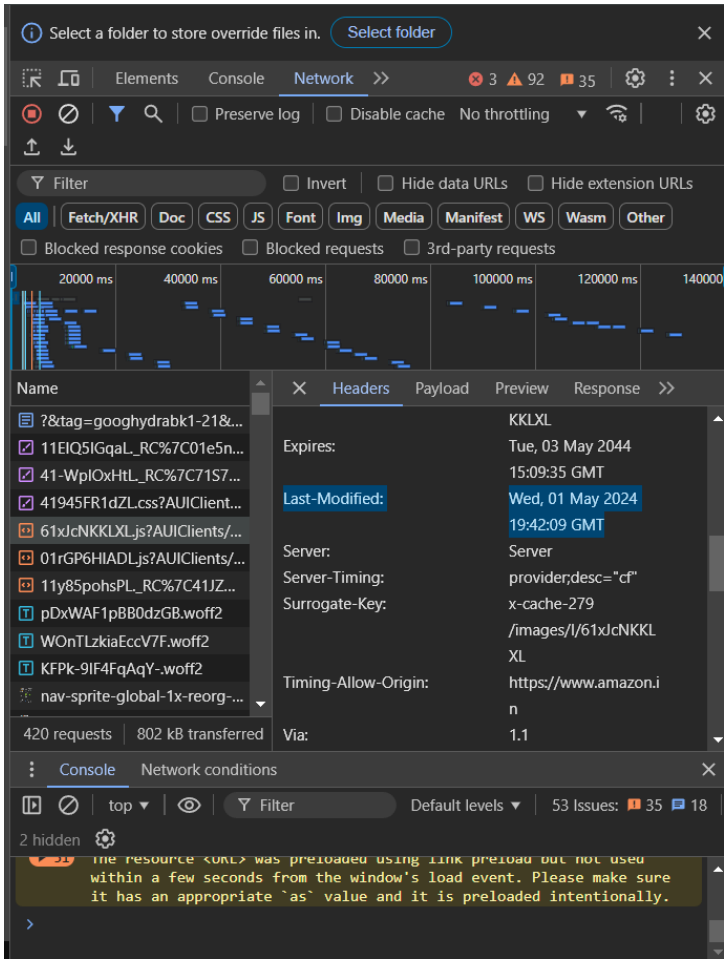
Ans: IP address: 192.168.56.1
IP address of gaia.cs.umass.edu server: [128.119.245.12]

4. What is the status code returned from the server to your browser?
Ans: 200



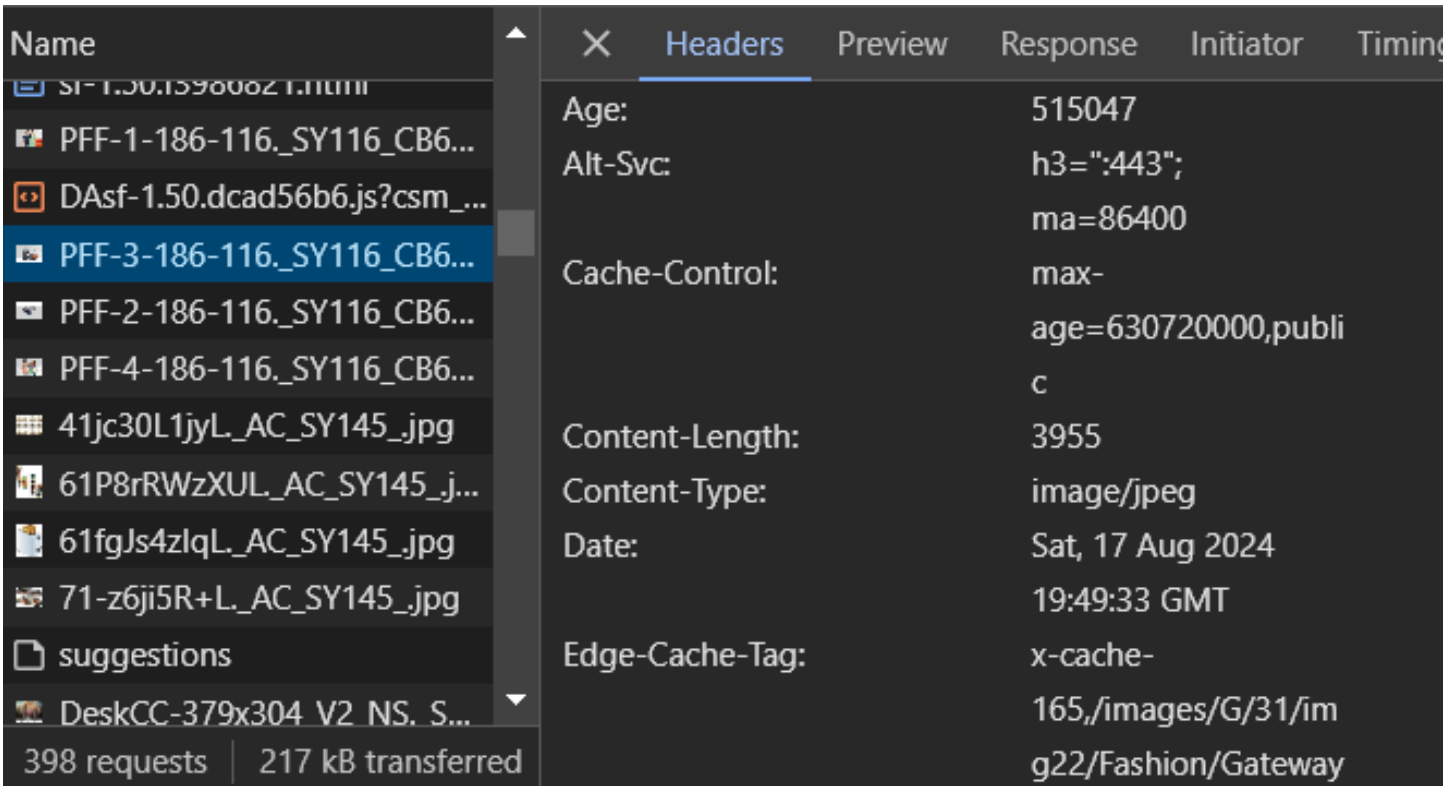
5. When was the HTML file that you are retrieving last modified at the server?

