CS 331: Computer Networks Assignment 1 SubmissionDate: Before 01-02-2025, 11:59pm

ASSIGNMENT 1

Team ID = 8
Nakul Ranka 24120035
Saumya Jaiswal 21110186

PCAP file selection: 8.pcap
Github Repo Link : https://github.com/nikuCollege/CN-Assignment1

Part 1: Metrics and Plots

All the results for the metrics and plot are compiled in the github repo as “Output.txt” file.

1. Total Packets: 328623
   Total Data Transferred: 324313533 bytes
   Min Packet Size: 42 bytes
   Max Packet Size: 1514 bytes
   Avg Packet Size: 986.886 bytes
2. All the unique pairs are listed in “Output.txt”.
3. Dictionary for the source and destination flows is in “Output.txt” in repository.
   Source-Destination Pair with Most Data Transferred
   - 180.149.61.76:443 -> 10.7.11.235:63908 : 64799744 bytes
4.
   - Packets per second (pps): 1886.23
   - Megabits per second (Mbps): 14.892

Part 2: Catch Me If You Can

Answers for these Extra Questions have also been included in Output.txt file.

Q 1]
The absolute difference of the Source port and Destination port value is given as 54286, The ACK flag is set, and the last 4 digits of the Acknowledgement number is ‘1203’. Find the Source IP and Destination IP.

Ans]
- Source IP: 10.7.11.235, Destination IP: 180.149.59.137, Source Port: 54729, Destination Port: 443, ACK Number: 0xb35e23c3

Q 2]
The first two digits of the checksum is 'b5' (it is of the form 0xb5___, hexadecimal notation), the urgent data pointer is set to 0 and the 4 four digits of Raw Sequence Number is '6183'. Find the source IP, destination IP and the complete checksum of this packet.

Ans] - Source IP: 23.54.155.211, Destination IP: 10.7.11.235, Checksum: 0xb55a

Q 3]
Tell the number of packets where the sum of source and destination ports is between 10,000 and 20,000.

Ans] 69 packets

Q 4]
Find all such packets whose acknowledgement number (raw) is in between 1678999000 <= ack_number <= 1700000000.

Ans] Included in Output.txt file in repo under "[Condition 4: Matching IPs Based on ACK Number Range]"

Part 3: Capture the packets

1. **a] List at-least 5 different application layer protocols.**

   Attached is the "***protocols.pcap*"** file, which captures all the below-mentioned protocols.
   protocols.pcap

   i) SMTP (Simple Mail Transfer Protocol):

- SMTP is an application layer protocol used for sending email between servers. It facilitates the transmission of email messages from the sender's mail server to the recipient's mail server, operating over TCP port 25, 587, or 465 (for secure connections). SMTP allows mail servers to relay emails to each other in a client-server manner.
- Operates at the Application Layer (Layer 7) of the OSI model.
- **RFC 5321.**

- Generated SMTP traffic by initiating a connection to an SMTP server OpenSSL: *openssl s_client -starttls smtp -connect smtp.gmail.com:587*

ii) DHCP (Dynamic Host Configuration Protocol):

- DHCP is an application layer protocol used to dynamically assign IP addresses and other network configuration information (like DNS servers) to devices on a network.
- operates at the **Application Layer** (Layer 7) of the OSI model.
- **RFC 2131**.
- generated automatically when a device connects to a network.

iii) SSDP (Simple Service Discovery Protocol):

- SSDP is used to discover devices and services on a local network, typically in UPnP applications like smart devices.
- operates at the **Application Layer** (Layer 7) but uses **UDP** as its transport protocol on **port 1900**.
- **RFC 6766**.

iv) OCSP (Online Certificate Status Protocol):

- it directly interacts with applications to verify the status of digital certificates, typically used in the context of SSL/TLS connections, to determine if a digital certificate has been revoked, providing real-time validation.
- operates over the transport layer (like TCP), the logic and message structure of OCSP itself belongs to the application layer.
- **RFC 6960**

