

# CS 331: Computer Networks

## Assignment 1

[Github Link](#)

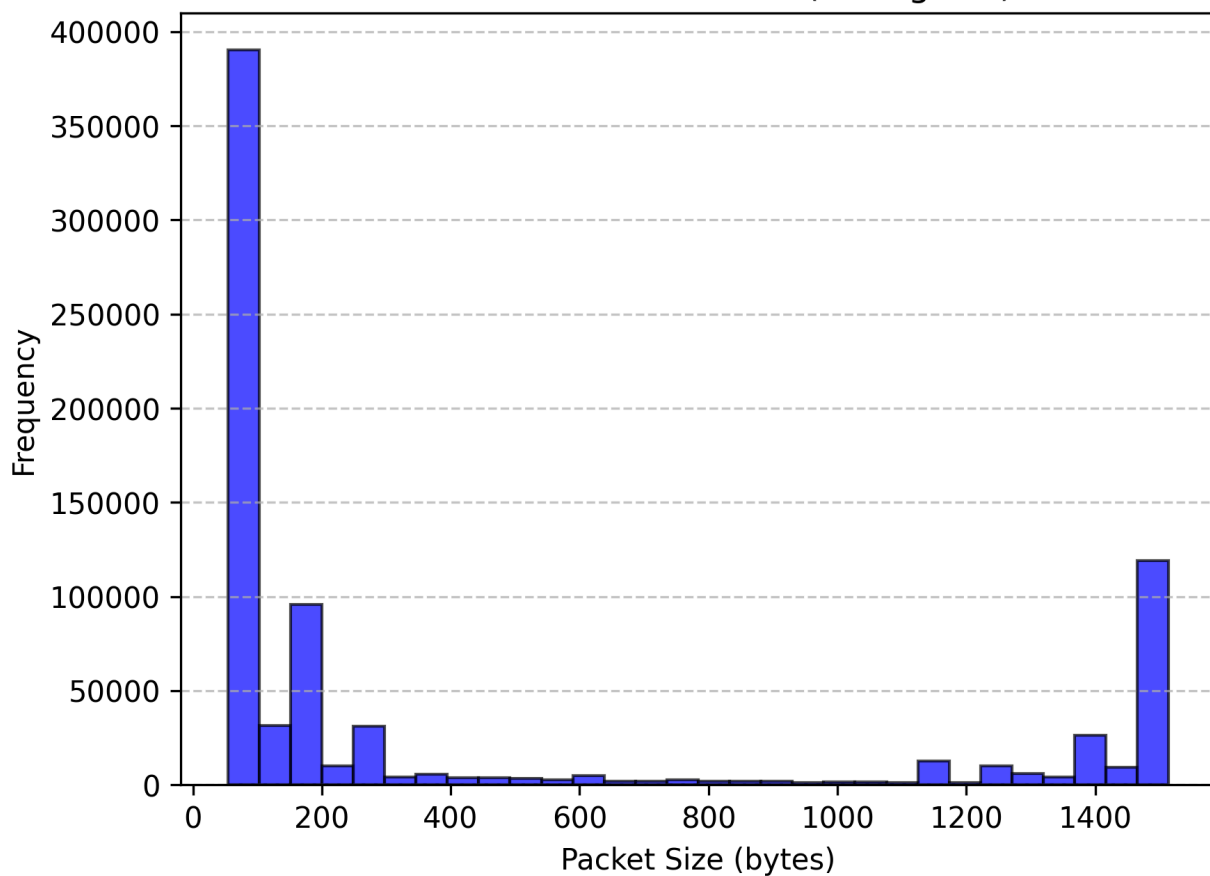
### Part 1: Metrics and Plots

1.

```
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
saloni98@SALONI:/mnt/d/SEM6/CN/kali_a1$ ^C
saloni98@SALONI:/mnt/d/SEM6/CN/kali_a1$ sudo tcpdump -i eth0 -tt -s 4096 -C 1000000 -w packet_capture.pcap
pcap
Actual: 792179 packets (355624326 bytes) sent in 40.96 seconds
Rated: 8681710.1 Bps, 69.45 Mbps, 19339.13 pps
Statistics for network device: eth0
  Successful packets: 792179
  Failed packets: 0
  Truncated packets: 0
  Retried packets (ENOBUFS): 0
  Retried packets (EAGAIN): 0
saloni98@SALONI:/mnt/d/SEM6/CN/kali_a1$

Packet captured! Size: 1514 bytes | Total Packets: 792179
Packet captured! Size: 54 bytes | Total Packets: 792179
^C^C^C
Capture complete.
Total Packets: 792179
Total Data Transferred: 355624326 bytes
Min Packet Size: 54 bytes
Max Packet Size: 1514 bytes
Avg Packet Size: 448.919 bytes
Most data transferred by: 172.16.133.95:49358 -> 157.56.240.102:443 with 173
42229 bytes
Packet size histogram saved to histogram_data.csv.
Detailed statistics saved to packet_statistics.txt
saloni98@SALONI:/mnt/d/SEM6/CN/A1$
```

