# Assignment 1

Anushika Mishra (22110029), Harshita Singh (22110299)

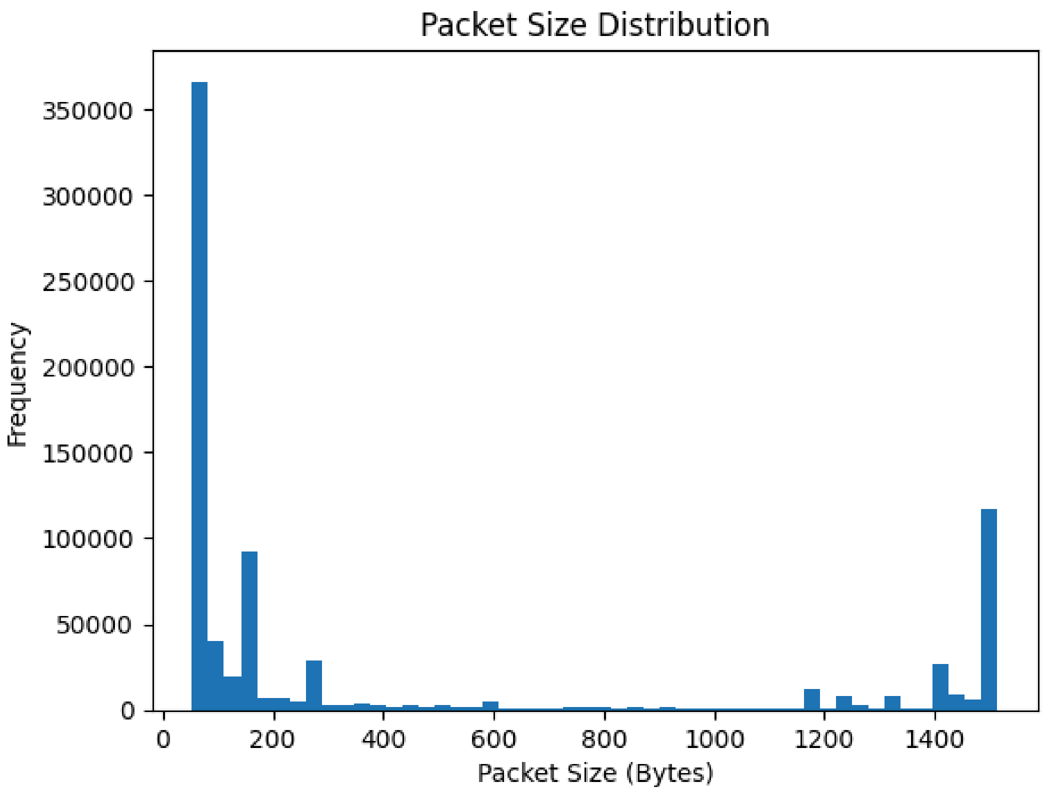
**NOTE : We have uploaded all the generated and recorded .pcap file on the drive link CN_Assignment1 (was not able to upload on Github).**

## Part 1: Metrics and Plots

**From the chosen X.pcap file, extract and generate the following metrics for the data as captured by your program when you perform the pcap replay using tools like tcpreplay:**

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

Answer:Total Data Transferred: 364569320 bytes
Total Packets: 805996
Min Packet Size: 54 bytes
Max Packet Size: 1514 bytes
Average Packet Size: 452.32150035484045 bytes



