CS 331: Computer Networks

Assignment 1

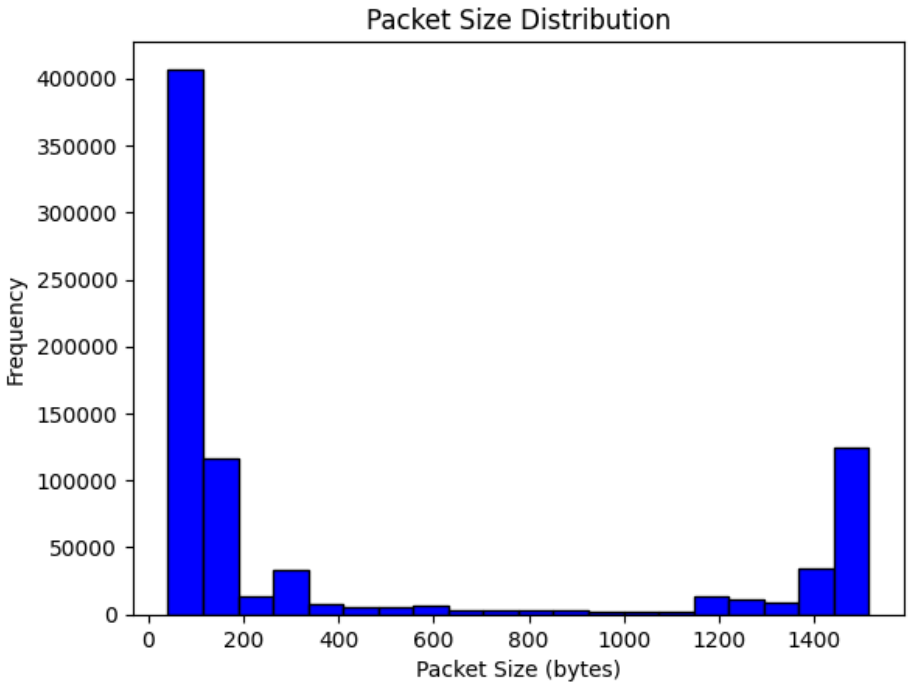
Group No. - 23
Team Members:
Aryan Sahu - 22110038
Dewansh Kumar - 22110071

Part 1: Metrics and Plots

Q1: Basic Metrics

- **File Analyzed:** `5.pcap`
- **Total Data Transferred:** 364,640,811 bytes
- **Total Packets Transferred:** 805,996
- **Minimum Packet Size:** 42 bytes
- **Maximum Packet Size:** 1514 bytes
- **Average Packet Size:** 452.41 bytes

Packet Size Distribution:



Q2: Unique Source-Destination Pairs

- The content of unique source-destination pairs have been save as a text file named unique_flows.txt.

unique_flows.txt

```
172.16.133.55:57079 -> 96.43.146.22:443
23.32.176.63:443 -> 172.16.133.73:59940
172.16.133.25:60425 -> 71.252.224.198:44248
172.16.133.73:59940 -> 23.32.176.63:443
68.64.21.42:1853 -> 172.16.133.36:62603
172.16.133.49:58246 -> 68.64.21.41:1853
8.8.4.4:53 -> 172.16.133.6:51363
172.16.133.153:36599 -> 172.16.128.202:53
68.64.21.41:1853 -> 172.16.133.60:63861
```

Q3: Flow Analysis

Source Flow Dictionary:

- The contents of source flow dictionary are saved as text file named source_flow_count.txt

source_flow_count.txt

```
172.16.133.55 : 66
23.32.176.63 : 9
172.16.133.25 : 105
172.16.133.73 : 117
68.64.21.42 : 106
172.16.133.49 : 132
```

Destination Flow Dictionary:

- The contents of destination flow dictionary are saved as text file named destination_flow_count.txt

destination_flow_count.txt

```
96.43.146.22 : 84
172.16.133.73 : 58
71.252.224.198 : 4
23.32.176.63 : 8
172.16.133.36 : 92
68.64.21.41 : 106
172.16.133.6 : 87
172.16.128.202 : 6
```