Ans:



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

Ans:



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.

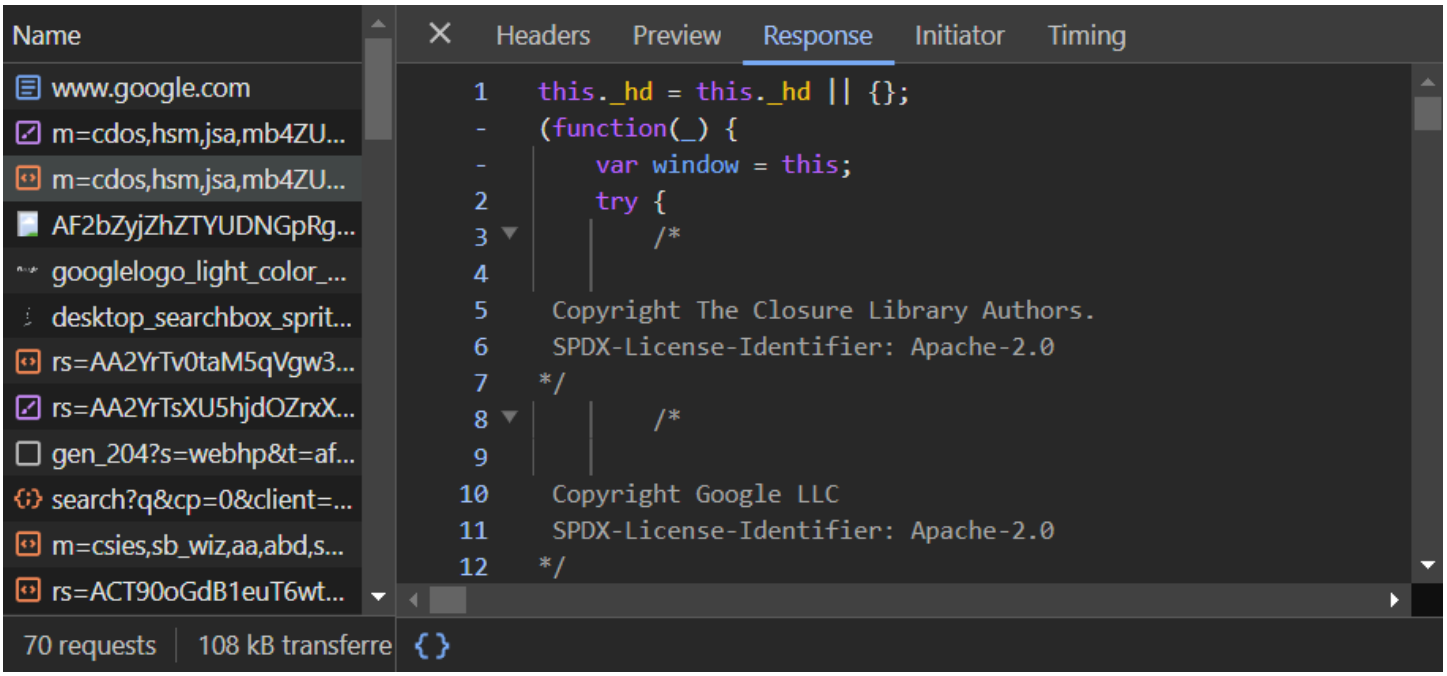
Ans: no, I don't see any in the HTTP Message below.

8. 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?
Ans: No, I cannot see it.

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

Ans:



10. 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?
Ans:

11. 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.
Ans:

12. How many HTTP GET request messages did your browser send? Answer: 1. Which packet number in the trace contains the GET message for the Bill or Rights?

Ans: 8.

13. Which packet number in the trace contains the status code and phrase associated with the

response to the HTTP GET request?