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

Answer: for this see the jupyter notebook in this

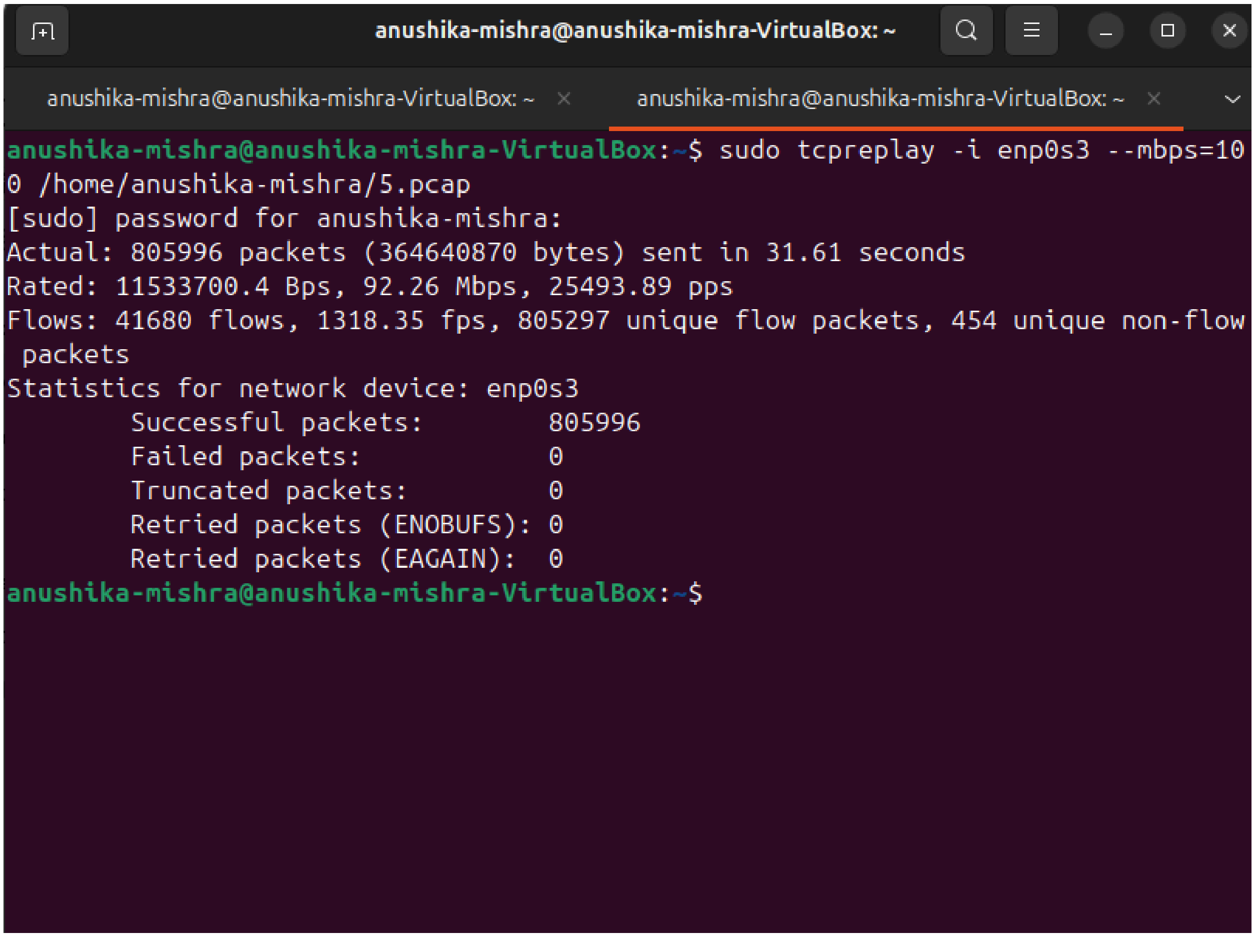
**3:Display a dictionary where the key is the IP address and the value is the total flows for that IP address as the source. Similarly display a dictionary where the key is the IP address and the value is the total flows for that IP address as the destination. Find out which source-destination (source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

Answer: **For this part see this github jupyter notebook**

**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 ij running both tcpreplay and your program on the same machine (VM), and s when running on different machines Two student group should run the program on two different machines, eg tcpreplay on physical machine of student and sniffer program physical-machine of Muten. Single students should run between two VMs**

Answer: For Single Machine: Source-Destination Pair with Most Data: ('172.16.133.95', '157.56.240.102')

Total Data Transferred: 17381571 bytes


anushika-mishra@anushika-mishra-VirtualBox: ~
anushika-mishra@anushika-mishra-VirtualBox: ~
anushika-mishra@anushika-mishra-VirtualBox: ~

```
anushika-mishra@anushika-mishra-VirtualBox:~$ sudo tcpreplay -i enp0s3 --mbps=10
0 /home/anushika-mishra/5.pcap
[sudo] password for anushika-mishra:
Actual: 805996 packets (364640870 bytes) sent in 31.61 seconds
Rated: 11533700.4 Bps, 92.26 Mbps, 25493.89 pps
Flows: 41680 flows, 1318.35 fps, 805297 unique flow packets, 454 unique non-flow
 packets
Statistics for network device: enp0s3
        Successful packets:        805996
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
anushika-mishra@anushika-mishra-VirtualBox:~$
```

## Part 2: Catch Me If You Can

**For the designated X.pcap file, extend the program to sniff and answer the specific questions:**

Q1.There is a tcp packet which contains the name of some file.

a.Find that file name.(hint: search for <The name of file is = > )

ANS: File Name: networking_Questions.pdf

b.Find tcp checksum of that packet

ANS: TCP Checksum: 35409

c.Find the source ip address of that packet

ANS: Source IP: 10.20.30.200

Q2.Find the number of packets with that ip address.

ANS: Number of packets from 10.20.30.200: 30

Q3.From localhost I have requested for the phone to find the company name of that phone. (hint: search for <Company of phone is = >)

a.Find port used by localhost.

ANS: Ports used by localhost: {1001, 1002}

b. Find number of packets from localhost.

