

CS 331: Computer Networks

Assignment 1

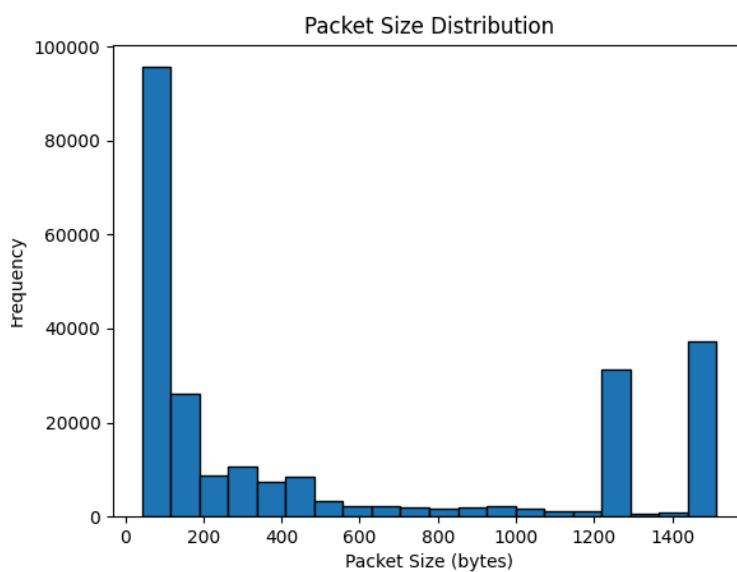
Pranav Patil - 22110199

The codes used to obtain the results are provided on
https://github.com/imPranav14/cs331_assignment1

Part 1: Metrics and Plots

1. Find the total amount of data transferred (in bytes), the total number of packets transferred, and the minimum, maximum, and average packet sizes. Also, show the distribution of packet sizes (e.g., by plotting a histogram of packet sizes).

--- Packet Statistics ---
Total Packets Transferred: 246519
Total Data Transferred: 134996148 bytes
Min Packet Size: 42 bytes
Max Packet Size: 1514 bytes
Average Packet Size: 547.61 bytes



2. Find unique source-destination pairs (source IP:port and destination IP:port) in the captured data.

Total Unique Source-Destination Pairs Found: 9615

3. Display a dictionary where the key is the IP address and the value is the total flows for that IP address as the source. Similarly display a dictionary where the key is the IP address and the value is the total flows for that IP address as the destination. Find out which source-destination (source IP:port and destination IP:port) have transferred the most data.

```
--- Source-Destination with Most Data Transferred ---  
Source-Destination Pair: ('23.52.40.154', 443, '10.240.0.249', 59231)  
Total Data Transferred: 19798738 bytes
```

```
--- Flow with Most Data Transferred ---  
Source: 0.40.236.254:N/A -> Destination: 64.0.128.6:N/A  
Total Bytes Transferred: 197520 bytes
```

4. List the top speed in terms of 'pps' and 'mbps' that your program is able to capture the content without any loss of data when i) running both tcpreplay and your program on the same machine (VM), and ii) when running on different machines: Two student group should run the program on two different machines eg. tcpreplay on physical-machine of student1 and sniffer program physical-machine of student2. Single students should run between two VMs.

Top speed 1500 pps or 6.57 Mbps

```
Actual: 246519 packets (134996148 bytes) sent in 164.34 seconds  
Rated: 821417.5 Bps, 6.57 Mbps, 1500.00 pps  
Flows: 9631 flows, 58.60 fps, 208120 unique flow packets, 38397 unique non-flow packets  
Statistics for network device: lo0  
  Successful packets:      246519  
  Failed packets:         0  
  Truncated packets:      0  
  Retried packets (ENOBUFS): 0  
  Retried packets (EAGAIN): 0
```

Part 2: Catch Me If You Can

1. In a TCP Packet captured, the ACK and PSH flag is set and the sum of source and destination ports value =60303. Find the IP Address of the source and destination.