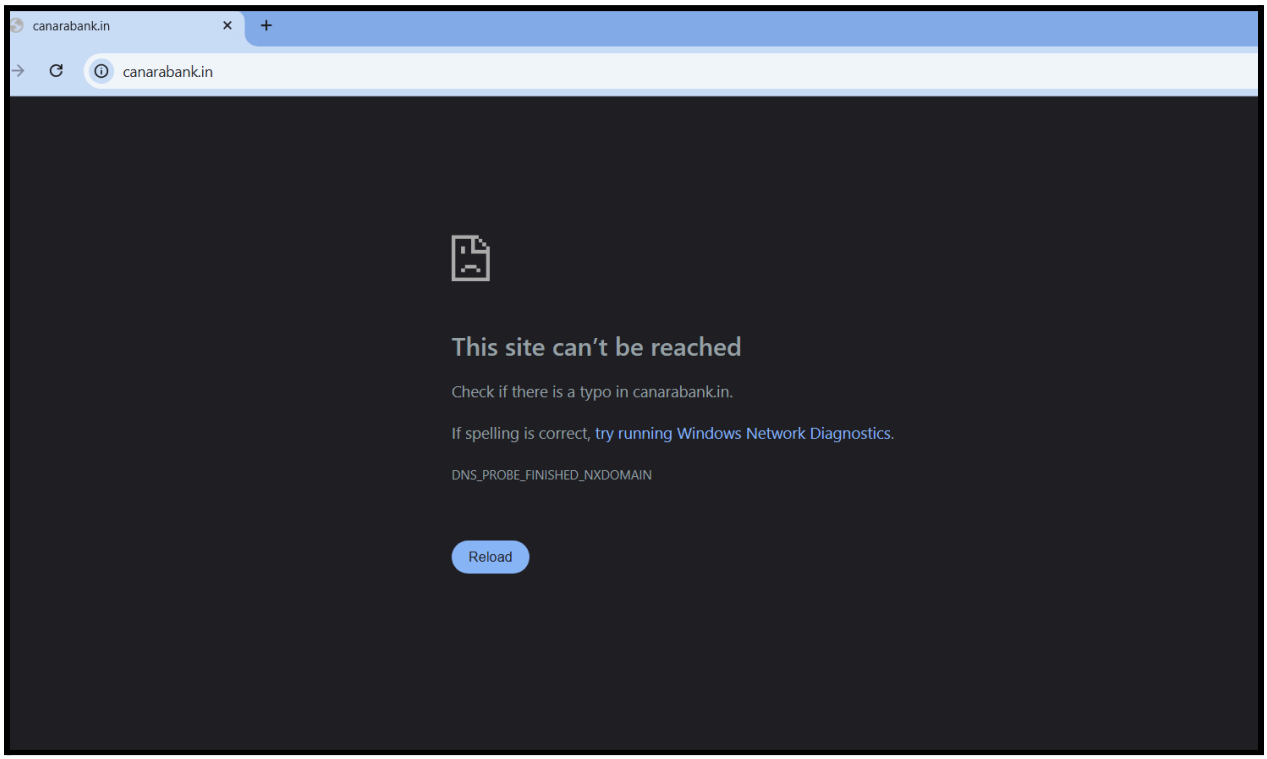
v) mDNS (Multicast DNS):

- used for resolving hostnames to IP addresses within a local network without the need for a centralized DNS server. It operates by using multicast to send DNS-like queries and responses to devices on the local network.
- operates at the **Application Layer** (Layer 7) of the OSI model, but it utilizes **UDP** as the transport protocol on **port 5353**.
- **RFC 6762**.