ANS: Number of packets from localhost: 30

## 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.**
**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.**

Answer- After running wireshark I performed certain activities (logged in canvas and put wrong credentials, then put the correct ones, opened MS teams and downloaded a file). After performing these activities several protocols were recorded by wireshark. I have tabulated the protocols recorded their layer of operation and their RFC number. The .pcap file generated for this has been uploaded to the drive CN_Assignment1 .

| Protocol | Layer | RFC Number |
|---|---|---|
| TCP | Transport (L4) | RFC 9293 |
| TLS v1.2 | Application (L7) | RFC 5246 |
| TLS v1.3 | Application (L7) | RFC 8446 |
| ARP | Network (L3) | RFC 826 |
| QUIC | Transport (L4) | RFC 9000 |
| DNS | Application (L7) | RFC 1035 |
| UDP | Transport (L4) | RFC 768 |
| ICMP | Network (L3) | RFC 792 |

| | | |
|---|---|---|
| NBNS | Application (L7) | RFC 1002 |

1. TCP (Transmission Control Protocol)

TCP is a transport layer protocol that sets up connections and makes sure data moves between devices. It starts with a three-way handshake, so both sides are ready to talk. TCP checks for mistakes, sends things again if needed, and controls the flow to keep data intact. People use it for web browsing (HTTP/HTTPS), email (SMTP IMAP), and moving files (FTP). TCP needs to confirm each packet, so it's slower than UDP but more trustworthy for important tasks.

---

2. TLS 1.2 (Transport Layer Security)

TLS 1.2 secures Internet communications playing a key role in HTTPS, email, and VoIP. It uses symmetric and asymmetric encryption to protect data and relies on hashing algorithms such as SHA-256 to maintain data integrity. This protocol brought in support for more robust cipher suites and Perfect Forward Secrecy (PFS). However, TLS 1.3 has taken its place because it offers better security and works more .

---

3. TLS 1.3 (Transport Layer Security)

TLS 1.3 has an impact on TLS 1.2 by getting rid of old cryptographic algorithms, cutting down on handshake delays, and boosting performance. It does away with RSA key exchange depending on Elliptic Curve Diffie-Hellman (ECDHE) to ensure forward secrecy. TLS 1.3 backs zero-round-trip time (0-RTT) resumption, which allows for quicker reconnections. It sees widespread use in securing websites, online banking, and encrypted messaging platforms.

---

4. ARP (Address Resolution Protocol)

ARP is a network layer protocol, which is used to map IP addresses to MAC addresses of a LAN. If a device is wishing to communicate with a device on the same subnet, it sends an ARP request in an attempt to obtain a MAC address for the addressee. The responding target device sends an ARP response containing its MAC address. ARP runs on IPv4 networks, but it can be susceptible to spoofing attacks (ARP poisoning).

---

5. QUIC (Quick UDP Internet Connections)

Google has developed QUIC as a transport layer protocol that promises to enhance the security and speed of the Internet. This protocol works over UDP and the security details are similar to TLS 1.3, but the connection establishment is quicker than that of TCP. The service area of QUIC can be found in Google services, HTTP/3, and some video streaming platforms to control latency and packet loss.

---

## 6. DNS (Domain Name System)

When we talk about "DNS," we're generally talking about IP addresses and their relations. A DNS server, which could be any of several domain names, can have the function of translating a URL to an IP address (and other information, like a controller). In the asset hierarchy, you have the top-level domain (another type of hierarchy) and authoritative servers--server-level trust. The DNS is the only assigned (initial) and the local (already assigned) network number of the client computer and the DNS server number of the remote node are depicted, separated by a tab. It relays commands for reference to a domain name server (DNS). It is one of the most important reasons why the internet exists. Moreover, it allows extensions like DNSSEC for security.

---

## 7. UDP (User Datagram Protocol)

UDP is a connectionless, fast transport protocol used in places where speed is more important than reliability. In contrast to TCP, it doesn't manage error correction or retransmissions at all, which is why it is great for instantaneous applications like VoIP, gaming, and video streaming. UDP packets are small and have low latency but can be lost in transit.