Total number of matching TCP packets: Zero

2. Find the number of TCP Packets which satisfy all the following conditions.

- a. The SYN flag is set.
 - b. Source Port number is divisible by 11.
 - c. Sequence Number(raw) > 100000
- Give their source and destination IP Addresses.

Total number of matching TCP packets: 223

3. Find the number of TCP Packets with source IP of form 18.234.xx.xxx. The source port number is a prime number and the destination port number is divisible by 11.

Total number of matching TCP packets: 11

4. The sum of the raw Sequence number and Acknowledgement number for a TCP packet is 2512800625. The last two digits of the checksum is 70 (it is of the form 0x____70, hexa decimal representation). Find the packet.

Total number of matching TCP packet: 1

```
Matching TCP Packet Found:
Source IP: 10.240.8.31
Destination IP: 10.7.11.235
Sequence Number: 1376971233
Acknowledgment Number: 1135829392
Checksum (hex): 0xe670
```

Part 3: Capture the packets

1. Run the Wireshark tool and capture the trace of the network packets on your host device. We expect you would be connected to the Internet and perform regular network activities.

I ran the Wireshark to capture the packets over the IITGN-SSO WIFI.

- a. List at-least 5 different application layer protocols that we have not discussed so far in the classroom and describe in 1-2 sentences the operation/usage of protocol and its layer of operation and indicate the associated RFC number if any.

1. DNS (Domain Name System)

- **Operation/Usage:** Resolves human-readable domain names (e.g., www.example.com) into IP addresses, enabling users to access resources on the internet.
- **RFC:** RFC 1035

2. NTP (Network Time Protocol)

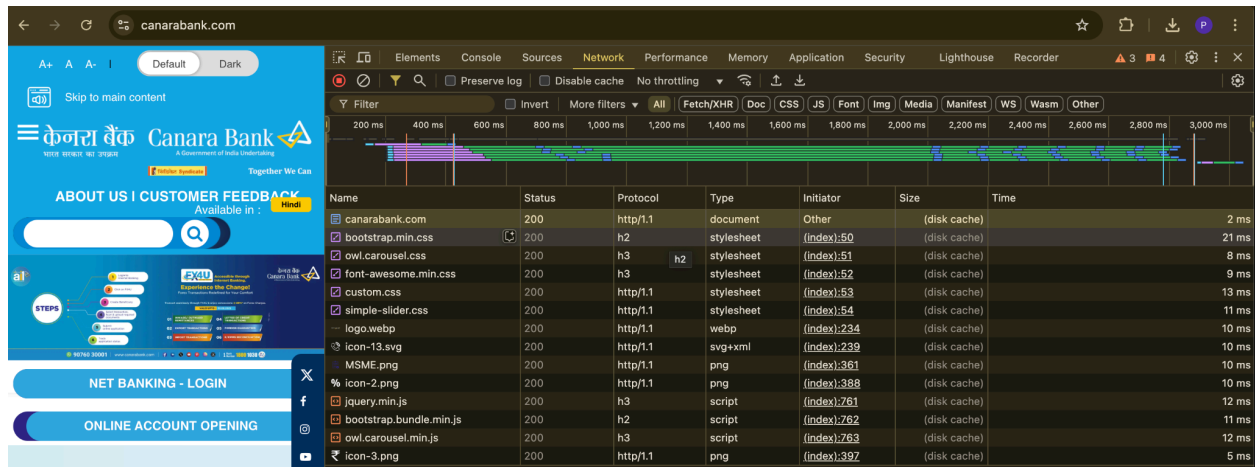
- **Operation/Usage:** Synchronizes the clocks of computers and devices over a network, ensuring accurate timekeeping for logging, authentication, and coordination.
- **RFC:** RFC 5905
- 3. **SNMP (Simple Network Management Protocol)**
 - **Operation/Usage:** Used for managing and monitoring network devices (e.g., routers, switches) by collecting information, configuring devices, and detecting faults.
 - **RFC:** RFC 1157 (SNMPv1), RFC 3411 (SNMPv3)
- 4. **LDAP (Lightweight Directory Access Protocol)**
 - **Operation/Usage:** Provides access to directory services (e.g., user authentication, directory lookups) in systems like Microsoft Active Directory.
 - **RFC:** RFC 4511 (LDAPv3)
- 5. **TFTP (Trivial File Transfer Protocol)**
 - **Operation/Usage:** A simple file transfer protocol used for transferring files between devices, often for booting diskless workstations or updating firmware.
 - **RFC:** RFC 1350
- 6. **SIP (Session Initiation Protocol)**
 - **Operation/Usage:** Used for initiating, maintaining, modifying, and terminating real-time sessions (e.g., voice and video calls) over IP networks, commonly in VoIP systems.
 - **RFC:** RFC 3261

