CS 331 - Computer Networks

Assignment 1

Guntas Singh Saran *22110089*

Hitesh Kumar *22110098*

Group 9

0.pcap

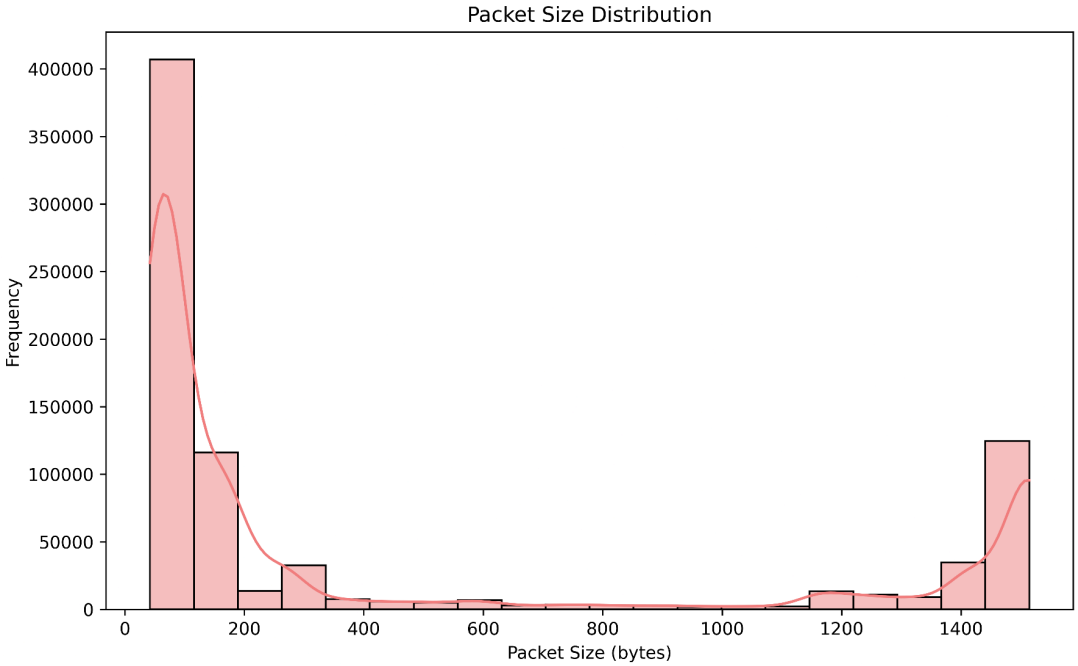
Raw Sockets

GitHub Repository Link: https://github.com/Hit2737/CN_A1

Part 1: Metrics and Plots

1. Data and Packet Metrics

- Total Data Transferred (in bytes): *364641929 bytes*
- Total Number of Packets Transferred: *805995*
- Minimum Packet Size: *42 bytes*
- Maximum Packet Size: *1514 bytes*
- Average Packet Size: *452.41 bytes*
- Packet Size Distribution



--- Packet Size Distribution Percentiles ---

50th percentile: 106.0 bytes

75th percentile: 868.0 bytes

90th percentile: 1514.0 bytes

95th percentile: 1514.0 bytes

99th percentile: 1514.0 bytes

Most packets lie between 60.0 and 868.0 bytes

2. Unique Source-Destination Pairs

- **Unique Source-Destination Pairs:**
  - List of unique *source IP: port* and *destination IP: port* pairs

Detailed view at [packet_flow.json]. These are some overall results:

"172.16.133.95:49358 → 157.56.240.102:443": 17342229,

"172.16.133.57:53807 → 68.64.21.62:1853": 17318420,

"172.16.133.36:64953 → 67.217.64.99:443": 15842153,

"67.217.64.99:443 → 172.16.133.26:53037": 14997326,

"172.16.128.201:1060 → 172.16.133.6:1731": 5264163,

"74.125.170.143:80 → 172.16.133.73:60658": 4718677,

"132.245.1.150:443 → 172.16.133.39:49311": 4635684,

……

……

"208.88.186.242:13392 → 172.16.255.1:50983": 60,

"172.16.255.1:50983 → 69.126.180.28:443": 60,

"192.168.3.131:57058 → 65.55.57.251:5480": 54,

"192.168.3.131:57058 → 65.55.57.251:80": 54,

"10.0.2.15:2489 → 65.55.25.60:5480": 54,

"10.0.2.15:2489 → 65.55.25.60:80": 54

  - Source-Destination pair with most data:

    172.16.133.95:49358 → 157.56.240.102:443 (***17342229 bytes***)

3. IP Address Flow Metrics

- **Dictionary of IP Addresses as Sources:**
  - Detailed view at src_flows.json
- **Dictionary of IP Addresses as Destinations:**
  - Detailed view at dst_flows.json
- **Source-Destination Pair with Most Data Transferred:**
  - 172.16.133.95:49358 → 157.56.240.102:443
  - 17342229 bytes

4. Capture Speed Metrics

To achieve this, we first ran **tcpreplay** on the **loopback interface** at some **high pps=10000** and got the time needed to send all 0.pcap packets (**80.59s**), and then we ran our sniffer with this similar timeout alongside tcpreplay to simulate the actual traffic of packets and then all our results are computed in this manner.

```
~/CN_A1 python3 sniffer_speed.py -i lo0 -t <timeout> -q <question-number>
```

```
~/CN_A1 sudo tcpreplay -i lo0 --pps=<pps> 0.pcap
```

So we ran our tests for **pps=[10000, 5000, 2500, 2000, 1900]** with each time finding the timeout by unitary method since at 10,000 pps we needed 81s to replay all packets using tcpreplay, we found the timeouts of the rest similarly as **timeout=[81s, 162s, 324s, 403s, 425s]**. We found that at

> **--pps=1900** packets per second or **--mbps=6.87,** we were able to transfer all packets with no loss taking around **--timeout=425**.

- **Top Speed (pps and mbps) Without Packet Loss:**
  - **Case 1:** Running tcpreplay and sniffer on the same machine (VM):