Source-Destination Pair with Most Data Transferred:

- **Pair:** `172.16.133.95:49358 -> 157.56.240.102:443`
- **Data Transferred:** 17,342,229 bytes

Q4: Packet Capture Performance

On the Same VM:

- **Packets Sent Using `tcpreplay`:**

```
dewansh@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$ sudo tcpreplay -i eth0 -p 3000 5.pcap
^C User interrupt...
sendpacket_abort
Actual: 6231 packets (2035453 bytes) sent in 2.07 seconds
Rated: 979861.7 Bps, 7.83 Mbps, 2999.58 pps
Flows: 1244 flows, 598.85 fps, 6227 unique flow packets, 4 unique non-flow packets
Statistics for network device: eth0
        Successful packets:        6230
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
dewansh@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$ sudo tcpreplay -i eth0 -p 2000 5.pcap
^C User interrupt...
sendpacket_abort
Actual: 3214 packets (1078245 bytes) sent in 1.60 seconds
Rated: 670731.4 Bps, 5.36 Mbps, 1999.29 pps
Flows: 768 flows, 477.74 fps, 3211 unique flow packets, 3 unique non-flow packets
Statistics for network device: eth0
        Successful packets:        3213
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

- **Packets Received Using `sniffer.py`:**

```
dewansh@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$ sudo python3 -u "/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN/sniffer.py"
Capturing packets for 10 seconds...
Total packets captured: 6150
Total data captured: 2013557 bytes
Capture duration: 10.10 seconds
Packets-per-second (PPS): 608.83
Bandwidth (Mbps): 1.59
Total data transferred: 2013557 bytes
Total packets transferred: 6150
Minimum packet size: 54 bytes
Maximum packet size: 1514 bytes
Average packet size: 327.41 bytes

Source-destination pair with most data transferred: 96.43.146.22:443 -> 172.16.133.109:49451 (209715 bytes)
dewansh@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$ sudo python3 -u "/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN/sniffer.py"
Capturing packets for 10 seconds...
Total packets captured: 3214
Total data captured: 1078245 bytes
Capture duration: 10.11 seconds
Packets-per-second (PPS): 317.94
Bandwidth (Mbps): 0.85
Total data transferred: 1078245 bytes
Total packets transferred: 3214
Minimum packet size: 54 bytes
Maximum packet size: 1514 bytes
Average packet size: 335.48 bytes

Source-destination pair with most data transferred: 96.43.146.22:443 -> 172.16.133.109:49451 (188637 bytes)
```

On Different VMs:

- **Packets Sent Using `tcpreplay`:**

```
        Retried packets (EAGAIN):  0
ubuntu@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$ sudo tcpreplay -p 1800 -i eth0 5.pcap
^C User interrupt...
sendpacket_abort
Actual: 9667 packets (3188519 bytes) sent in 5.37 seconds
Rated: 593616.0 Bps, 4.74 Mbps, 1799.73 pps
Statistics for network device: eth0
        Successful packets:        9666
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
ubuntu@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$ sudo tcpreplay -p 1500 -i eth0 5.pcap
^C User interrupt...
sendpacket_abort
Actual: 6268 packets (2046534 bytes) sent in 4.17 seconds
Rated: 489865.8 Bps, 3.91 Mbps, 1500.33 pps
Statistics for network device: eth0
        Successful packets:        6267
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
ubuntu@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$
```

- **Packets Received Using `sniffer.py`:**