2. Analyze the following details by visiting the following websites in your favourite browser

I have used Google Chrome for the analysis.

a. Identify `request line` with the version of the application layer protocol and the IP address. Also, identify whether the connection(s) is/are persistent or not.

i) canarabank.com



Name	Headers	Preview	Response	Initiator	Timing
canarabank.com	General				
bootstrap.min.css	Request URL: https://canarabank.com/ Request Method: GET Status Code: 200 OK (from disk cache) Remote Address: 107.162.160.8:443 Referrer Policy: strict-origin-when-cross-origin				
owl.carousel.css					
font-awesome.min.css					
custom.css					
simple-slider.css					
logo.webp					

Request Line: GET / HTTP/1.1

IP Address: 107.162.160.8

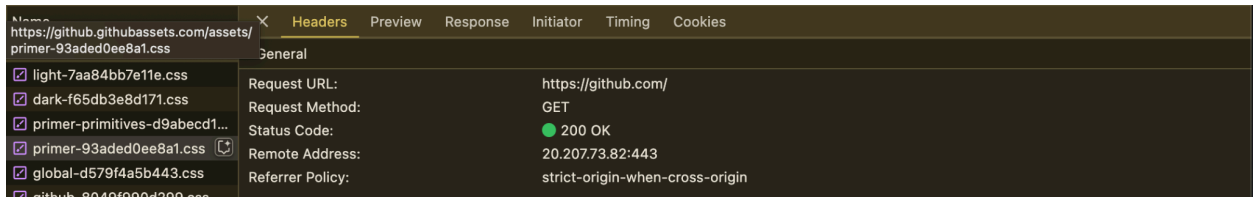
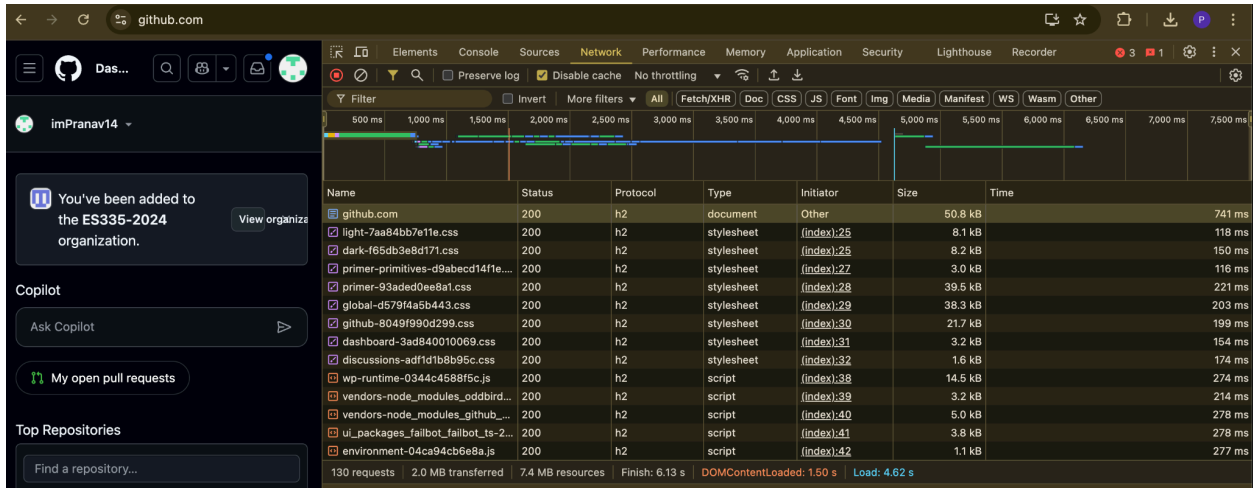
Port: 443

