

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

Debugger Network Style Editor Performance Memory Storage Accessibility Application

	File	Initiator	Type	Transferred	Size	
prod.ads.p...	ydUu3ZjEx4-B5Lufmypi0NqdfuZh3doEVs2ffQNVk=.10324.jpg	activity-stream.bundle.j...	jpeg	NS_BINDING_ABORTED	10.32 kB	
prod.ads.p...	CAP5k4gWqcBGwir7bEEEmBWveLMtvdFu-y_kyO3txFA=.9991.jpg	activity-stream.bundle.j...	jpeg	NS_BINDING_ABORTED	9.99 kB	
pocket.cdn....	https://s3.us-east-1.amazonaws.com/pocket-curatedcorpusapi-prc	lazy-imageset	jpeg	13.93 kB	12.83 kB	
pocket.cdn....	https://s3.us-east-1.amazonaws.com/pocket-curatedcorpusapi-prc	lazy-imageset	jpeg	14.08 kB	12.97 kB	
pocket.cdn....	https://s3.us-east-1.amazonaws.com/pocket-curatedcorpusapi-prc	lazy-imageset	jpeg	17.78 kB	16.68 kB	

Headers Cookies Request Response Timings

Filter Headers

GET https://img-getpocket.cdn.mozilla.net/404x202/filters:format(jpe0/https%3A%2F%2Fs3.us-east-1.amazonaws.com%2Fpocket-curated69d-9246-49af-b5c2-e1630f420e87.png

Status 200

Version HTTP/2

Transferred 17.78 kB (16.68 kB size)

Referrer Policy strict-origin-when-cross-origin

Request Priority Low

DNS Resolution System

Response Headers (1.109 kB)

access-control-allow-origin: *

age: 70938

alt-svc: clear

cache-control: max-age=3600,public,public

content-length: 16675

content-security-policy: default-src 'none'; img-src 'self'; script-srne'

content-type: image/jpeg

date: Sat, 17 Aug 2024 21:40:40 GMT

etag: "36cd7cbc7667e9d3790639089600d21fd9b1e42f"

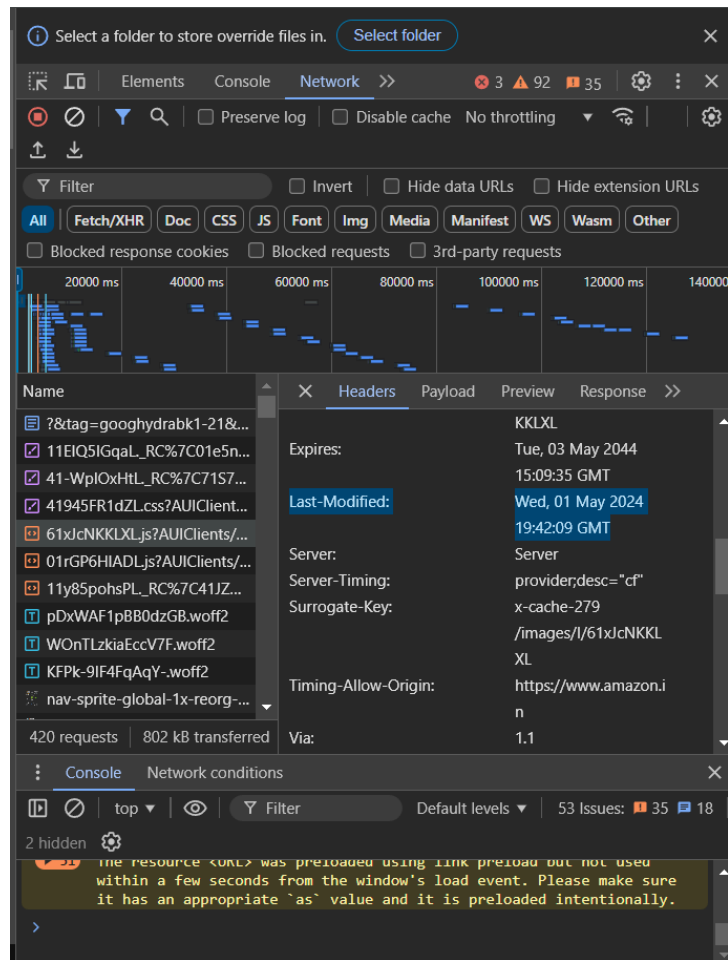
server: nginx

strict-transport-security: max-age=63072000; includeSubdomain

kB transferred Finish: 706 ms load: 302 ms

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:

Name	×	Headers	Preview	Response	Initiator	Timing
ST-1.50.15980821.html		Age:		515047		
PFF-1-186-116._SY116_CB6...		Alt-Svc:		h3=":443";		
DAsf-1.50.dcad56b6.js?csm_...				ma=86400		
PFF-3-186-116._SY116_CB6...		Cache-Control:		max-		
PFF-2-186-116._SY116_CB6...				age=630720000,publi		
PFF-4-186-116._SY116_CB6...				c		
41jc30L1jyL_AC_SY145_.jpg		Content-Length:		3955		
61P8rRWzXUL_AC_SY145_.j...		Content-Type:		image/jpeg		
61fgJs4zlqL_AC_SY145_.jpg		Date:		Sat, 17 Aug 2024		
71-z6ji5R+L_AC_SY145_.jpg				19:49:33 GMT		
suggestions		Edge-Cache-Tag:		x-cache-		
DeskCC-379x304 V2 NS. S...				165,/images/G/31/im		
398 requests				g22/Fashion/Gateway		
217 kB transferred						

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.