```
Bandwidth (Mbps): 2.61
dewansh@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$ sudo python3 "/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN/capture.py"
Capturing packets for 10 seconds...
Total packets captured: 9650
Total data captured: 3181138 bytes
Capture duration: 10.09 seconds
Packets-per-second (PPS): 956.68
Bandwidth (Mbps): 2.52
dewansh@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$ sudo python3 "/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN/capture.py"
Capturing packets for 10 seconds...
Total packets captured: 6268
Total data captured: 2046534 bytes
Capture duration: 10.15 seconds
Packets-per-second (PPS): 617.68
Bandwidth (Mbps): 1.61
dewansh@DESKTOP-V3L98F8:/mnt/c/Users/Rakesh/OneDrive/Desktop/Sem6/CN$
```

Top Speed Without Packet Loss:

- **Same Machine:**
  - **Packets Per Second (pps):** *1999.29 pps*
  - **Mbps:** *5.36 Mbps*
- **Different Machines:**
  - **Packets Per Second (pps):** *1500.33 pps*
  - **Mbps:** *3.91 Mbps*

Part 2: Catch Me If You Can

Q1: File Analysis

- **File Name:** `networking_Questions.pdf`
- **TCP Checksum:** 35409
- **Source IP Address:** `10.20.30.200`

Q2: Packet Count for IP `10.20.30.200`

- **Number of Packets:** 30

Q3: Localhost Analysis

- **Port Used by Localhost:** 1001
- **Number of Packets from Localhost:** 30

Part 3: Capture the Packets

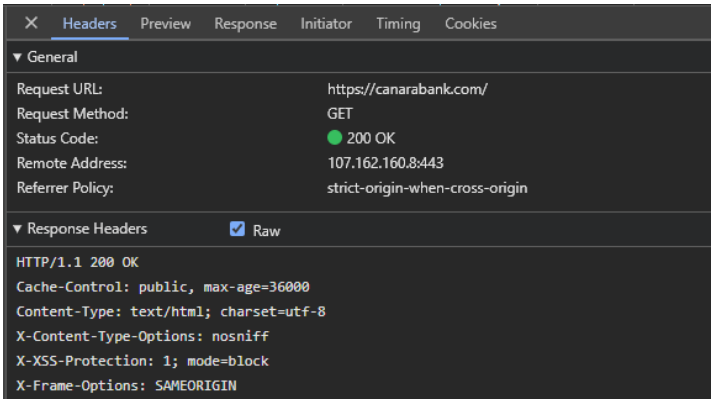
Q1: Application Layer Protocols

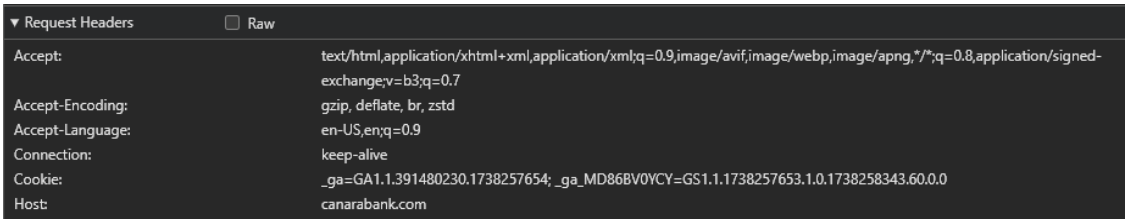
1. **QUIC (Quick UDP Internet Connections)** – Transport Layer
    - QUIC is a transport-layer protocol designed by Google to improve HTTP/3 performance by reducing latency and connection establishment time over UDP. It integrates encryption, reliability, and multiplexing. *(RFC 9000)*
2. **TLSv1.3 (Transport Layer Security)** – Application Layer
    - TLS 1.3 is a cryptographic protocol that provides end-to-end security for data transmission over networks, ensuring encryption, authentication, and integrity for applications like HTTPS. *(RFC 8446)*
3. **DNS (Domain Name System)** – Application Layer
    - DNS translates human-readable domain names into IP addresses, enabling efficient routing of internet traffic and functioning as the internet's phonebook. *(RFC 1035)*