Response Headers	Raw
Cache-Control:	public, max-age=36000
Content-Security-Policy:	default-src data: https; img-src 'self' data: https; style-src 'self' 'unsafe-inline' fonts.googleapis.com stackpath.bootstrapcdn.com cdnjs.cloudflare.com cdn.jsdelivr.net; script-src 'self' cdnjs.cloudflare.com cdn.jsdelivr.net www.googletagmanager.com code.highcharts.com cabprod.gupshup.io 'unsafe-inline' 'unsafe-eval';
Content-Type:	text/html; charset=utf-8
Date:	Sat, 01 Feb 2025 13:42:03 GMT

Request Headers	Raw
Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-GB,en-US;q=0.9,en;q=0.8,hi;q=0.7
Cache-Control:	no-cache
Connection:	keep-alive

Connection: keep-alive (Persistent) in request, close (Not Persistent) in response

ii. Github.com



Request Line: GET / HTTP/2 (h2 type)

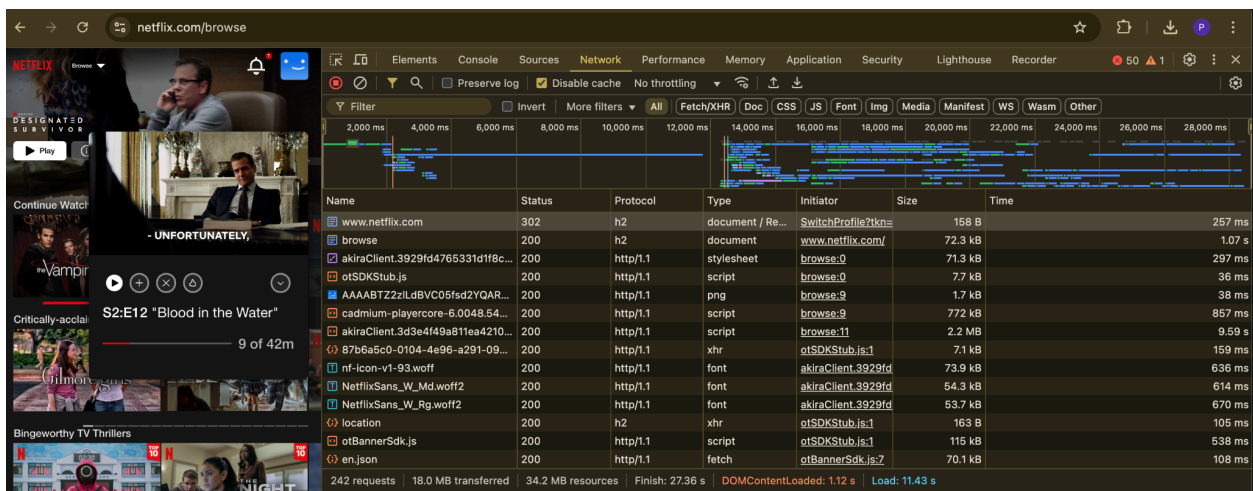
IP Address: 20.207.73.82

Port: 443

Connection: Persistent*

* Websites with Protocol as H2 (HTTP/2) have connection type as Persistent by Design.

iii. netflix.com



Name	Headers	Preview	Response	Initiator	Timing	Cookies
www.netflix.com	General					
browse	Request URL:	https://www.netflix.com/	GET			
akiraClient.3929fd4	Request Method:	GET				
otSDKStub.js	Status Code:	302 Found				
AAAABTZ2zlLdBVC05fsd2Y...	Remote Address:	54.170.196.176:443				
cadmium-playercore-6.004...	Referrer Policy:	strict-origin-when-cross-origin				
akiraClient.3d3e4f49a811ea...						