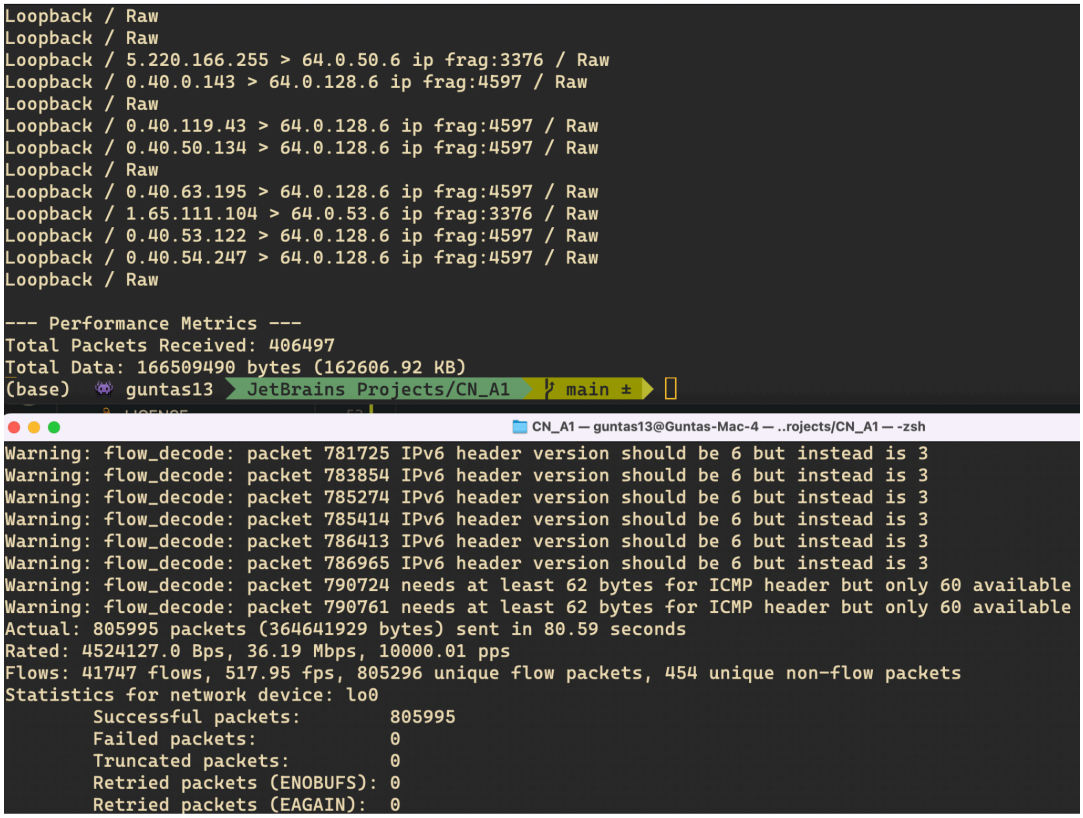


*Fig: tcpreplay at **pps=10,000** and sniffer being able to capture only half of packets.*

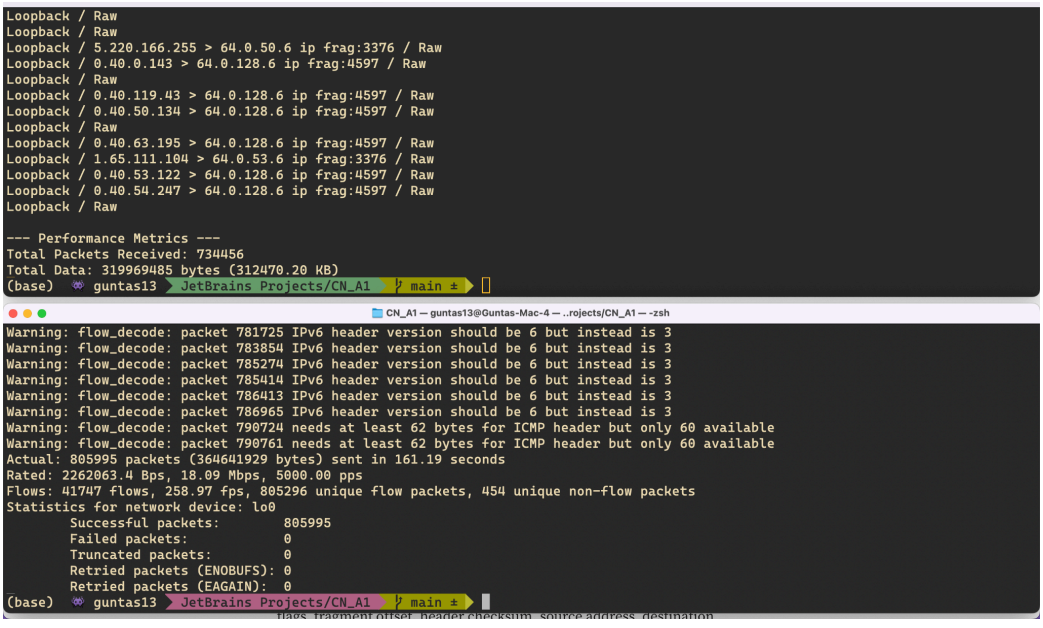


*Fig: tcpreplay at **pps=5000** and sniffer capturing **734456 out of 805995** packets*