4. **ARP (Address Resolution Protocol)** – Link Layer
    - ARP maps IP addresses to MAC addresses within a local network, allowing devices to communicate over Ethernet and Wi-Fi networks. *(RFC 826)*
5. **ICMP (Internet Control Message Protocol)** – Network Layer
    - ICMP is used for diagnostic and error reporting in networks, enabling tools like ping and traceroute to assess connectivity and detect issues. *(RFC 792)*

Q2: Website Analysis

a. Request Line and Connection Type

1. **Canarabank.com**

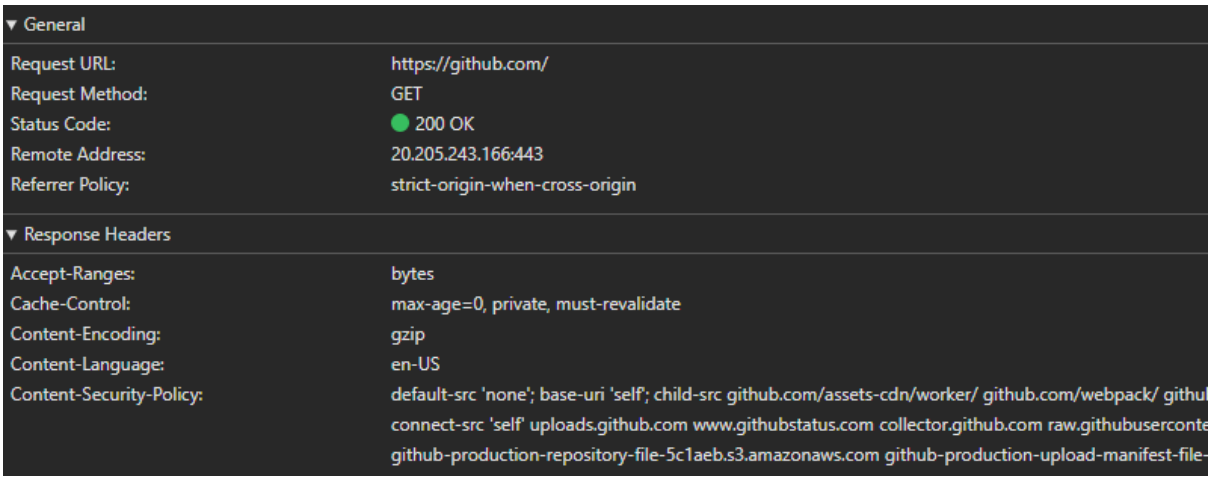


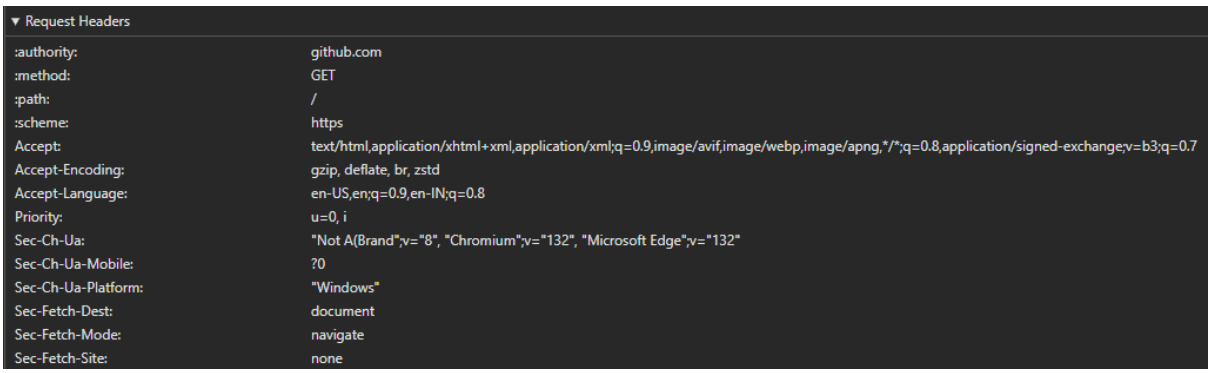


- Even though the client requested a persistent connection (keep-alive), the server's response (connection: close) overrides it. This means the TCP connection will terminate immediately after the response is sent, making it a non-persistent connection.

    - **Request Line:** `GET / HTTP/1.1`
    - **IP Address:** *107.162.160.8:443*
    - **Connection Type:** Non-persistent (Server response: `Connection: close`)

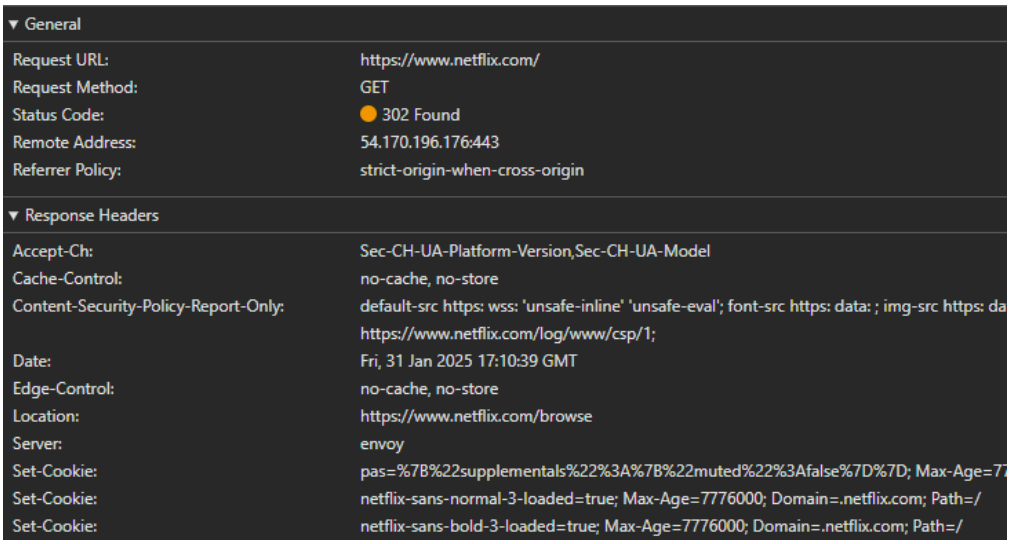
2. **Github.com**

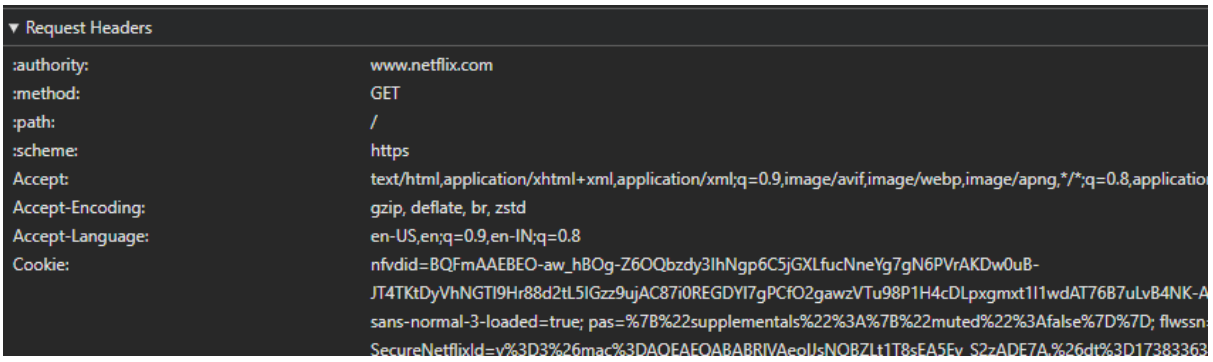




- **Request Line:** `GET / HTTP/1.1`