Packet Size Distribution (Histogram)



2

Dictionary of unique source-destination pairs are stored in packet\_statistics.txt.

3

Dictionary of source IP flow counts and destination IP flow counts is also stored in packet\_statistics.txt.

## Part 2: Catch Me If You Can

### 4.pcap

```
saloni98@SALONI:/mnt/d/SEM6/CN/kali_a1$ sudo tcpreplay -i eth0 --topspeed 4.
pcap
Actual: 792179 packets (355624326 bytes) sent in 22.43 seconds
Rated: 15851930.8 Bps, 126.81 Mbps, 35311.32 pps
Statistics for network device: eth0
  Successful packets: 792179
  Failed packets: 0
  Truncated packets: 0
  Retried packets (ENOBUFS): 0
  Retried packets (EAGAIN): 0
saloni98@SALONI:/mnt/d/SEM6/CN/kali_a1$ ^C
saloni98@SALONI:/mnt/d/SEM6/CN/kali_a1$

Packet Captured! Size: 62 bytes
Packet Captured! Size: 1514 bytes
Packet Captured! Size: 54 bytes
Packet Captured! Size: 63 bytes
Packet Captured! Size: 63 bytes
Packet Captured! Size: 88 bytes
Packet Captured! Size: 62 bytes
^C
Capture complete.
Total packets captured: 792179
Total packets containing hidden message: 11
saloni576@SALONI:/mnt/d/SEM6/CN/A1$ |
```

Q.1 Hidden Message: Welcome to Computer Networks CS331

Q.2 Total packets containing the hidden message: 11

Q.3 Protocol Used:TCP

Q.4 TCP Checksum:0xf049

*Note: To run the programs, I used two different versions of Ubuntu while doing Part 1 and Part 2 of the assignment.*

```
Retried packets (EAGAIN): 0
saloni98@SALONI:/mnt/d/SEM6/CN/kali_a1$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 20.04.6 LTS
Release: 20.04
Codename: focal
saloni98@SALONI:/mnt/d/SEM6/CN/kali_a1$

Detailed statistics saved to packet_statistics.txt
saloni576@SALONI:/mnt/d/SEM6/CN/A1$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 22.04.5 LTS
Release: 22.04
Codename: jammy
saloni576@SALONI:/mnt/d/SEM6/CN/A1$ |
```

## Part 3: Capture the Packets

Q.1.a.

Application layers captured by Wireshark are as follows:

### 1. MDNS (Multicast DNS)

87105	1308.510222	10.1.0.10	224.0.0.251	MDNS	315	Standard query 0x0000 ANY _afpovertcp._tcp.local, "QM" questio
1132...	1992.357321	10.7.39.20	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DESKTOP-DCD9693.local, "QM" question
1132...	1992.358243	fe80::258e:c0c3:4c7...	ff02::fb	MDNS	101	Standard query 0x0000 ANY DESKTOP-DCD9693.local, "QM" question
1132...	1992.362833	fe80::258e:c0c3:4c7...	ff02::fb	MDNS	139	Standard query response 0x0000 AAAA fe80::258e:c0c3:4c7:934f A
1132...	1992.364846	10.7.39.20	224.0.0.251	MDNS	119	Standard query response 0x0000 AAAA fe80::258e:c0c3:4c7:934f A
1132...	1992.709605	10.7.39.20	224.0.0.251	MDNS	95	Standard query 0x0000 ANY DESKTOP-DCD9693._display._tcp.local,
1132...	1992.710598	fe80::258e:c0c3:4c7...	ff02::fb	MDNS	115	Standard query 0x0000 ANY DESKTOP-DCD9693._display._tcp.local,
1132...	1992.972987	10.7.39.20	224.0.0.251	MDNS	95	Standard query 0x0000 ANY DESKTOP-DCD9693._display._tcp.local,
1132...	1992.974105	fe80::258e:c0c3:4c7...	ff02::fb	MDNS	115	Standard query 0x0000 ANY DESKTOP-DCD9693._display._tcp.local,

Operation: MDNS allows devices on a local network to resolve hostnames to IP addresses without requiring a DNS server. It's commonly used for service discovery on home networks.