Request Line: GET / HTTP/2 (h2 type)

IP Address: 54.170.196.176

Port: 443

Connection: Persistent*

* Websites with Protocol as H2 (HTTP/2) have connection type as Persistent by Design.

b. For any one of the websites, list any three header field names and corresponding values in the request and response message.

Response Headers:

Response Headers	Raw
Cache-Control:	public, max-age=36000
Content-Security-Policy:	default-src data: https;; img-src * 'self' data: https;; style-src 'self' 'unsafe-inline' fonts.googleapis.com stackpath.bootstrapcdn.com cdnjs.cloudflare.com cdn.jsdelivrivr.net; script-src 'self' cdnjs.cloudflare.com cdn.jsdelivrivr.net www.googletagmanager.com code.highcharts.com cabprod.gupshup.io 'unsafe-inline' 'unsafe-eval';
Content-Type:	text/html; charset=utf-8
Date:	Sat, 01 Feb 2025 14:06:39 GMT
Referrer-Policy:	no-referrer-when-downgrade
Set-Cookie:	NSC_10.14.241.15_TTM=ffffff0906ef1545525d5f4f58455e445a4a4216cb; expires=Sat, 01-Feb-2025 14:39:06 GMT; path=/; secure; httponly
Set-Cookie:	TS019d7cd7=01f1d06fc3f9b71af52f91b11de141677b9bfadda55595273266925d5b0c604a8252fb5f4799240b20ec358cf8a4b9ff074c03d6d2; Path=/; Secure; HTTPOnly
Set-Cookie:	TSbefe164a027=082eb9432aab20001157263a2ac4c287e5935f052b9dc8a8b8bdfd74b84122a1ae3394fefaec5e0f08f7e0836d1130003c9052d3006e73bea30c009b7e9f5be67ba2d3535103e4d68efd1f9749f8108623894768d0913ba3010b3e674844ff07; Path=/
Strict-Transport-Security:	max-age=31536000; includeSubDomains; preload
Transfer-Encoding:	chunked

Cache-control: public, max-age=36000

Content-security-policy: default-src data: https;; img-src * 'self' data: https;; style-src 'self' 'unsafe-inline' fonts.googleapis.com stackpath.bootstrapcdn.com cdnjs.cloudflare.com cdn.jsdelivrivr.net; script-src 'self' cdnjs.cloudflare.com cdn.jsdelivrivr.net www.googletagmanager.com code.highcharts.com cabprod.gupshup.io 'unsafe-inline' 'unsafe-eval';

Content-type: text/html; charset=utf-8

Request Headers:

▼ Request Headers <input type="checkbox"/> Raw	
Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-GB,en-US;q=0.9,en;q=0.8,hi;q=0.7
Cache-Control:	no-cache
Connection:	keep-alive
Cookie:	NSC_10.14.241.15_TTM=ffffffff0906ef1545525d5f4f58455e445a4a4216cb; cook-parent=1; TS019d7cd7=01f1d06fc3f9b71af52f91b11de141677b9bfadda55595273266925d5b0c604a8252fb5f4799240b20ec358cf8a4b9ff074c03d6d2; TSbefe164a027=082eb9432aab2000bee3f80f23d278d3b5a0f9d4a6ce446021041ababc39f865622b8769c320b59308e86206f81130003ae579d421203141c57ec692ed53b5c6f9442a3fc19d4c935912c80383d67a375f298688550491178ec6d50f0d9edd2b
Host:	canarabank.com
Pragma:	no-cache

accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

accept-encoding: gzip, deflate, br, zstd

accept-language: en-GB,en-US;q=0.9,en;q=0.8,hi;q=0.7

cache-control: no-cache




connection: keep-alive

b. Any three HTTP error codes obtained while loading one of the pages with a brief description.

1. Error code 302

The HTTP 302 status code is a redirection status code. It indicates that the requested resource has been temporarily moved to a different URI (Uniform Resource Identifier).

The client (e.g., the browser) is expected to make a new request to the URI provided in the Location header of the response.