Ans: packet 10.

14. What is the status code and Phrase in the response?

Ans: 200 (OK)

15. How many data-containing TCP segments were needed to carry the single HTTP

response and the text of the Bill of Rights?

Ans: three packets (10, 11, 13 in the trace)

16. How many HTTP GET request messages did your browser send?

Ans: there were three HTTP GET messages sent: packet 10 in the trace (to get the base file), packet 17 (to get the Pearson logo) and packet 20 (to get the 5th edition textbook cover).

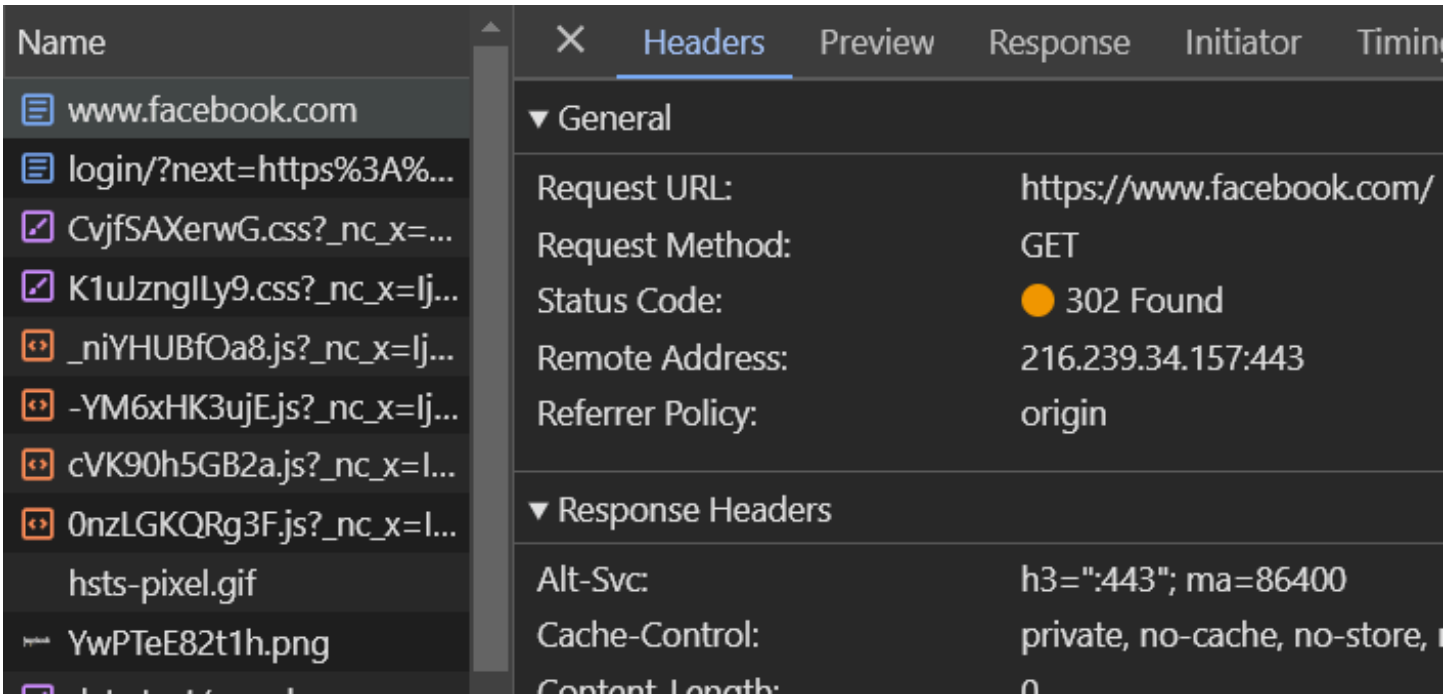
17. Can you tell whether your browser downloaded the two images serially, or whether they

were downloaded from the two web sites in parallel?

Ans: The downloads occurred in parallel. Note that the two GET messages for the images are in packets 17 and 20. The 200OK reply containing the images show up as packets 25, and 54. Thus the request for the second image file (packet 20) was made BEFORE packet 25, the first image file was received.

18. hat is the server's response (status code and phrase) in response to the initial HTTP

GET message from your browser?
Answer:


Name
www.facebook.com
login/?next=https%3A%...
CvjfSAXerwG.css?_nc_x=...
K1uJzngILy9.css?_nc_x=Ij...
_niYHUBfOa8.js?_nc_x=Ij...
-YM6xHK3ujE.js?_nc_x=Ij...
cVK90h5GB2a.js?_nc_x=I...
0nzLGKQRg3F.js?_nc_x=I...
hsts-pixel.gif
YwPTeE82t1h.png
Headers
Preview
Response
Initiator
Timing
General
Request URL:
https://www.facebook.com/
Request Method:
GET
Status Code:
302 Found
Remote Address:
216.239.34.157:443
Referrer Policy:
origin
Response Headers
Alt-Svc:
h3=":443"; ma=86400
Cache-Control:
private, no-cache, no-store,