Layer: Application (Layer 7)

RFC: RFC 6762

## 2. DHCPv6 (Dynamic Host Configuration Protocol for IPv6)

1131...	1991.797127	0.0.0.0	255.255.255.255	DHCP	364 DHCP Request	- Transaction ID 0x44df1441
1131...	1991.848106	1.1.1.1	10.7.39.20	DHCP	346 DHCP ACK	- Transaction ID 0x44df1441
1131...	1991.837828	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd
1132...	1992.846465	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd
1132...	1993.857255	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd
1133...	1995.869547	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd
1140...	1999.878938	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd

Operation: DHCPv6 is a protocol used to assign IPv6 addresses to devices on a network and provide configuration information such as DNS servers and prefixes.

Layer: Application (Layer 7)

RFC: RFC 8415

## 3. DHCP (Dynamic Host Configuration Protocol)

1131...	1991.797127	0.0.0.0	255.255.255.255	DHCP	364 DHCP Request	- Transaction ID 0x44df1441
1131...	1991.848106	1.1.1.1	10.7.39.20	DHCP	346 DHCP ACK	- Transaction ID 0x44df1441
1131...	1991.837828	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd
1132...	1992.846465	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd
1132...	1993.857255	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd
1133...	1995.869547	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd
1140...	1999.878938	fe80::258e:c0c3:4c7...	ff02::1:2	DHCPv6	157 Solicit	XID: 0xc29b81 CID: 000100012aa63d550c37966fe7bd

Operation: DHCP assigns IPv4 addresses and other network configuration parameters, such as the gateway and DNS server, to devices on a network.

Layer: Application (Layer 7)

RFC: RFC 2131

## 4. OCSP (Online Certificate Status Protocol)

1705...	3666.354819	142.251.42.3	10.7.39.20	OCSP	330 Response
1705...	3666.444653	142.251.42.3	10.7.39.20	OCSP	766 Response

Operation: OCSP is used to check the revocation status of digital certificates in real time, enhancing the security of SSL/TLS connections.

Layer: Application (Layer 7)

RFC: RFC 6960

## 5. LLMNR (Link-Local Multicast Name Resolution)

21259	516.097356	fe80::258e:c0c3:4c7...	ff02::1:3	LLMNR	95 Standard query	0x19b2 ANY DESKTOP-DCD9693
21261	516.097934	10.7.39.20	224.0.0.252	LLMNR	75 Standard query	0x19b2 ANY DESKTOP-DCD9693
21281	516.234778	fe80::258e:c0c3:4c7...	ff02::1:3	LLMNR	95 Standard query	0xb2ed ANY DESKTOP-DCD9693
21282	516.235136	10.7.39.20	224.0.0.252	LLMNR	75 Standard query	0xb2ed ANY DESKTOP-DCD9693
30735	754.115928	fe80::258e:c0c3:4c7...	ff02::1:3	LLMNR	95 Standard query	0x87f6 ANY DESKTOP-DCD9693
30736	754.116248	10.7.39.20	224.0.0.252	LLMNR	75 Standard query	0x87f6 ANY DESKTOP-DCD9693

Operation: LLMNR allows devices on the same local network to resolve hostnames without requiring a DNS server. It enables communication between devices on link-local IPv4 or IPv6 networks.

Layer: Application (Layer 7)