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

i) canarabank.in

- Received error “DNS_PROBE_FINISHED_NXDOMAIN, it means the browser cannot resolve the domain name “canarabank.in” to an IP address.



a)

- **Request Line:** N/A (Domain does not resolve)
- **Protocol Version:** N/A
- **IP Address:** Not found (DNS resolution failed)
- **Connection Type:** Not established
- **Performance Metrics :** No data available (site unreachable)
- **Cookies :** None (no response received)
- **Browser Used :** Version 132.0.6834.160

Conclusively, the domain canarabank.in is either incorrect, inactive, or does not exist.

ii) github.com

a)

Request Line: https://github.com

Protocol Version: HTTP/2

“ went to console and typed [console.log(window.performance.getEntriesByType("navigation")[0].nextHopProtocol)] , it returned “h2” which means HTTP/2

Request Method: GET

Status Code: 200 OK

IP Address: 20.207.73.82; 443 (port)

Connection Type: Persistent (protocol used HTTP/2 which always uses persistent connections)

b)

Request Headers:

1) **Authority :** github.com
2) **Accept-Encoding:** gzip, deflate, br, zstd
3) **User -Agent :** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36

Response Headers:

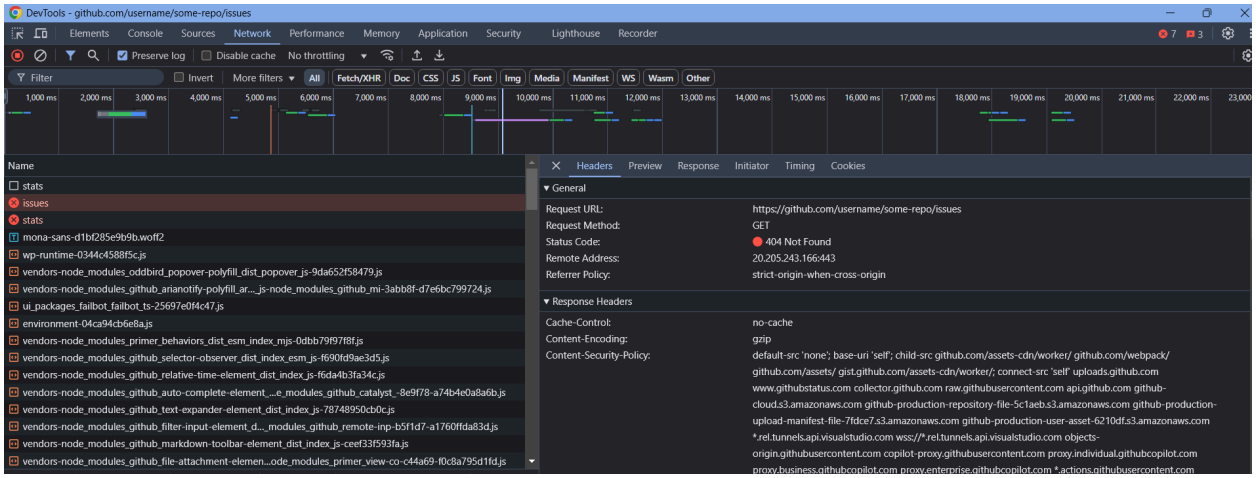
4) **Content-Type:** text/html; charset=utf-8
5) **Server:** GitHub.com
6) **Cache-Control:** max-age=0, private, must-revalidate

HTTP ERROR CODES

1. **404 - Not Found**

   URL : https://github.com/username/some-repo/issues

   This URL points to a non-existent GitHub repository, hence received 404 error.



2. **500 Internal Server Error**
    - If the GitHub server is temporarily unavailable or if there's an issue with their backend, receive 500 error.
3. **502 Bad Gateway**
    - If there's a **gateway** issue, and the server cannot fulfill the request or during peak times or server outages, 502 error is received.