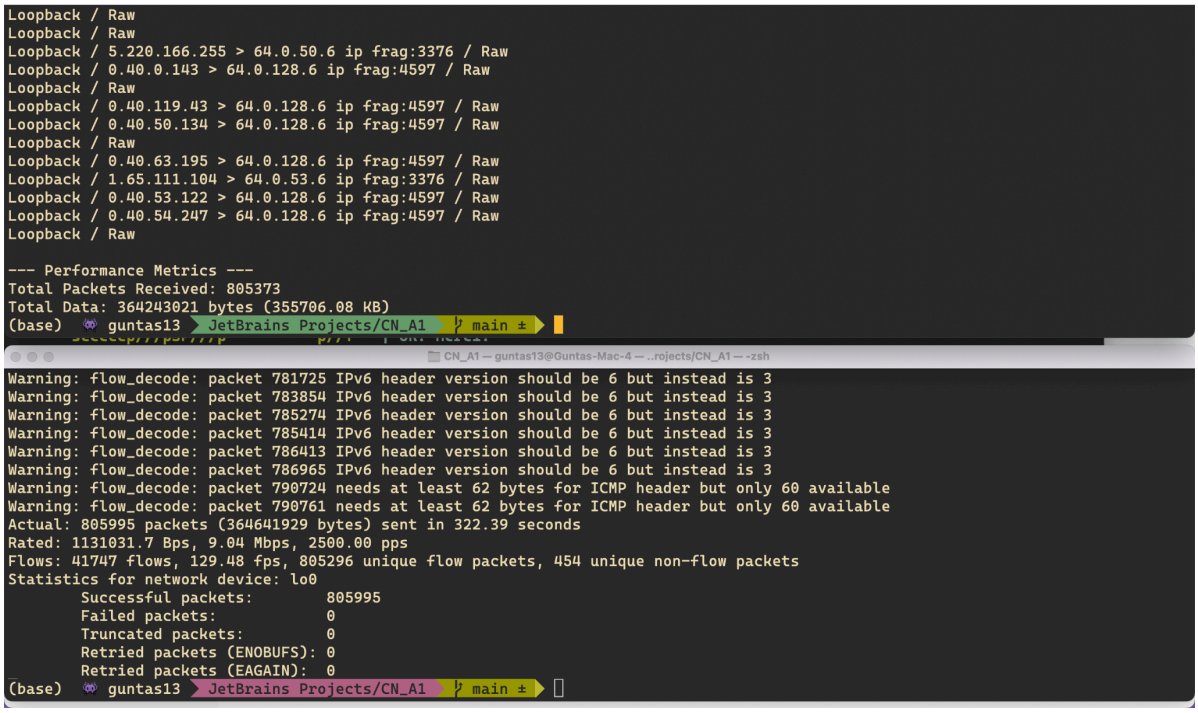


*Fig: tcpreplay at **pps=2500** and sniffer capturing **805373 out of 805995** packets.*