RFC: RFC 4795

## Q.2.a

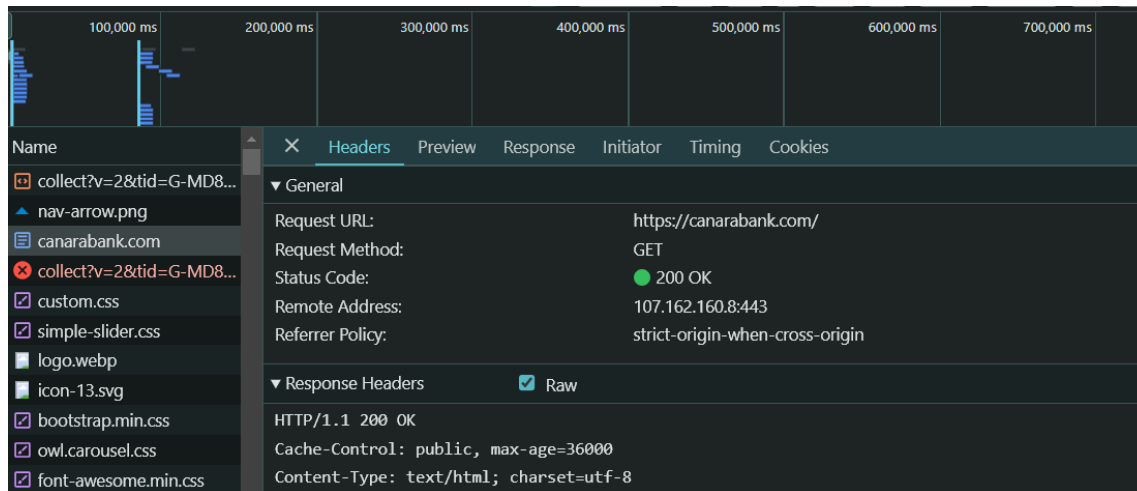
### 1.Canarabank.com

**Request line:**GET / HTTP/1.1

**IP address:**107.162.160.8:443

**Connection:** keep-alive (in request header)

**Connection:**close (in response header)



The client (Google Chrome) requested a persistent connection by sending the Connection: keep-alive header. However, the server responded with Connection: close, indicating that it will terminate the connection after completing the response. Therefore, the connection is **not persistent** for this page.

### 2.Github.com

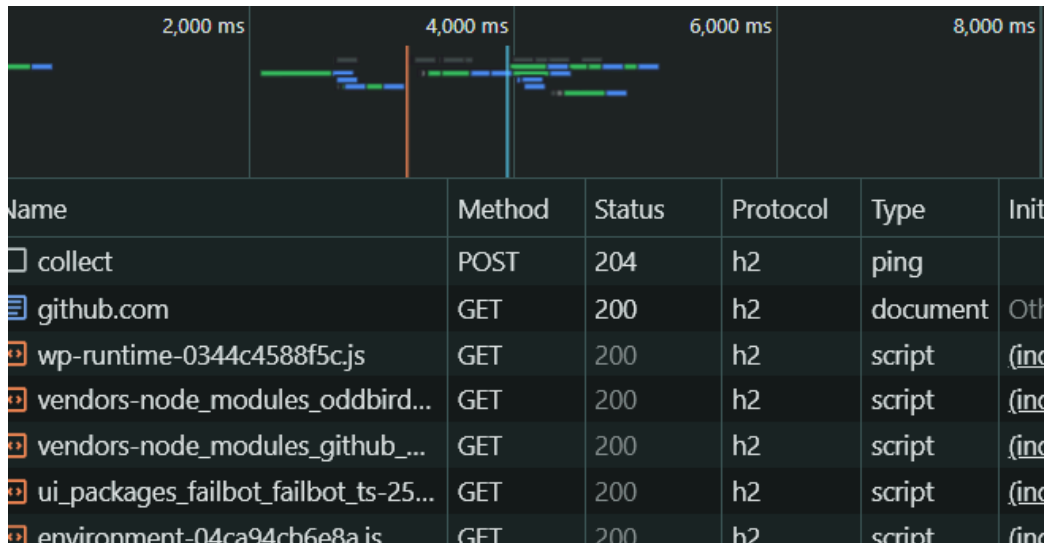
**Protocol:** HTTP/2

**IP Address:** 20.205.243.166:443

Since GitHub uses HTTP/2, there is no traditional request line. Instead, HTTP/2 employs pseudo-headers to carry essential information in a binary format, which is more efficient than the conventional request structure.

#### Connection Details:

HTTP/2 assumes persistent connections by default, eliminating the need for explicit headers such as Connection: keep-alive. Therefore, the connection is inherently **persistent** for GitHub.