---

## 8. ICMP (Internet Control Message Protocol)

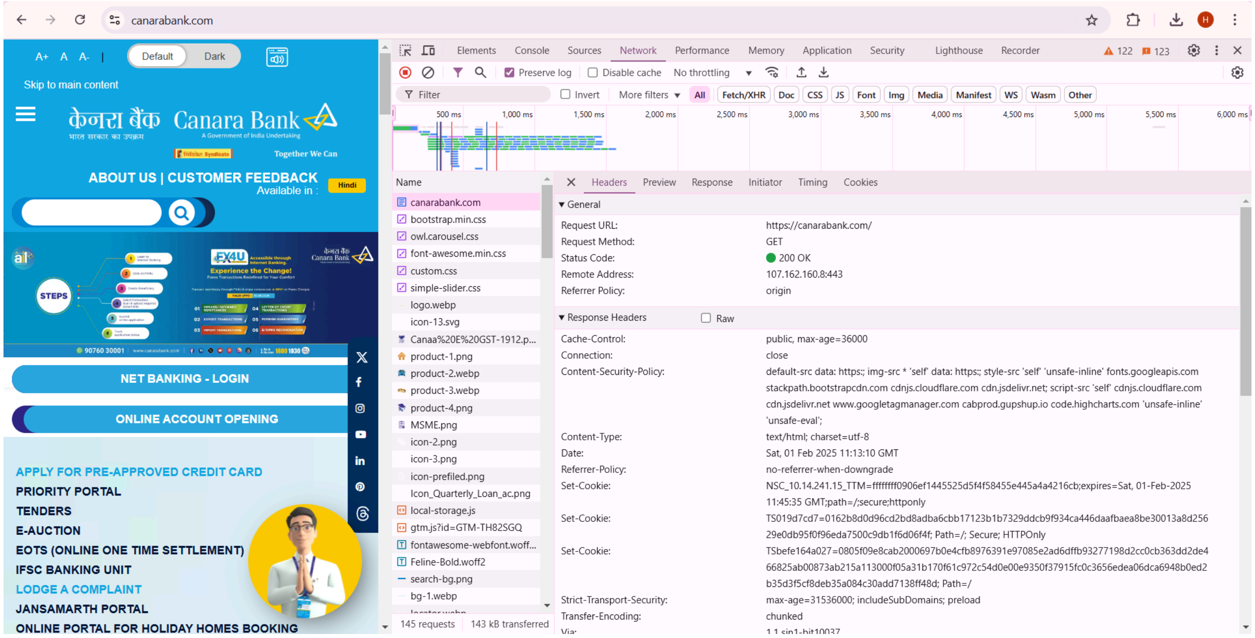
ICMP stands for Internet Control Message Protocol and is a network-layer protocol that is used for diagnostics and error reporting. It allows for the use of tools such as ping and traceroute to check network connectivity and path latency. The ICMP messages that exist are Destination Unreachable, Time Exceeded, and Echo Request/Reply. Although it does not support user-data the fact that it can be helpful in troubleshooting network issues makes it useful.

---

## 9. NBNS (NetBIOS Name Service)

NBNS performs the NetBIOS name to IP mapping in Windows-based network for local networks like DNS. It uses UDP port 137 and is an essential part of NetBIOS over TCP/IP (NBT). In the past, NBNS was widely popular in older Windows systems but now it is by and large replaced by DNS and Active Directory. It is susceptible to spoofing attacks and may face security risks.

**2. Analyze the following details by visiting the following websites in your favourite browser.**
**i) canarabank.in**
**ii) github.com**
**iii) netflix.com**
**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.**

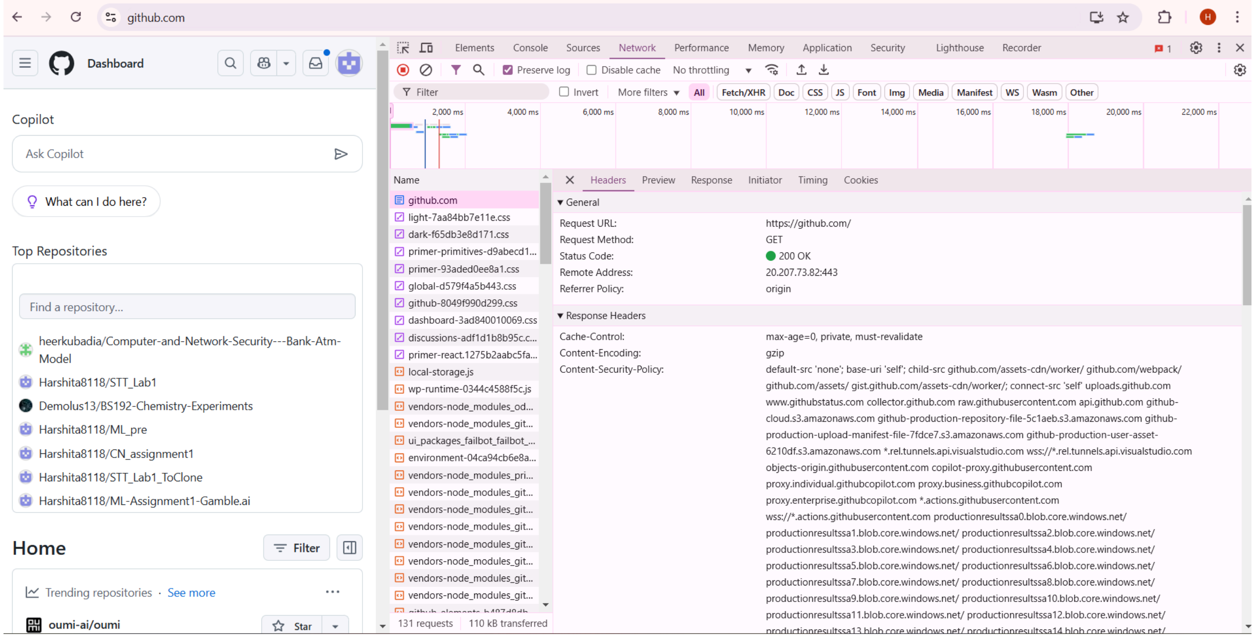


```
Request URL:                 https://canarabank.com/
Request Method:              GET
Status Code:                 ● 200 OK
Remote Address:              107.162.160.8:443
Referrer Policy:             origin

▼ 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 cabprod.gupshup.io code.highcharts.com 'unsafe-inline'
                             'unsafe-eval';
Content-Type:                text/html; charset=utf-8
Date:                        Sat, 01 Feb 2025 11:13:10 GMT
Referrer-Policy:             no-referrer-when-downgrade
Set-Cookie:                  NSC_10.14.241.15_TTM=ffffffff0906ef1445525d5f4f58455e445a4a4216cb;expires=Sat, 01-Feb-2025
                             11:45:35 GMT;path=/;secure;httponly
Set-Cookie:                  TS019d7cd7=0162b8d0d96cd2bd8adba6cbb17123b1b7329ddcb9f934ca446daafbaea8be30013a8d256
                             29e0db95f0f96eda7500c9db1f6d06f4f; Path=/; Secure; HTTPOnly
Set-Cookie:                  TSbefe164a027=0805f09e8cab2000697b0e4cfb8976391e97085e2ad6dffb93277198d2cc0cb363dd2de4
                             66825ab00873ab215a113000f05a31b170f61c972c54d0e00e9350f37915fc0c3656edea06dca6948b0ed2
                             b35d3f5cf8deb35a084c30add7138ff48d; Path=/
Strict-Transport-Security:   max-age=31536000; includeSubDomains; preload
Transfer-Encoding:           chunked
Via:                         1.1 sin1-bit10037
```

```
Name
canarabank.com
bootstrap.min.css
owl.carousel.css
font-awesome.min.css
custom.css
simple-slider.css
logo.webp
icon-13.svg
Canaa%20E%20GST-1912.p...
product-1.png
product-2.webp
product-3.webp
product-4.png
MSME.png
icon-2.png
icon-3.png
icon-prefiled.png
Icon_Quarterly_Loan_ac.png
local-storage.js
gtm.js?id=GTM-TH82SGQ
fontawesome-webfont.woff...
Feline-Bold.woff2
search-bg.png
bg-1.webp
145 requests   143 kB transferred
```