- **IP Address:** *20.205.243.116:443*
- **Connection Type:** Persistent

3. **Netflix.com**





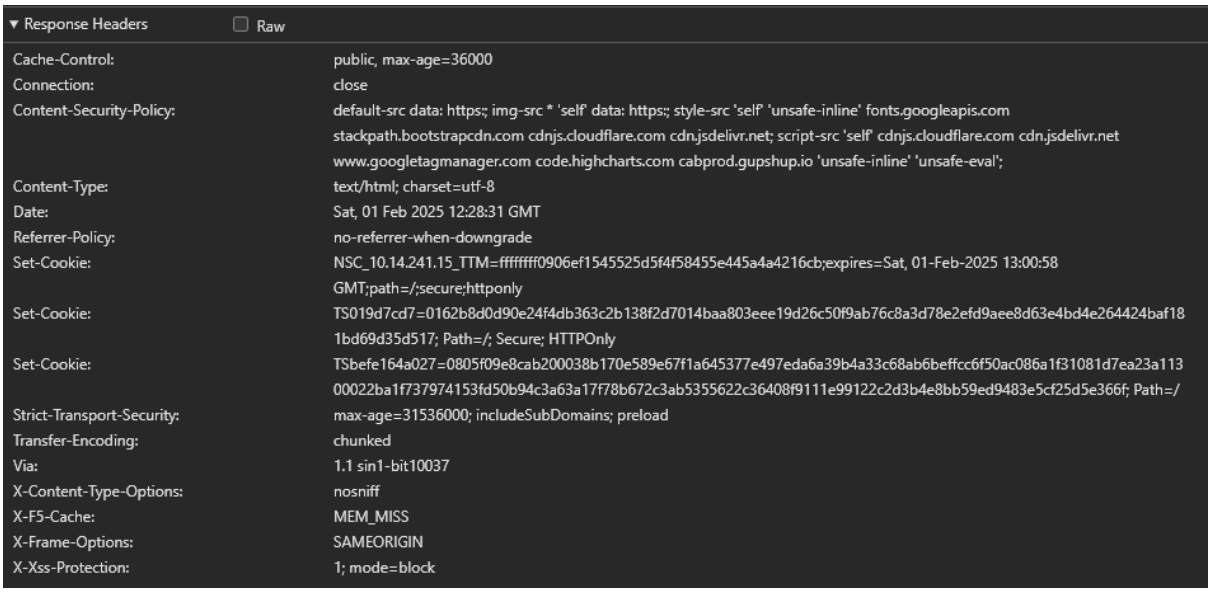
- **Request Line:** `GET / HTTP/1.1`
- **IP Address:** *54.170.196.176:443*
- **Connection Type:** Persistent

b. Header Fields and Error Codes

Website Analyzed: Canarabank.com

In the following Image we can see the three (or more) header fields.

Response Headers:



▼ Response Headers ☐ Raw

Cache-Control:	public, max-age=36000
Connection:	close
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 12:28:31 GMT
Referrer-Policy:	no-referrer-when-downgrade
Set-Cookie:	NSC_10.14.241.15_TTM=ffffffff0906ef1545525d5f4f58455e445a4a4216cb;expires=Sat, 01-Feb-2025 13:00:58 GMT;path=/;secure;httponly
Set-Cookie:	TS019d7cd7=0162b8d0d90e24f4db363c2b138f2d7014baa803eee19d26c50f9ab76c8a3d78e2efd9aee8d63e4bd4e264424baf181bd69d35d517; Path=/; Secure; HTTPOnly
Set-Cookie:	TSbefe164a027=0805f09e8cab200038b170e589e67f1a645377e497eda6a39b4a33c68ab6beffcc6f50ac086a1f31081d7ea23a11300022ba1f737974153fd50b94c3a63a17f78b672c3ab5355622c36408f9111e99122c2d3b4e8bb59ed9483e5cf25d5e366f; Path=/