The image shows a detailed view of a network request for 'github.com'. The 'Headers' tab is selected, showing the following information:

- General:**
  - Request URL: https://github.com/
  - Request Method: GET
  - Status Code: 200 OK
  - Remote Address: 20.205.243.166:443
  - Referrer Policy: strict-origin-when-cross-origin
- Response Headers:**
  - Cache-Control: max-age=0, private, must-revalidate

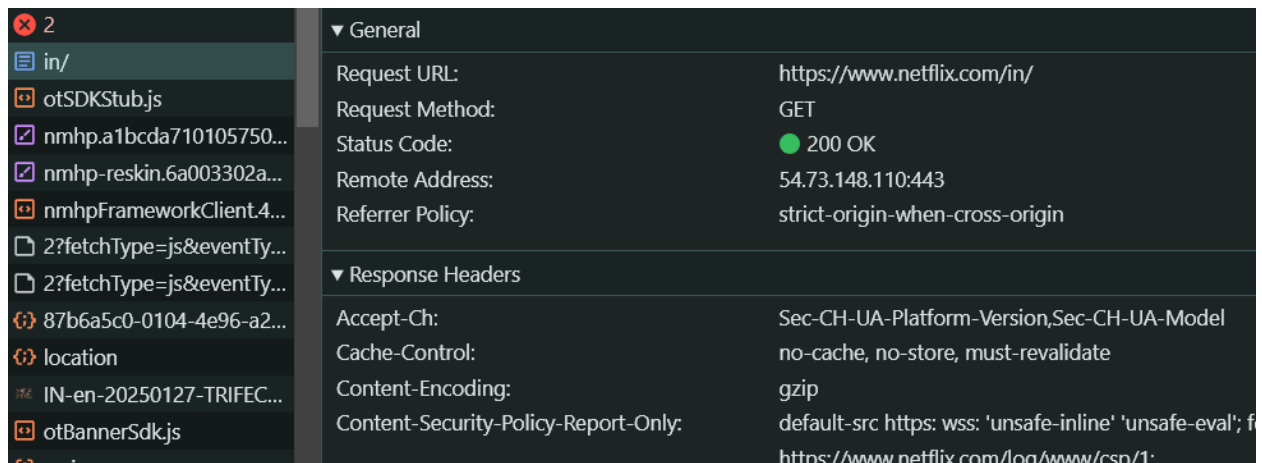
### 3. Netflix.com

**Protocol:** HTTP/2

**IP Address:** 54.73.148.110:443

Similar to GitHub, Netflix utilizes HTTP/2, which replaces traditional request lines with pseudo-headers for efficiency.

2	POST	(canceled)		fetch	
in/	GET	200	h2	document	Other
otSDKStub.js	GET	200	http/1.1	script	in/0



### Connection Details:

Since HTTP/2 implicitly supports persistent connections, the connection remains **persistent** without the need for explicit headers

### Q.2.b

#### Request header:

Header file	Value
authority	github.com
method	GET
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 header:

Header file	Value
Content type	text/html; charset=utf-8
Server	GitHub.com
Cache-Control	max-age=0, private, must-revalidate

## HTTP error codes:

### 1. 404 Not Found

The screenshot shows the DevTools Network tab with a list of network requests. The request for `favicon.ico` is highlighted, showing a status of 404. The details panel for this request is open, showing the request URL, method, status code, remote address, and referrer policy.

Name	Method	Status	Protocol	Type	Initiator
favicon.ico	GET	404	http/1.1	text/html	Other
bot-icon.png	GET	404	http/1.1	text/html	webpack://cpg
collect?v=2&tid=G-MD86BV0YCY&otm=45ie51u0v86904983...arabankd...	POST	204	h2	fetch	

Details for `favicon.ico`:

- Request URL: `https://canarites.canarabankdigi.in/favicon.ico`
- Request Method: `GET`
- Status Code: `404 Not Found`
- Remote Address: `103.122.53.22:443`
- Referrer Policy: `strict-origin-when-cross-origin`

This error occurs when the server cannot find the requested resource. It usually happens when the URL is incorrect or the resource (like a webpage or file) has been moved or deleted.

### 2. 403 Forbidden error

The screenshot shows the DevTools Network tab with a list of network requests. The request for `j_security_check?locale=en` is highlighted, showing a status of 403. The details panel for this request is open, showing the request URL, method, status code, and referrer policy.

Name	Method	Status	Protocol	Type
j_security_check?locale=en	POST	403	http/1.1	fetch
j_security_check?locale=en	POST	403	http/1.1	fetch

Details for `j_security_check?locale=en`:

- Request URL: `https://online.canarabank.in/digxj_security_check?locale=en`
- Request Method: `POST`
- Status Code: `403 Forbidden (from service worker)`
- Referrer Policy: `strict-origin-when-cross-origin`

A 403 error means that access to the requested resource is denied for some reason, even though the request was understood by the server. The server is actively refusing to fulfill the request.