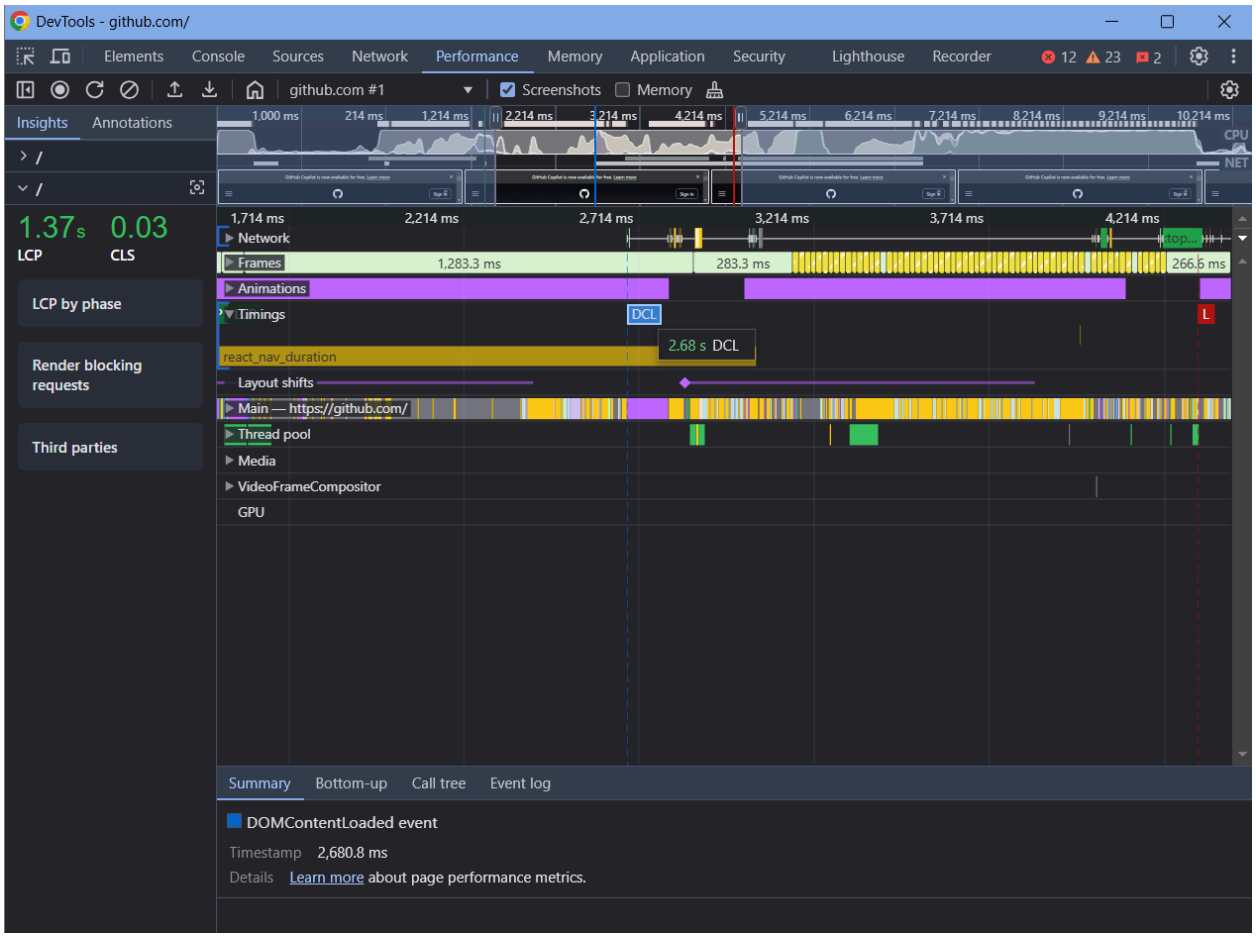
c)

i) **Browser Name** : Google Chrome (Version 132.0.6834.160)