Request line - GET / HTTP/1.1
Layer protocol - HTTP
IP - 107.162.160.8:443
Connection - Persistent


github.com
Dashboard
Copilot
Ask Copilot
What can I do here?
Top Repositories
Find a repository...
heerkubadia/Computer-and-Network-Security---Bank-Atm-Model
Harshita8118/STT_Lab1
Demolus13/BS192-Chemistry-Experiments
Harshita8118/ML_pre
Harshita8118/CN_assignment1
Harshita8118/STT_Lab1_ToClone
Harshita8118/ML-Assignment1-Gamble.ai
Home
Filter
Trending repositories · See more
oumi-ai/oumi
Star
Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder
Preserve log
Disable cache
No throttling
Filter
Invert
More filters
All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other
2,000 ms 4,000 ms 6,000 ms 8,000 ms 10,000 ms 12,000 ms 14,000 ms 16,000 ms 18,000 ms 20,000 ms 22,000 ms
Name
github.com
light-7aa84bb7e11e.css
dark-f65db3e8d171.css
primer-primitives-d9abecd1...
primer-93aded0ee8a1.css
global-d579f4a5b443.css
github-8049f990d299.css
dashboard-3ad840010069.css
discussions-adf1d1b8b95c.c...
primer-react.1275b2aabc5fa...
local-storage.js
wp-runtime-0344c4588f5c.js
vendors-node_modules_od...
vendors-node_modules_git...
ui_packages_failbot_failbot_...
environment-04ca94cb6e8a...
vendors-node_modules_pri...
vendors-node_modules_git...
131 requests
110 kB transferred
Headers Preview Response Initiator Timing Cookies

▼ General

Request URL: https://github.com/
Request Method: GET
Status Code: ● 200 OK
Remote Address: 20.207.73.82:443
Referrer Policy: origin