### 3.400 Bad Request

A 400 Bad Request error means that the server was unable to process the request because it was malformed in some way. This is a client-side error, meaning that the problem lies with the request sent by the client (the browser or application).

The screenshot shows the Chrome DevTools Console with a list of errors on the left and the details of a selected error on the right. The error is a 400 Bad Request (from service worker) for the URL `https://online.canarabank.in/digx/cz/v1/credentials/validateforgotUserId?loc...`. The status code is 400, and the referrer policy is `strict-origin-when-cross-origin`. The response headers show `Cache-Control: max-age=0, no-cache, no-store, must-revalidate` and `Connection: close`.

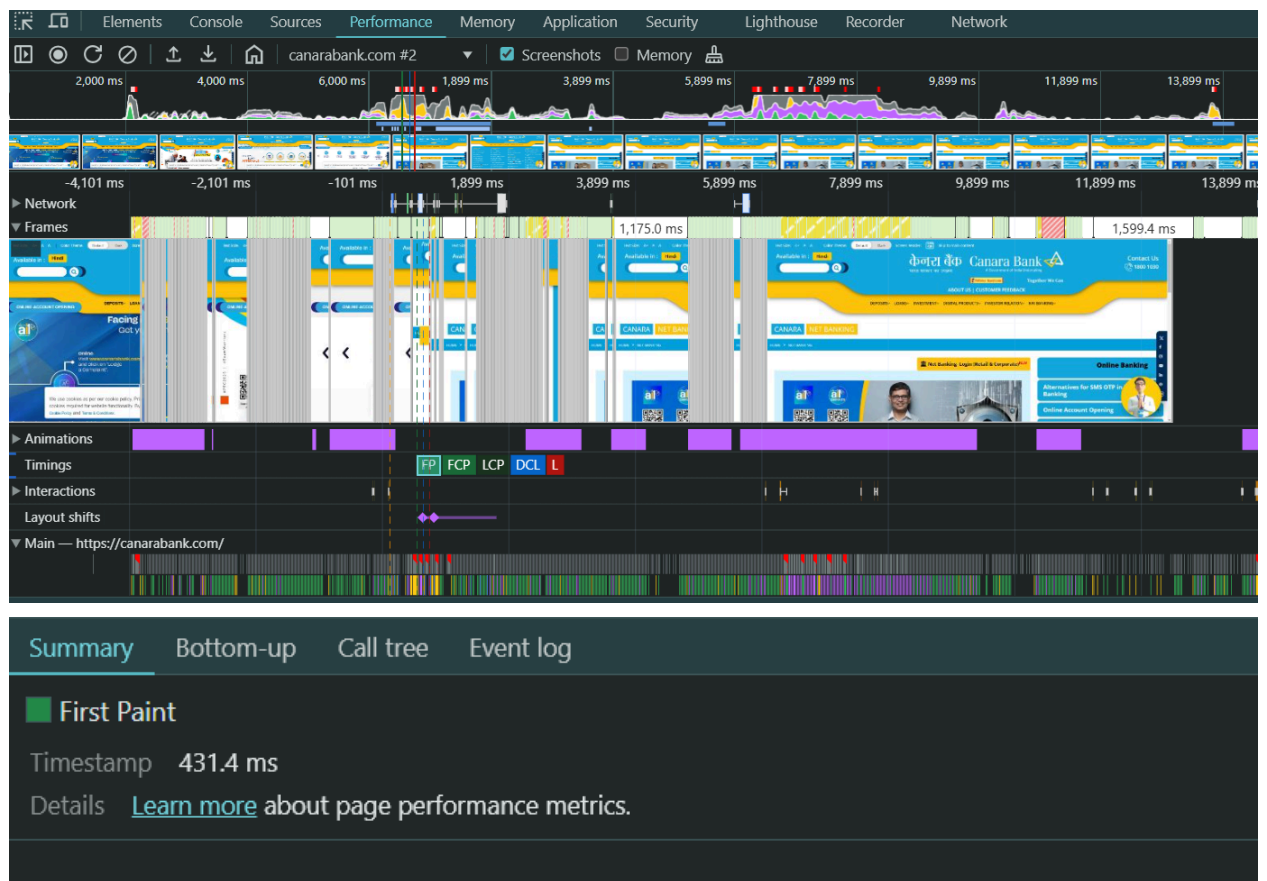
General	
Request URL:	<code>https://online.canarabank.in/digx/cz/v1/credentials/validateforgotUserId?loc...</code>
Request Method:	POST
Status Code:	400 Bad Request (from service worker)
Referrer Policy:	<code>strict-origin-when-cross-origin</code>