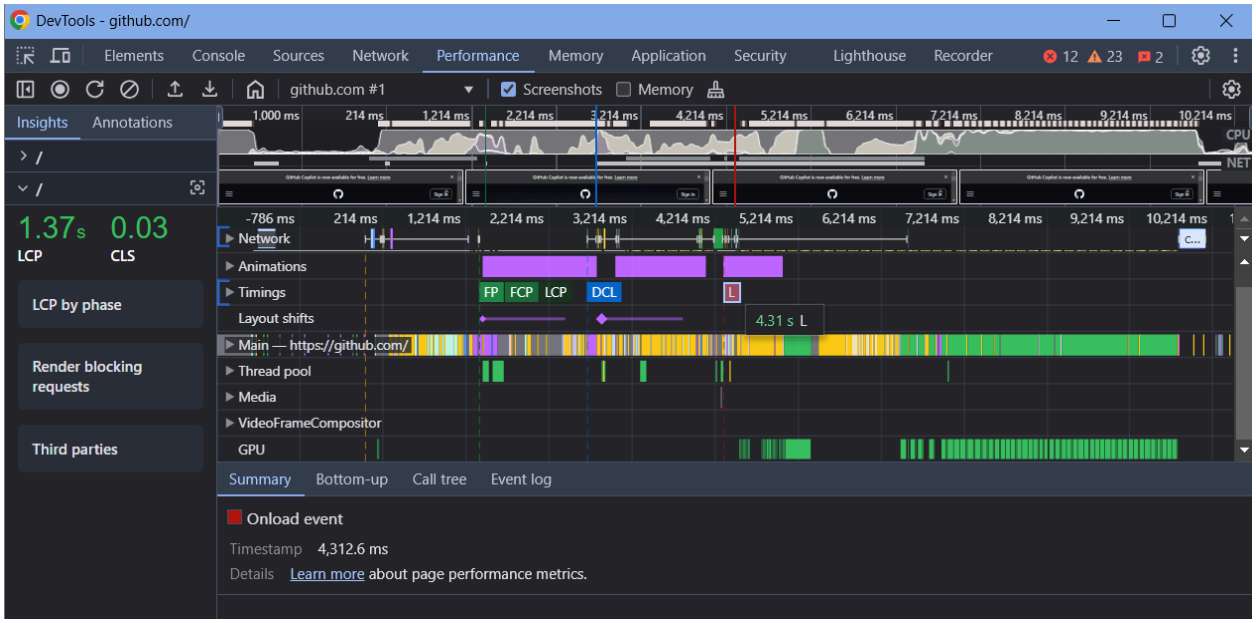
ii) **Page:** hhtps://github.com

Metrics

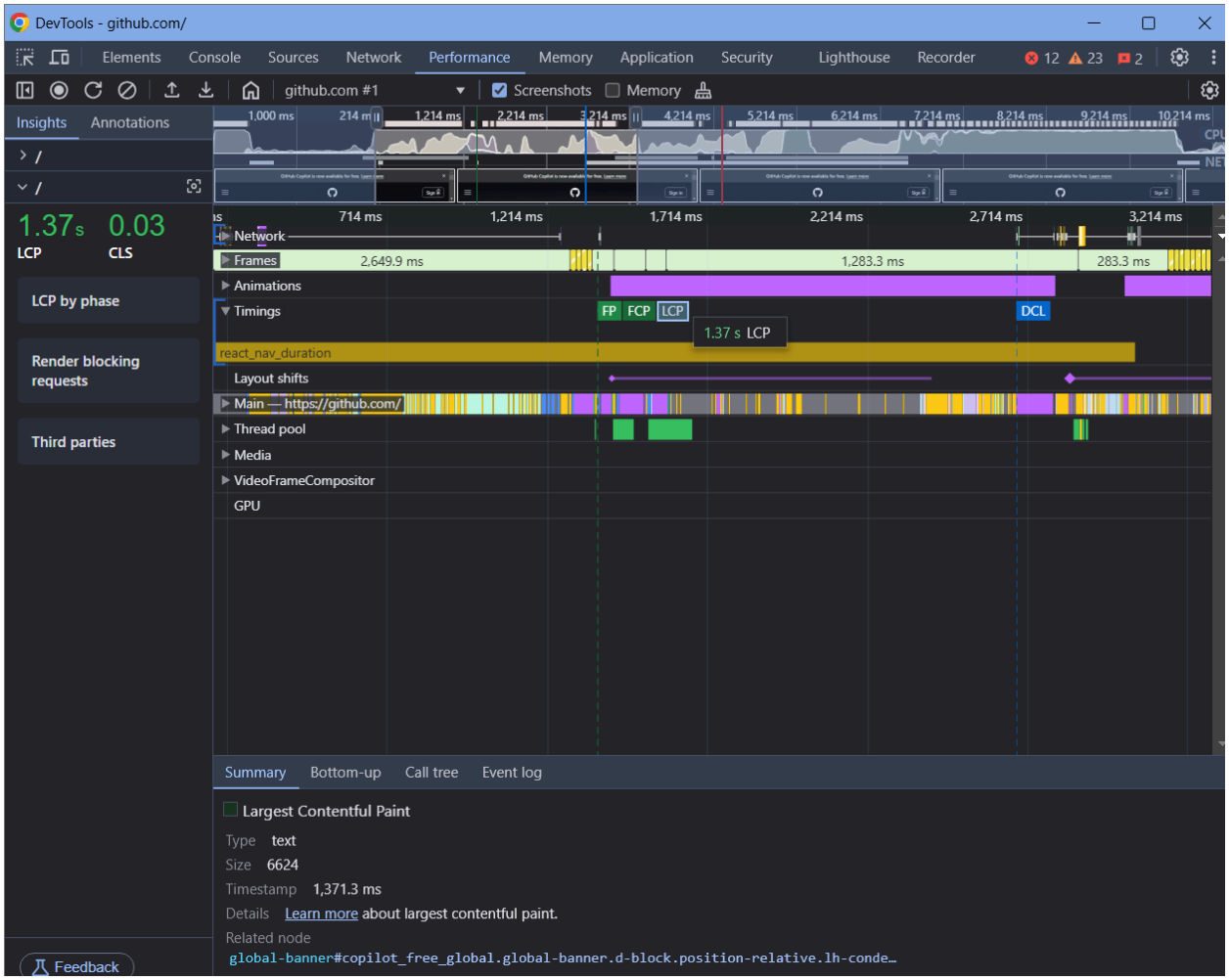
7) DOMContentLoaded: 2.68s



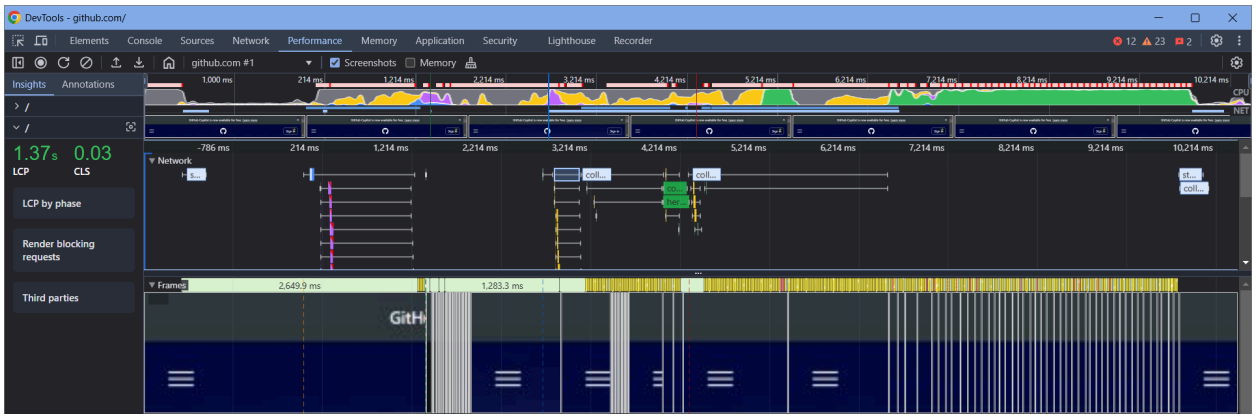
8) Page Load Time: 4.31s



9) Largest Contentful Paint: 1.37s



4)Frames and the Network Requests



COOKIES USED

1. **device_id :** stores a unique identifier for the device that the user is accessing the website from.

2. **gh_sess:** a session identifier cookie, used by GitHub to maintain the user's login session across multiple requests during their visit to the site.