Name	Status	Protocol	Type	Initiator	Size	Time
 www.netflix.com	302	h2	document / Re...	Other	1.3 kB	1.36 s
 browse	200	h2	document	www.netflix.com/	46.8 kB	1.27 s
 akiraClient.3929fd4765331d1f8c...	200	http/1.1	stylesheet	browser:0	71.3 kB	178 ms
 otSDKStub.js	200	http/1.1	script	browser:0	7.7 kB	1.21 s

2. Error code 404

The HTTP 404 status code is a client error code. It indicates that the server cannot find the requested resource. This is one of the most common error codes encountered on the web.

Name	Status	Protocol	Type	Initiator	Size	Time
cs331computernetworks	404	h2	document	Other	127 kB	1.14 s
mona-sans-d1bf285e9b9...	200	h2	font	cs331computer	84.6 kB	1.06 s
light-7aa84bb7e11e.css	200	h2	stylesheet	cs331computer	8.3 kB	354 ms

3. Error code 307

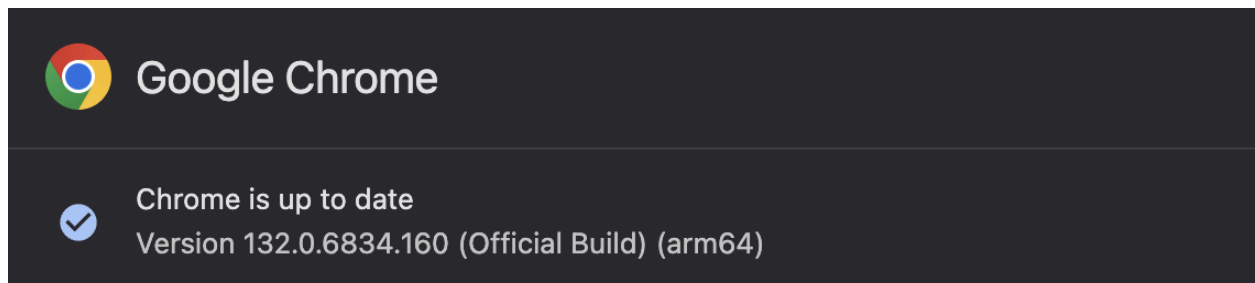
The 307 status code indicates that the requested resource has been temporarily moved to a different URI. The client should repeat the request to the new URL provided in the response's location header.

Name	Status	Protocol	Type	Initiator	Size	Time
gtm.js?id=GTM-T...	307	http/1.1	script / ...	Search?out	0 B	18 ms
internal-banner.w...	200	http/1.1	webp	Search?out	1.5 kB	259 ms
jquery.min.js	200	h3	script	Search?out	28.1 kB	230 ms

C) Capture the Performance metrics that your browser records when a page is loaded and also report the list the cookies used and the associated flags in the request and response headers. Please report the browser name and screenshot of the performance metrics reported for any one of the page loads.

1. Browser Details

Google Chrome 132.0.6834.160 (Official Build) (arm64)



2. Request details

Request URL: <https://www.netflix.com/>

Method: GET

Headers:

- Accept: text/html, application/xml, image/*
- Accept-Encoding: : gzip, deflate, br, zstd
- User-Agent: Mozilla/5.0 (Linux; Android 11; Surface Duo) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
- Sec-Ch-Ua-Platform: "macOS"
- Cookies include session ID, login status (logged_in=yes), and preferred theme (dark).

```
▼ Request Headers
:authority:                github.com
:method:                   GET
:path:                     /
:scheme:                   https
Accept:                    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding:           gzip, deflate, br, zstd
Accept-Language:           en-GB,en-US;q=0.9,en;q=0.8,hi;q=0.7
Cache-Control:             no-cache
Cookie:                    _device_id=2fbab4b50c01d55e713059ade1856b91; _octo=GH1.1.1312290437.1708890681;
                           GHCC=Required:1-Analytics:1-SocialMedia:1-Advertising:1;
                           MicrosoftApplicationsTelemetryDeviceId=3633786c-bd4e-4c2f-b18f-db4d0a5aae1f;
                           MSFPC=GUID=f7797462044f42a991ae73ef1634a42f&HASH=f779&LV=202406&V=4&LU=17183109968
                           39; saved_user_sessions=117572469%3AbhJX0zIHUly72fSgqdM_P3x3J-1AGuw3jJJ9s8pWbRc0XBi7;
                           user_session=bhJX0zIHUly72fSgqdM_P3x3J-1AGuw3jJJ9s8pWbRc0XBi7; __Host-
                           user_session_same_site=bhJX0zIHUly72fSgqdM_P3x3J-1AGuw3jJJ9s8pWbRc0XBi7; logged_in=yes;
                           dotcom_user=imPranav14;
                           color_mode=%7B%22color_mode%22%3A%22auto%22%2C%22light_theme%22%3A%7B%22name%2
                           2%3A%22light%22%2C%22color_mode%22%3A%22light%22%7D%2C%22dark_theme%22%3A%7B%
                           22name%22%3A%22dark%22%2C%22color_mode%22%3A%22dark%22%7D%7D; cpu_bucket=lg;
                           tz=Asia%2FCalcutta; preferred_color_mode=dark;
```

```
Pragma:                    no-cache
Priority:                   u=0, i
Sec-Ch-Ua:                 "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
Sec-Ch-Ua-Mobile:         ?0
Sec-Ch-Ua-Platform:       "macOS"
Sec-Fetch-Dest:           document
Sec-Fetch-Mode:           navigate
Sec-Fetch-Site:           none
Sec-Fetch-User:           ?1
Upgrade-Insecure-Requests: 1
User-Agent:                Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
                           Chrome/132.0.0.0 Safari/537.36
```

3. RESPONSE DETAILS

Content-Type: text/html; charset=utf-8


Content-Encoding: gzip

Cache-Control: max-age=0, private, must-revalidate

Security Headers:

- Strict-Transport-Security: max-age=31536000
- X-Frame-Options: deny
- X-Content-Type-Options: nosni
- X-XSS-Protection: 0
- Content-Security-Policy: Restricts external sources and inline scripts.

▼ Response Headers	
Cache-Control:	max-age=0, private, must-revalidate
Content-Encoding:	gzip
Content-Security-Policy:	default-src 'none'; base-uri 'self'; child-src github.com/assets-cdn/worker/ github.com/webpack/ github.com/assets/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com www.githubstatus.com collector.github.com raw.githubusercontent.com api.github.com github-cloud.s3.amazonaws.com github-production-repository-file-5c1aeb.s3.amazonaws.com github-production-upload-manifest-file-7fdce7.s3.amazonaws.com github-production-user-asset-6210df.s3.amazonaws.com *.rel.tunnels.api.visualstudio.com wss://*.rel.tunnels.api.visualstudio.com objects-origin.githubusercontent.com copilot-proxy.githubusercontent.com proxy.individual.githubcopilot.com proxy.business.githubcopilot.com proxy.enterprise.githubcopilot.com *.actions.githubusercontent.com productionresultssa0.blob.core.windows.net/ productionresultssa1.blob.core.windows.net/ productionresultssa2.blob.core.windows.net/ productionresultssa3.blob.core.windows.net/ productionresultssa4.blob.core.windows.net/ productionresultssa5.blob.core.windows.net/ productionresultssa6.blob.core.windows.net/ productionresultssa7.blob.core.windows.net/ productionresultssa8.blob.core.windows.net/ productionresultssa9.blob.core.windows.net/ productionresultssa10.blob.core.windows.net/ productionresultssa11.blob.core.windows.net/ productionresultssa12.blob.core.windows.net/ productionresultssa13.blob.core.windows.net/ productionresultssa14.blob.core.windows.net/