▼ Response Headers

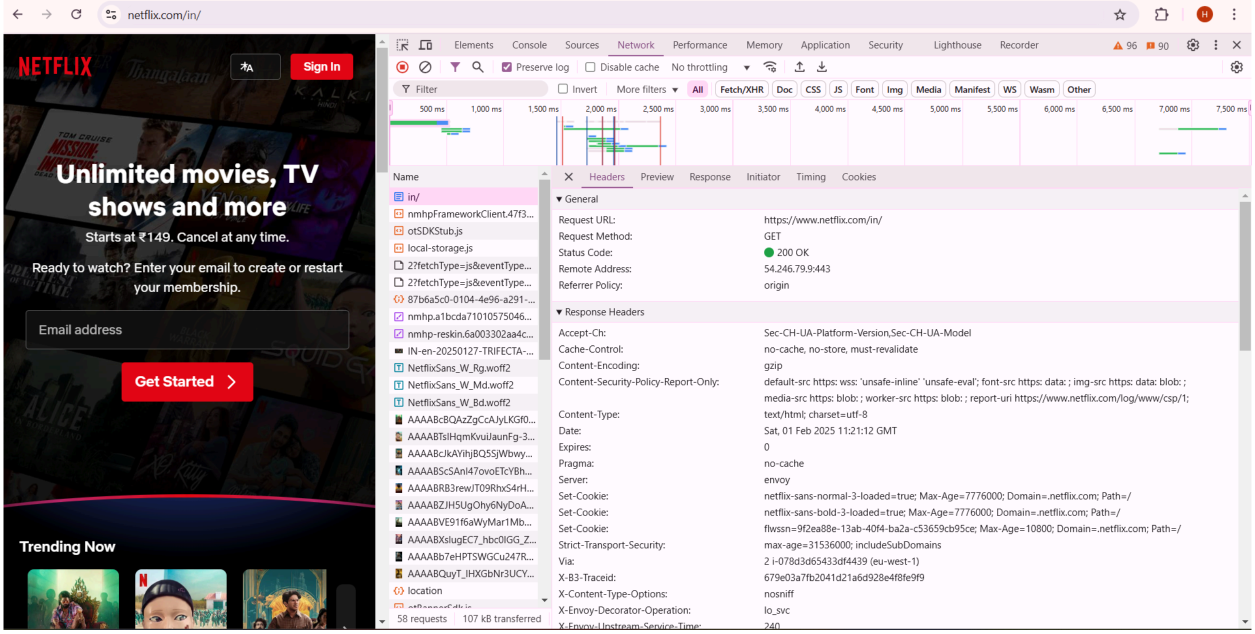
Cache-Control: max-age=0, private, must-revalidate
Content-Encoding: gzip
Content-Security-Policy: default-src 'none'; base-uri 'self'; child-src github.com/assets-cdn/worker/ github.com/webpack/ github.com/assets/ gist.github.com/assets-cdn/worker/; connect-src 'self' uploads.github.com www.githubstatus.com 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 wss://*.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/

Request line - GET /in/ HTTP/1.1

Layer protocol - HTTP

IP - 20.207.73.82:443

Connection - Persistent (by default)


netflix.com/in/
NETFLIX
Sign In
Unlimited movies, TV shows and more
Starts at ₹149. Cancel at any time.
Ready to watch? Enter your email to create or restart your membership.
Email address
Get Started
Trending Now
Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder
96 90
Preserve log
Disable cache
No throttling
Filter
Invert
More filters
All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other
500 ms 1,000 ms 1,500 ms 2,000 ms 2,500 ms 3,000 ms 3,500 ms 4,000 ms 4,500 ms 5,000 ms 5,500 ms 6,000 ms 6,500 ms 7,000 ms 7,500 ms
Name
in/
nmhpFrameworkClient.47f3...
otSDKStub.js
local-storage.js
2?fetchType=js&eventType...
2?fetchType=js&eventType...
87b6a5c0-0104-4e96-a291-...
nmhp.a1bcda71010575046...
nmhp-reskin.6a003302aa4c...
IN-en-20250127-TRIFECTA-...
NetflixSans_W_Rg.woff2
NetflixSans_W_Md.woff2
NetflixSans_W_Bd.woff2
location
58 requests
107 kB transferred
Headers Preview Response Initiator Timing Cookies

▼ General

Request URL: https://www.netflix.com/in/
Request Method: GET
Status Code: ● 200 OK
Remote Address: 54.246.79.9:443
Referrer Policy: origin

▼ Response Headers

Accept-Ch: Sec-CH-UA-Platform-Version,Sec-CH-UA-Model
Cache-Control: no-cache, no-store, must-revalidate
Content-Encoding: gzip
Content-Security-Policy-Report-Only: default-src https: wss: 'unsafe-inline' 'unsafe-eval'; font-src https: data: ; img-src https: data: blob: ; media-src https: blob: ; worker-src https: blob: ; report-uri https://www.netflix.com/log/www/csp/1;
Content-Type: text/html; charset=utf-8
Date: Sat, 01 Feb 2025 11:21:12 GMT
Expires: 0
Pragma: no-cache
Server: envoy
Set-Cookie: netflix-sans-normal-3-loaded=true; Max-Age=7776000; Domain=.netflix.com; Path=/
Set-Cookie: netflix-sans-bold-3-loaded=true; Max-Age=7776000; Domain=.netflix.com; Path=/
Set-Cookie: flwssn=9f2ea88e-13ab-40f4-ba2a-c53659cb95ce; Max-Age=10800; Domain=.netflix.com; Path=/
Strict-Transport-Security: max-age=31536000; includeSubDomains
Via: 2 i-078d3d65433df4439 (eu-west-1)
X-B3-Traceid: 679e03a7fb2041d21a6d928e4f8fe9f9
X-Content-Type-Options: nosniff
X-Envoy-Decorator-Operation: lo_svc
X-Envoy-Upstream-Service-Time: 240