Strict-Transport-Security:	max-age=31536000; includeSubDomains; preload
Transfer-Encoding:	chunked
Via:	1.1 sin1-bit10037
X-Content-Type-Options:	nosniff
X-F5-Cache:	MEM_MISS
X-Frame-Options:	SAMEORIGIN
X-Xss-Protection:	1; mode=block

Request Headers:

▼ 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-US,en;q=0.9
Connection:	keep-alive
Cookie:	_ga=GA1.1.391480230.1738257654; _ga_MD86BV0YCY=GS1.1.1738334360.2.1.1738335590.60.0.0
Host:	canarabank.com
Sec-Ch-Ua:	"Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Windows"
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36

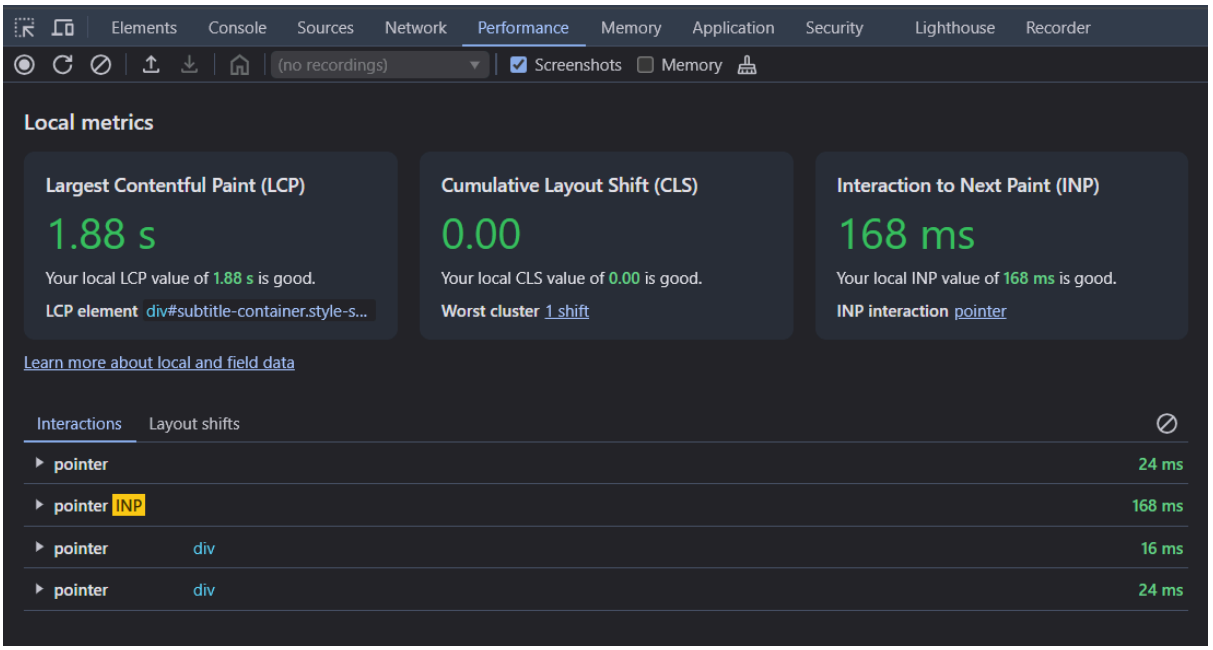
HTTP Error Codes:

1. `400 Bad Request` – The server cannot process the request due to a client error.
2. `404 Not Found` – The requested resource could not be found on the server.
3. `500 Internal Server Error` – The server encountered an unexpected condition.

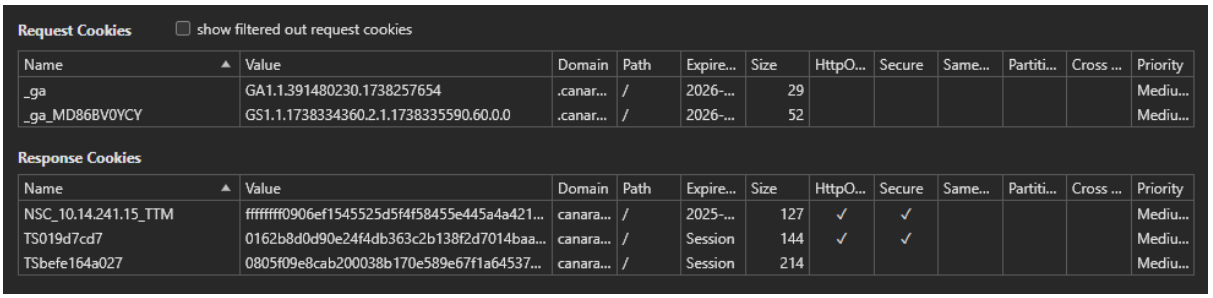
c. Performance Metrics and Cookies

Browser Used: *Chrome*

Performance Metrics:



Cookies



Submission Details

- **GitHub Repository Link:**
  https://github.com/dewanshkumar123/CN-Assignment-1