Response Headers	
Cache-Control:	<code>max-age=0, no-cache, no-store, must-revalidate</code>
Connection:	<code>close</code>

### Q.2.c

#### Performance metrics and cookies

##### 1. Canarabank.com



FP: 431.42 ms

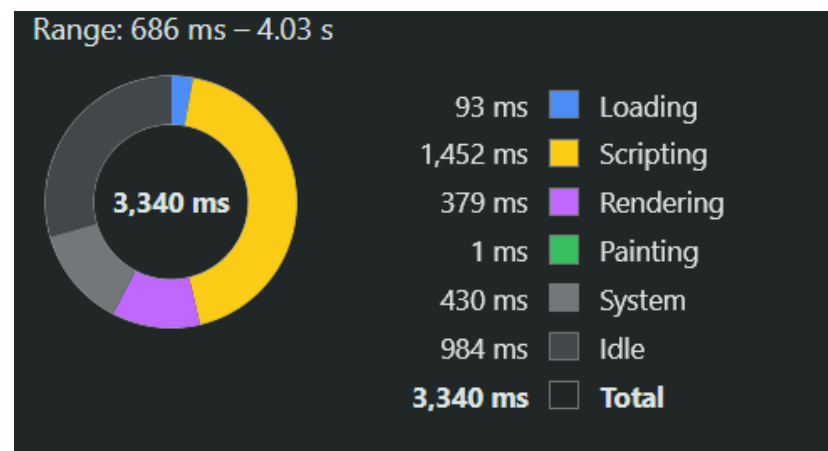
FCP: 431.42 ms

LCP: 431.42

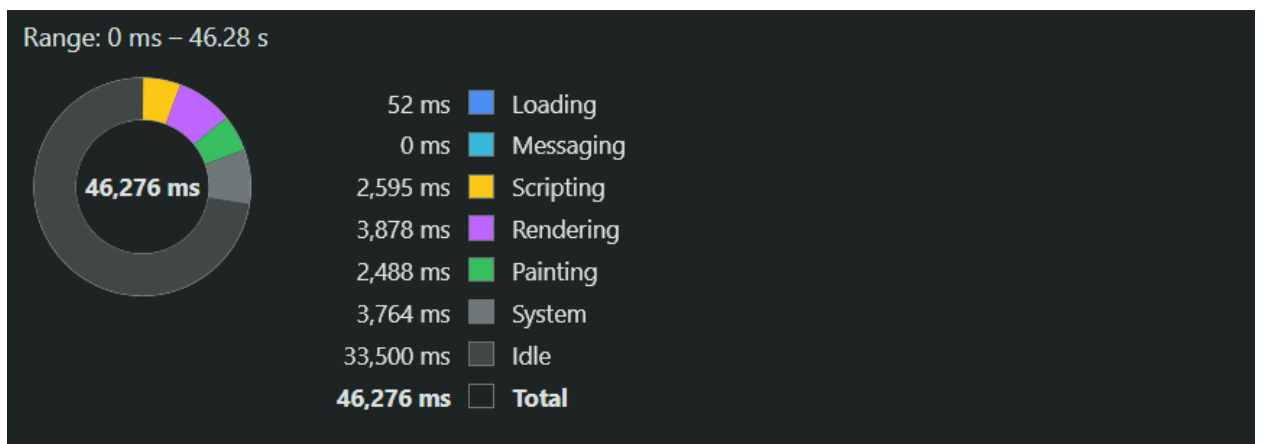
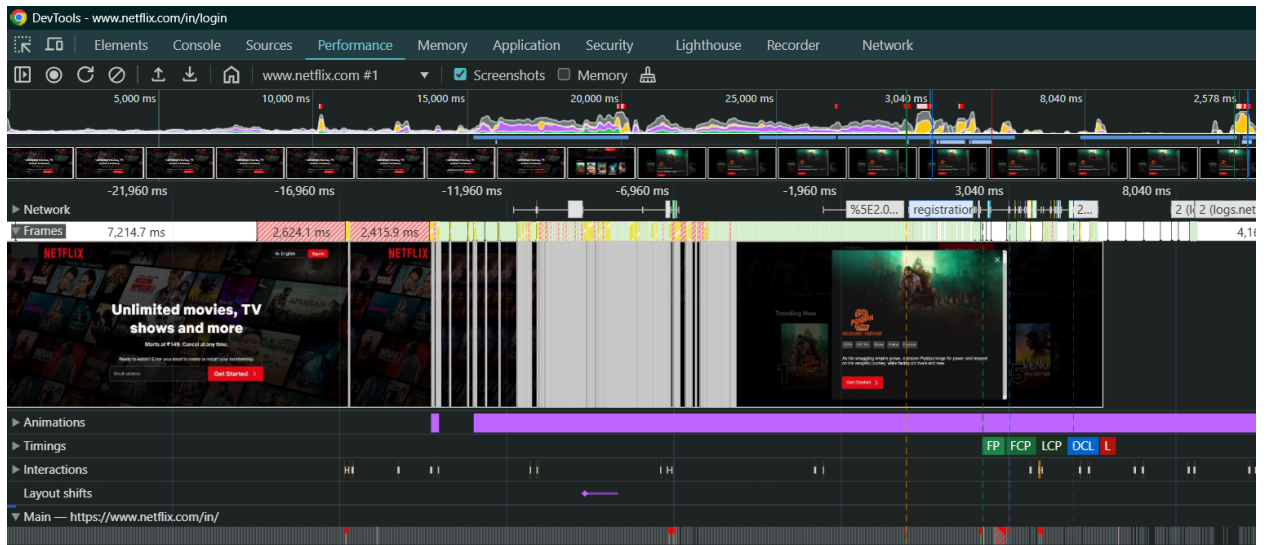