Request line - GET /in/ HTTP/1.1

Layer protocol - HTTP

IP - 54.246.79.9:443

Connection - Persistent (by default)

**b. For any one of the websites, list any three header field names and corresponding values in the request and response message. Any three HTTP error codes obtained while loading one of the pages with a brief description.**

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

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

referer:https://www.google.com/

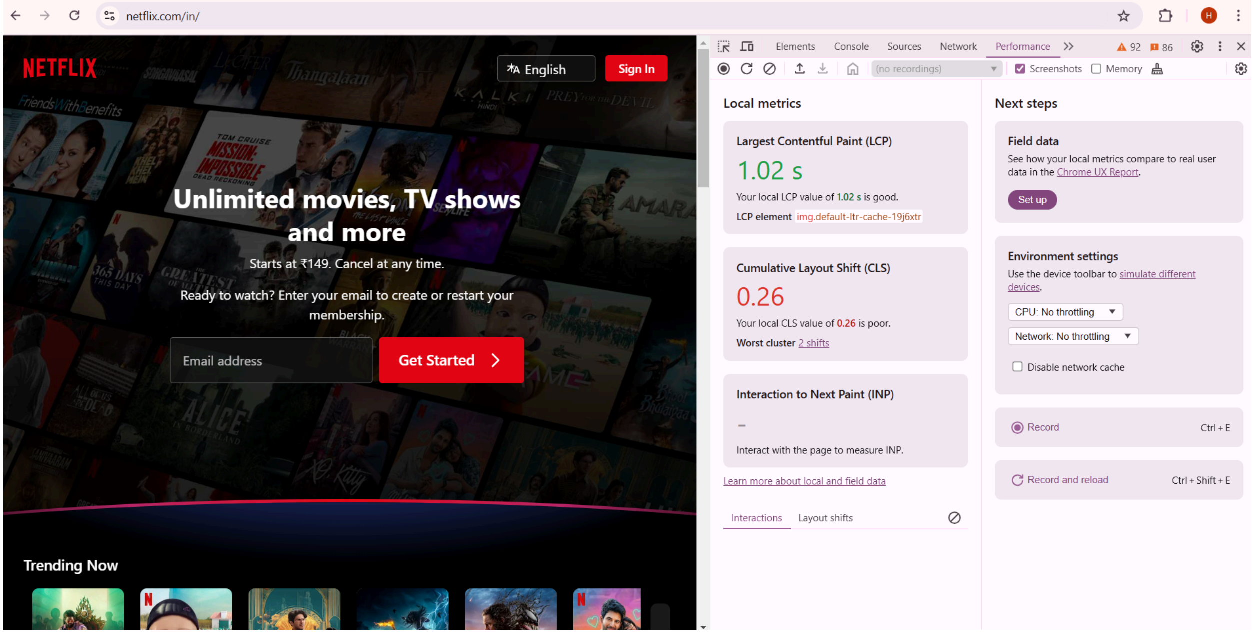
Errors:

404 Not Found: This error occurs when the server cannot find the requested resource. It typically happens when the URL is incorrect or the page has been removed. It's one of the most common errors users encounter when navigating websites.

500 Internal Server Error: This error indicates that something has gone wrong on the server's side, preventing it from fulfilling the request. It is a general-purpose error, often pointing to issues such as server misconfigurations or unhandled exceptions in the server's code.

403 Forbidden: This error occurs when the server understands the request but refuses to authorize it. It typically happens when a user doesn't have the necessary permissions to access the resource, such as when trying to access a restricted page or a private file without the appropriate credentials.

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.



Local metrics

Largest Contentful Paint (LCP)

1.02 s

Your local LCP value of 1.02 s is good.

LCP element img.default-ltr-cache-19j6xtr

Cumulative Layout Shift (CLS)

0.26

Your local CLS value of 0.26 is poor.

Worst cluster 2 shifts

Interaction to Next Paint (INP)

–

Interact with the page to measure INP.

Learn more about local and field data

Interactions | Layout shifts

Next steps

Field data

See how your local metrics compare to real user data in the Chrome UX Report.

Set up

Environment settings

Use the device toolbar to simulate different devices.