	inline' github.githubassets.com; upgrade-insecure-requests; worker-src github.com/assets-cdn/worker/ github.com/webpack/ github.com/assets/ gist.github.com/assets-cdn/worker/
Content-Type:	text/html; charset=utf-8
Date:	Sat, 01 Feb 2025 14:19:29 GMT
Etag:	W/"ce519617a87f373d1866453c4209b1b3"
Referrer-Policy:	origin-when-cross-origin, strict-origin-when-cross-origin
Server:	GitHub.com
Set-Cookie:	_gh_sess=RcbboQF6VXLPVM%2B%2B7Jp3ONxJ%2FUBC85xdS5jPSQ9GmNQYKATiDLT6AccdbOelpbf6EQm8Q5GGUiEMH0WDQm%2Fyfr%2B14JThwrhddIH0c5WON3oHJSe9gxzp%2FePxQHA8%2FCfOdeUxA8hQUajKEb43rZK%2FivMgCYdiWqZVwMqdMO1UlnQQA9x8VK4tKE3wIObUsHqLj%2FDhyofkDggmBsUZ61Vax7Iclkm3ivzYPT5PJ5BJ8lixL%2Fm8bnvAfu9RUdznWY0PA%2FWm79ve0VI88FrFFKsGWE9GC3sqHsFs4e9%2B7DSP%2FC4YyHIAcQuDo%2F9cl53pA%2Bnlmj458Mi%2BeGD7uLNinnSAxaVv1lcuYIFEBTnLUGdwfZTrmSqn9%2F9wc2qfthFRtvHolsJVhX%2FtoKicHh60DKmEFMCws%3D--SDA%2FtnanEyJ6aW90--UcqUsDlz649eheEv%2F2Utaw%3D%3D; path=/; secure; HttpOnly; SameSite=Lax
Strict-Transport-Security:	max-age=31536000; includeSubdomains; preload
Vary:	X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame 
Vary:	Accept-Encoding, Accept, X-Requested-With Override header
X-Content-Type-Options:	nosniff
X-Frame-Options:	deny
X-Github-Request-Id:	96A8:0A2C:D01CF5:106851D:679E2D71
X-Xss-Protection:	0

4. Cookies

Key Cookies:

- `_gh_sess` (Session Cookie)
- `logged_in=yes`

- preferred_color_mode=dark
- cpu_bucket=lg
- tz=Asia%2Calcutta

Security Flags: - HttpOnly and Secure are applied to session cookies.

Request Cookies ☐ show filtered out request cookies

Name	Cookies that were sent to the server in the 'cookie' header of the request	Domain	Path	Expires	Size	HttpOnly	Secure	SameSite	Partitioned	CrossSite	Priority
GHCv...	required:1-analytics1-SocialMedia...	.gith...	/	202...	54		✓	Lax			Medi...
MSFPC	GUID=17797462044f42a991ae73ef1...	.gith...	/	202...	83		✓	None			Medi...
MicrosoftApplicationsTel...	3633786c-bd4e-4c2f-b18f-db4d0a...	.gith...	/	202...	74		✓	None			Medi...
__Host-user_session_sa...	bhJX0zIHUly72fSgqgDM_P3x3J-1AG...	.gith...	/	202...	77	✓	✓	Strict			Medi...
__device_id	2fbab4b50c01d55e713059ade1856...	.gith...	/	202...	42	✓	✓	Lax			Medi...
_gh_sess	7G%2Fzvw0MTUoFwysbBw4e6op8...	.gith...	/	Sess...	498	✓	✓	Lax			Medi...
_octo	GH1.1.1312290437.1708890681	.gith...	/	202...	32		✓	Lax			Medi...
color_mode	%7B%22color_mode%22%3A%22a...	.gith...	/	Sess...	214		✓	Lax			Medi...
cpu_bucket	lg	.gith...	/	Sess...	12		✓	Lax			Medi...
dotcom_user	imPranav14	.gith...	/	202...	21	✓	✓	Lax			Medi...
logged_in	yes	.gith...	/	202...	12	✓	✓	Lax			Medi...
preferred_color_mode	dark	.gith...	/	Sess...	24		✓	Lax			Medi...
saved_user_sessions	117572469%3AbhJX0zIHUly72fSgq...	.gith...	/	202...	79	✓	✓	Lax			Medi...
tz	Asia%2FCalcutta	.gith...	/	Sess...	17		✓	Lax			Medi...
user_session	bhJX0zIHUly72fSgqgDM_P3x3J-1AG...	.gith...	/	202...	60	✓	✓	Lax			Medi...