3. **_octo:** for tracking user behavior on the site, such as interactions with GitHub's various features

4. **color_mode:** stores the user's preferred color mode (light or dark) for the UI.

5. **cpu_bucket :** used to allocate resources or set preferences for a particular user based on their CPU performance.

6. **logged_in:** stores information about whether the user is logged into the website or not.

7. **preferred_color_mode:** this cookie stores a user's preference for the theme of the website (dark or light).

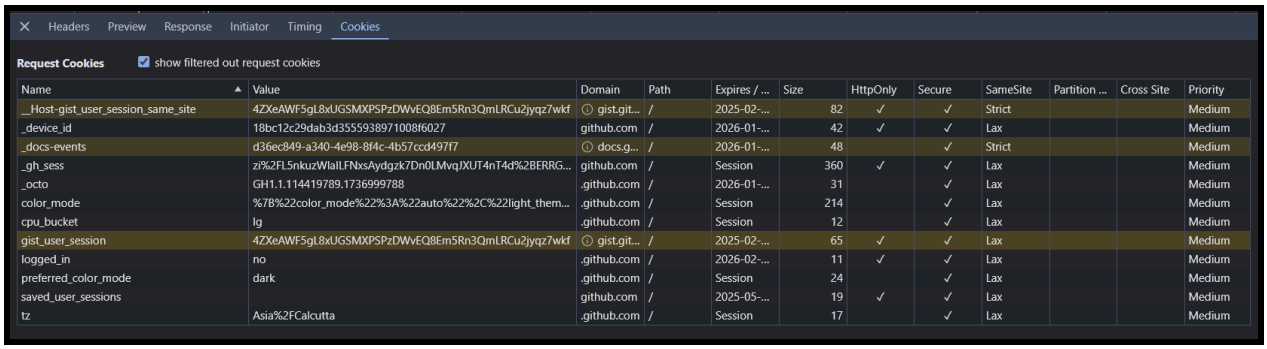
8. **saved_user_sessions**: store information about a user's previous sessions.

9. **tz:** stores the user's timezone.

COOKIE FLAGS:

1. **Http-Only** : ensures that the cookie cannot be accessed or modified via JavaScript running on the client side.
2. **Secure** : ensures that the cookie is only sent over secure (HTTPS) connections, protecting it from being transmitted over an unencrypted connection (HTTP).
3. **SameSite** : restricts how cookies are sent with cross-site requests.
    a. **Strict**: The cookie is only sent to the server if the request is made from the same origin.
    b. **Lax**: The cookie is sent with top-level navigation and GET requests, but not with other types of cross-origin requests.
    c. **None**: The cookie is sent with all requests, including cross-origin requests, but **must also be marked as Secure**.

Screenshot of the Cookies Tab associated with "github.com" website



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Cross Site	Priority
__Host-gist_user_session_same_site	4ZXeAWF5gL8xUGSMXPSPzDWvEQ8Em5Rn3QmLRCu2jyqz7wkf	gist.git...	/	2025-02-...	82	✓	✓	Strict			Medium
_device_id	18bc12c29dab3d35559389710 08f6027	github.com	/	2026-01-...	42	✓	✓	Lax			Medium
_docs-events	d36ec849-a340-4e98-8f4c-4b57ccd497f7	docs.g...	/	2026-01-...	48		✓	Strict			Medium
_gh_sess	zi%2FL5nkuzWlalLFNxsAydgzk7Dn0LMvqJXUT4nT4d%2BERRG...	github.com	/	Session	360	✓	✓	Lax			Medium
_octo	GH1.1.114419789.1736999788	.github.com	/	2026-01-...	31		✓	Lax			Medium
color_mode	%7B%22color_mode%22%3A%22auto%22%2C%22light_them...	.github.com	/	Session	214		✓	Lax			Medium
cpu_bucket	lg	.github.com	/	Session	12		✓	Lax			Medium
gist_user_session	4ZXeAWF5gL8xUGSMXPSPzDWvEQ8Em5Rn3QmLRCu2jyqz7wkf	gist.git...	/	2025-02-...	65	✓	✓	Lax			Medium
logged_in	no	.github.com	/	2026-02-...	11	✓	✓	Lax			Medium
preferred_color_mode	dark	.github.com	/	Session	24		✓	Lax			Medium
saved_user_sessions		github.com	/	2025-05-...	19	✓	✓	Lax			Medium
tz	Asia%2FCalcutta	.github.com	/	Session	17		✓	Lax			Medium

iii) netflix.com

a)