CPU: No throttling

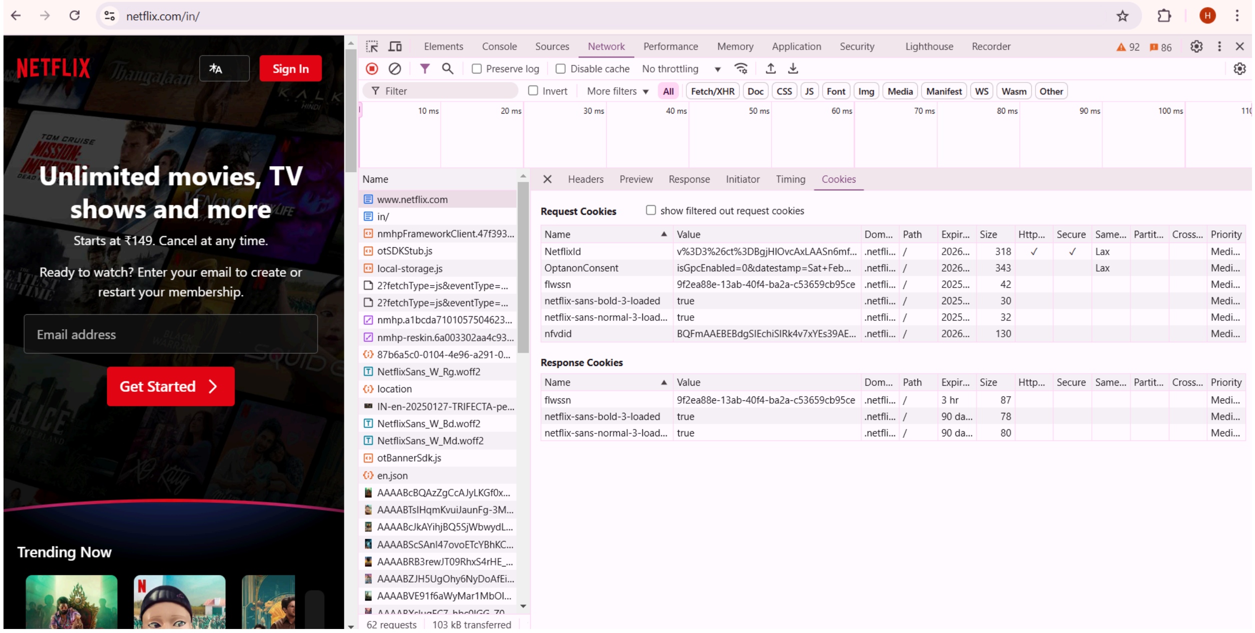
Network: No throttling

□ Disable network cache

Record Ctrl + E

Record and reload Ctrl + Shift + E

The cookies used can be seen in cookies tab-



Name

www.netflix.com
in/
nmhpFrameworkClient.47f393...
otSDKStub.js
local-storage.js
2?fetchType=js&eventType=...
2?fetchType=js&eventType=...
nmhp.a1bcda7101057504623...
nmhp-reskin.6a003302aa4c93...
87b6a5c0-0104-4e96-a291-0...
NetflixSans_W_Rg.woff2
location
IN-en-20250127-TRIFECTA-pe...
NetflixSans_W_Bd.woff2
NetflixSans_W_Md.woff2
otBannerSdk.js
en.json
AAAABcBQAzZgCcAJyLKGf0x...
AAAABTsIHqmKvuiJaunFg-3M...
AAAABcJkAYihjBQ5SjWbwydL...
AAAABScSAnl47ovoETcYBhKC...
AAAABRB3rewJT09RhxS4rHE_...
AAAABZJH5UgOhy6NyDoAfEi...
AAAABVE91f6aWyMar1MbOl...

62 requests | 103 kB transferred

Headers | Preview | Response | Initiator | Timing | Cookies

**Request Cookies** □ show filtered out request cookies

| Name ▲ | Value | Dom... | Path | Expir... | Size | Http... | Secure | Same... | Partit... | Cross... | Priority |
|---|---|---|---|---|---|---|---|---|---|---|---|
| NetflixId | v%3D3%26ct%3DBgjHIOvcAxLAASn6mf... | .netfli... | / | 2026... | 318 | ✓ | ✓ | Lax | | | Medi... |
| OptanonConsent | isGpcEnabled=0&datestamp=Sat+Feb... | .netfli... | / | 2026... | 343 | | | Lax | | | Medi... |
| flwssn | 9f2ea88e-13ab-40f4-ba2a-c53659cb95ce | .netfli... | / | 2025... | 42 | | | | | | Medi... |
| netflix-sans-bold-3-loaded | true | .netfli... | / | 2025... | 30 | | | | | | Medi... |
| netflix-sans-normal-3-load... | true | .netfli... | / | 2025... | 32 | | | | | | Medi... |
| nfvdid | BQFmAAEBEBdgSIEchiSIRk4v7xYEs39AE... | .netfli... | / | 2026... | 130 | | | | | | Medi... |

**Response Cookies**

| Name ▲ | Value | Dom... | Path | Expir... | Size | Http... | Secure | Same... | Partit... | Cross... | Priority |
|---|---|---|---|---|---|---|---|---|---|---|---|
| flwssn | 9f2ea88e-13ab-40f4-ba2a-c53659cb95ce | .netfli... | / | 3 hr | 87 | | | | | | Medi... |
| netflix-sans-bold-3-loaded | true | .netfli... | / | 90 da... | 78 | | | | | | Medi... |
| netflix-sans-normal-3-load... | true | .netfli... | / | 90 da... | 80 | | | | | | Medi... |