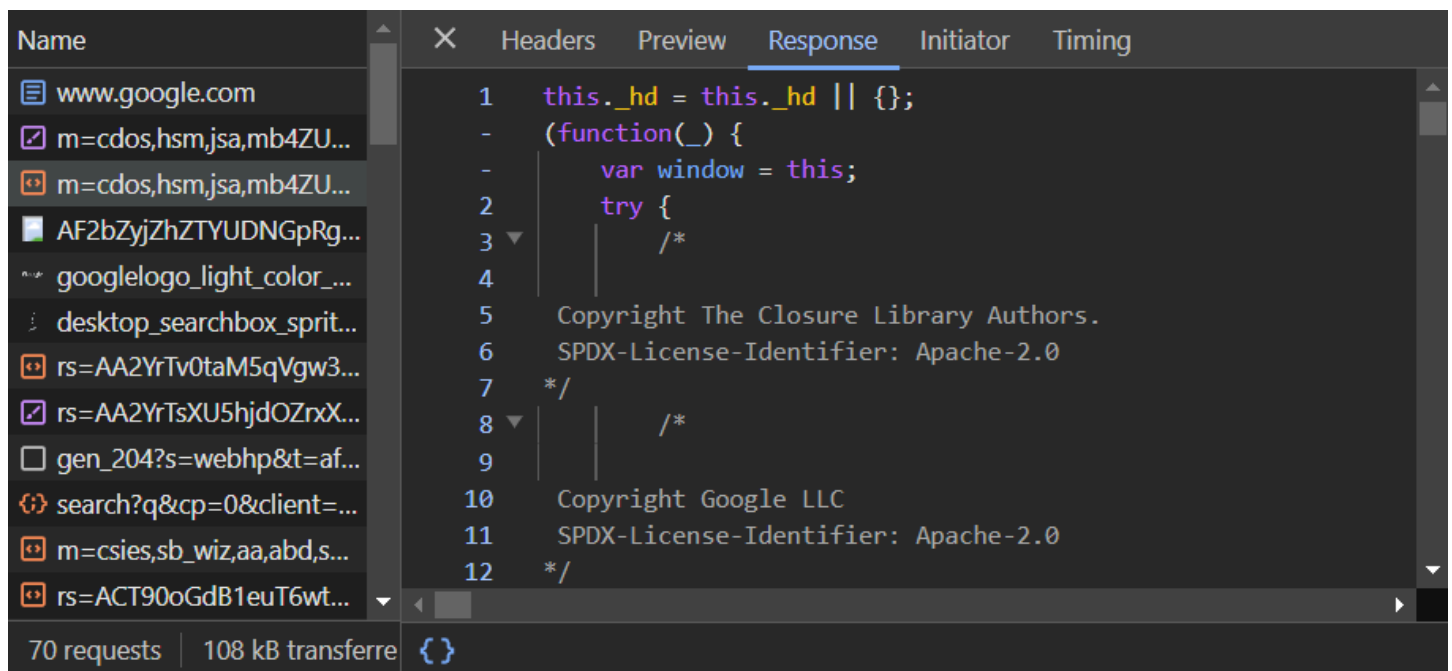
8. Inspect the contents of the first HTTP GET request from your browser to the server.

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:



Content-Type: text/javascript; charset=UTF-8

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

Answer:

Name	×	Headers	Preview	Response	Initiator	Timing
www.facebook.com	▼	General				
login/?next=https%3A%...		Request URL:		https://www.facebook.com/		
CvjfSAXerwG.css?_nc_x=...		Request Method:		GET		
K1uJznglLy9.css?_nc_x=lj...		Status Code:		● 302 Found		
_niYHUBfOa8.js?_nc_x=lj...		Remote Address:		216.239.34.157:443		
-YM6xHK3ujE.js?_nc_x=lj...		Referrer Policy:		origin		
cVK90h5GB2a.js?_nc_x=l...		▼ Response Headers				
0nzLGKQRg3F.js?_nc_x=l...		Alt-Svc:		h3=":443"; ma=86400		
hsts-pixel.gif		Cache-Control:		private, no-cache, no-store,		
YwPTeE82t1h.png		Content-Length:		0		