Browser used: Google Chrome

### 3. Netflix.com



Browser used : Google Chrome



FP : 2.26s

FCP: 2.26s

LCP : 2.26s

DCL: 3.07s

L: 5.00s

Browser used: Google Chrome

## Cookies for github.com

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Partiti...	Cross S...	Priority
__Host-user_session_same_site	dKTSrQ5XReCpN...	github.com	/	2025-02-14T15:52:12.566Z	77	✓	✓	Strict			Medium
_device_id	0f374781d40abb...	github.com	/	2026-01-31T15:52:12.566Z	42	✓	✓	Lax			Medium
_gh_sess	6ZID8RyCszbaTV...	github.com	/	Session	634	✓	✓	Lax			Medium
_octo	GH1.1.202461684...	github.com	/	2025-04-23T10:03:30.715Z	32		✓	Lax			Medium
color_mode	%7B%22color_mo...	.github.com	/	Session	214		✓	Lax			Medium
cpu_bucket	xlq	.github.com	/	Session	13		✓	Lax			Medium
dotcom_user	Rutuj18	.github.com	/	2026-01-17T19:22:39.496Z	18	✓	✓	Lax			Medium
logged_in	yes	.github.com	/	2026-01-17T19:22:39.496Z	12	✓	✓	Lax			Medium
preferred_color_mode	dark	.github.com	/	Session	24		✓	Lax			Medium
saved_user_sessions	117572304%3AdK...	github.com	/	2025-04-17T19:22:38.495Z	79	✓	✓	Lax			Medium
tz	Asia%2FCalcutta	.github.com	/	Session	17		✓	Lax			Medium
user_session	dKTSrQ5XReCpN...	github.com	/	2025-02-14T15:52:12.566Z	60	✓	✓	Lax			Medium

1. \_Host-user\_session\_same\_site  
Flags: HttpOnly, Secure, SameSite(Strict)
2. \_device\_id  
Flags: HttpOnly, Secure, SameSite(Lax)
3. \_gh\_sess  
Flags: HttpOnly, Secure, SameSite(Lax)
4. \_octo  
Flags: Secure, SameSite(Lax)
5. color\_mode  
Flags: Secure, SameSite(Lax)
6. cpu\_bucket  
Flags: Secure, SameSite(Lax)
7. dotcom\_user  
Flags: HttpOnly, Secure, SameSite(Lax)
8. logged\_in  
Flags: HttpOnly, Secure, SameSite(Lax)
9. preferred\_color\_mode  
Flags: Secure, SameSite(Lax)
10. saved\_user\_sessions  
Flags: HttpOnly, Secure, SameSite(Lax)
11. tz

Flags:Secure, SameSite(Lax)

12. user\_session

Flags:HttpOnly,Secure, SameSite(Lax)