Request Line: https://www.netflix.com/

Protocol Version: HTTP/2

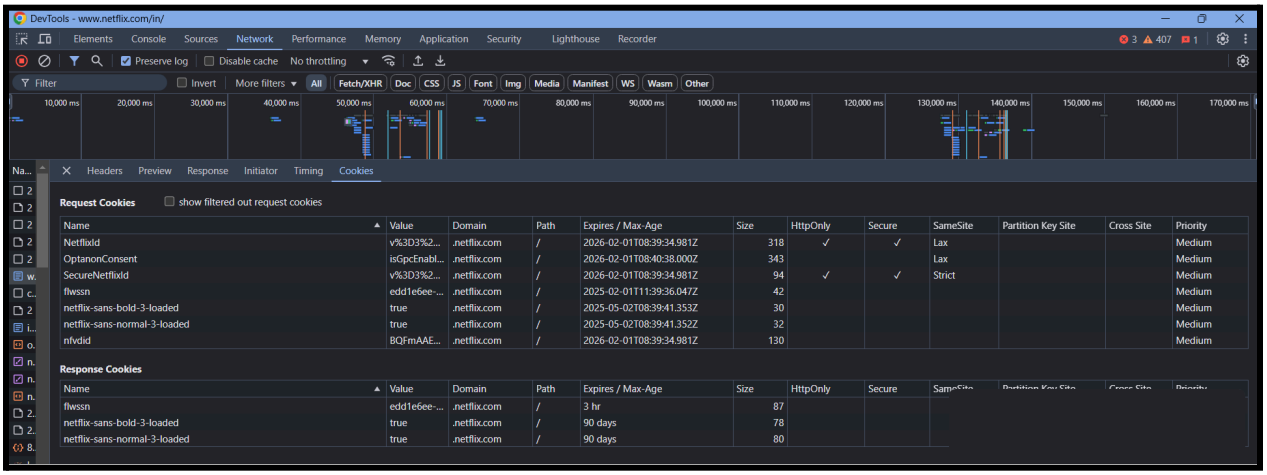
Request Method: GET

Status Code: 302 Found

IP Address: 54.155.246.232; 443 (port)

Connection Type: Persistent (protocol used HTTP/2 which always uses persistent connections)

Cookies and Flags Used -



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Partition Key Site	Cross Site	Priority
NetflixId	v%3D3%2...	.netflix.com	/	2026-02-01T08:39:34.981Z	318	✓	✓	Lax			Medium
OptanonConsent	isGpcEnabl...	.netflix.com	/	2026-02-01T08:40:38.000Z	343			Lax			Medium
SecureNetflixId	v%3D3%2...	.netflix.com	/	2026-02-01T08:39:34.981Z	94	✓	✓	Strict			Medium
flwssn	edd1e6ee-...	.netflix.com	/	2025-02-01T11:39:36.047Z	42						Medium
netflix-sans-bold-3-loaded	true	.netflix.com	/	2025-05-02T08:39:41.353Z	30						Medium
netflix-sans-normal-3-loaded	true	.netflix.com	/	2025-05-02T08:39:41.352Z	32						Medium
nfvdid	BQFmAAE...	.netflix.com	/	2026-02-01T08:39:34.981Z	130						Medium

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure
flwssn	edd1e6ee-...	.netflix.com	/	3 hr	87		
netflix-sans-bold-3-loaded	true	.netflix.com	/	90 days	78		
netflix-sans-normal-3-loaded	true	.netflix.com	/	90 days	80		