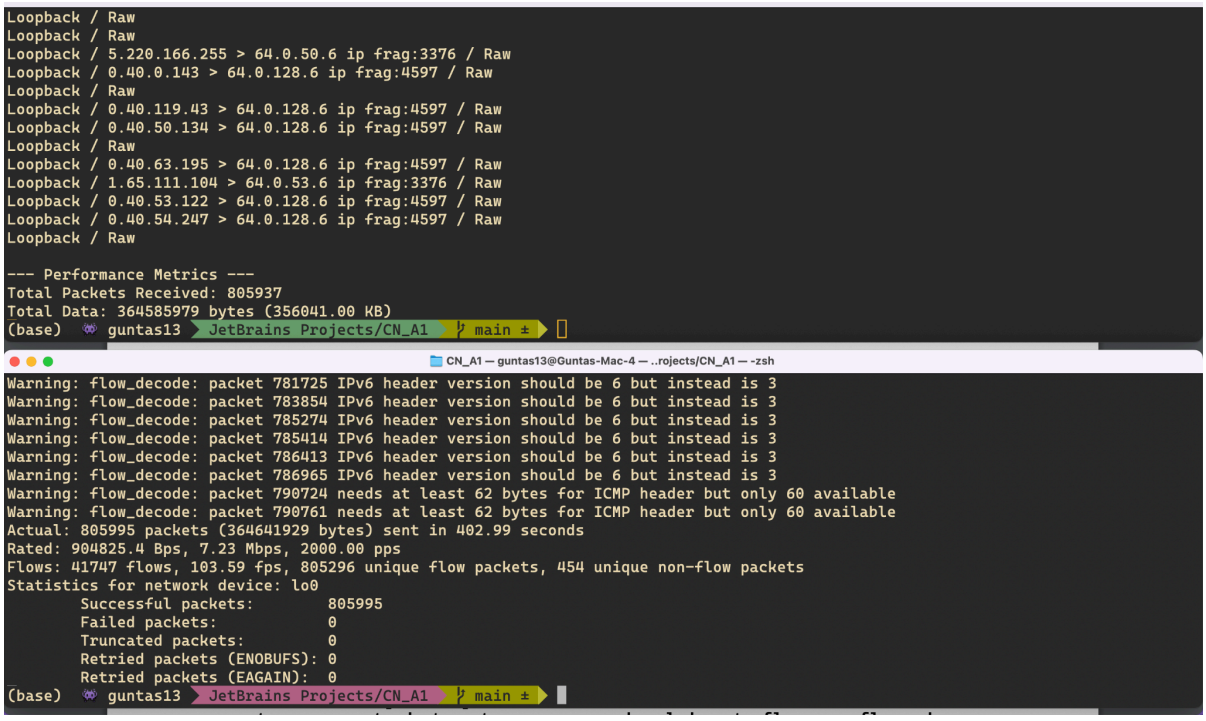


*Fig: tcpreplay at **pps=2000** and sniffer capturing **805937 out of 805995** packets.*

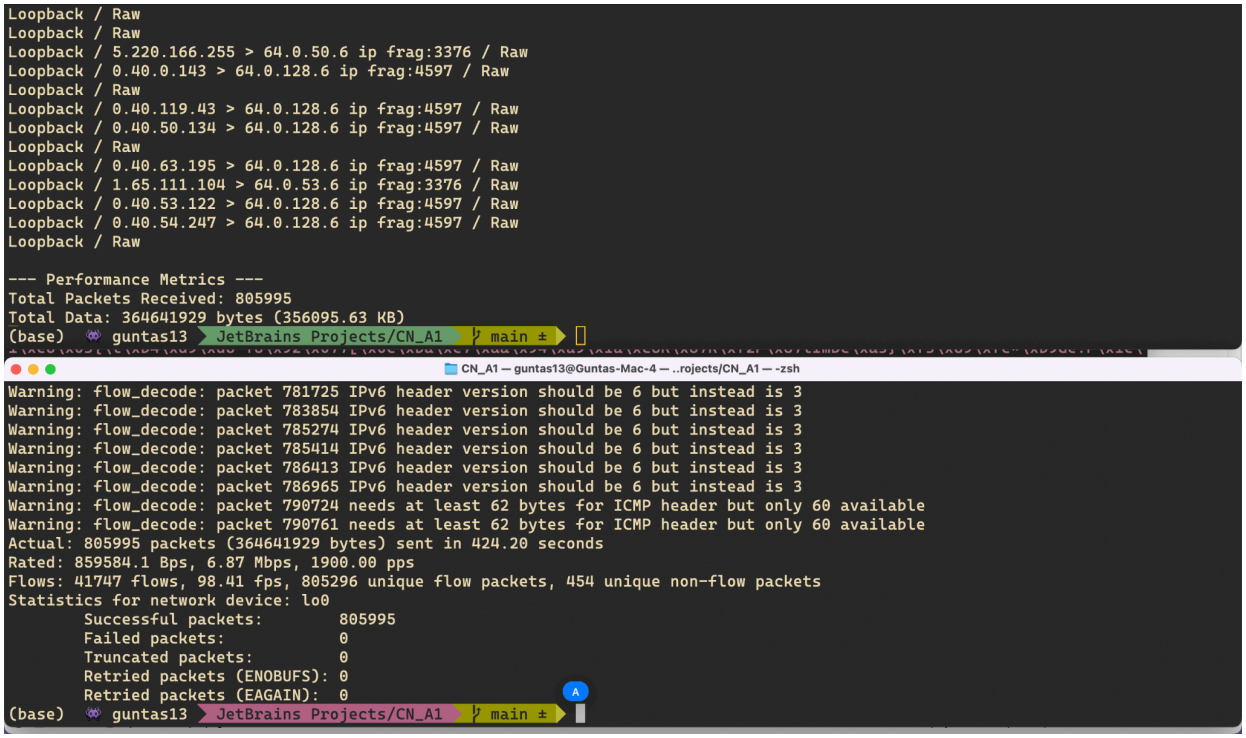


*Fig: **tcpreplay at pps=1900 and sniffer capturing all of 805995 packets with no loss***

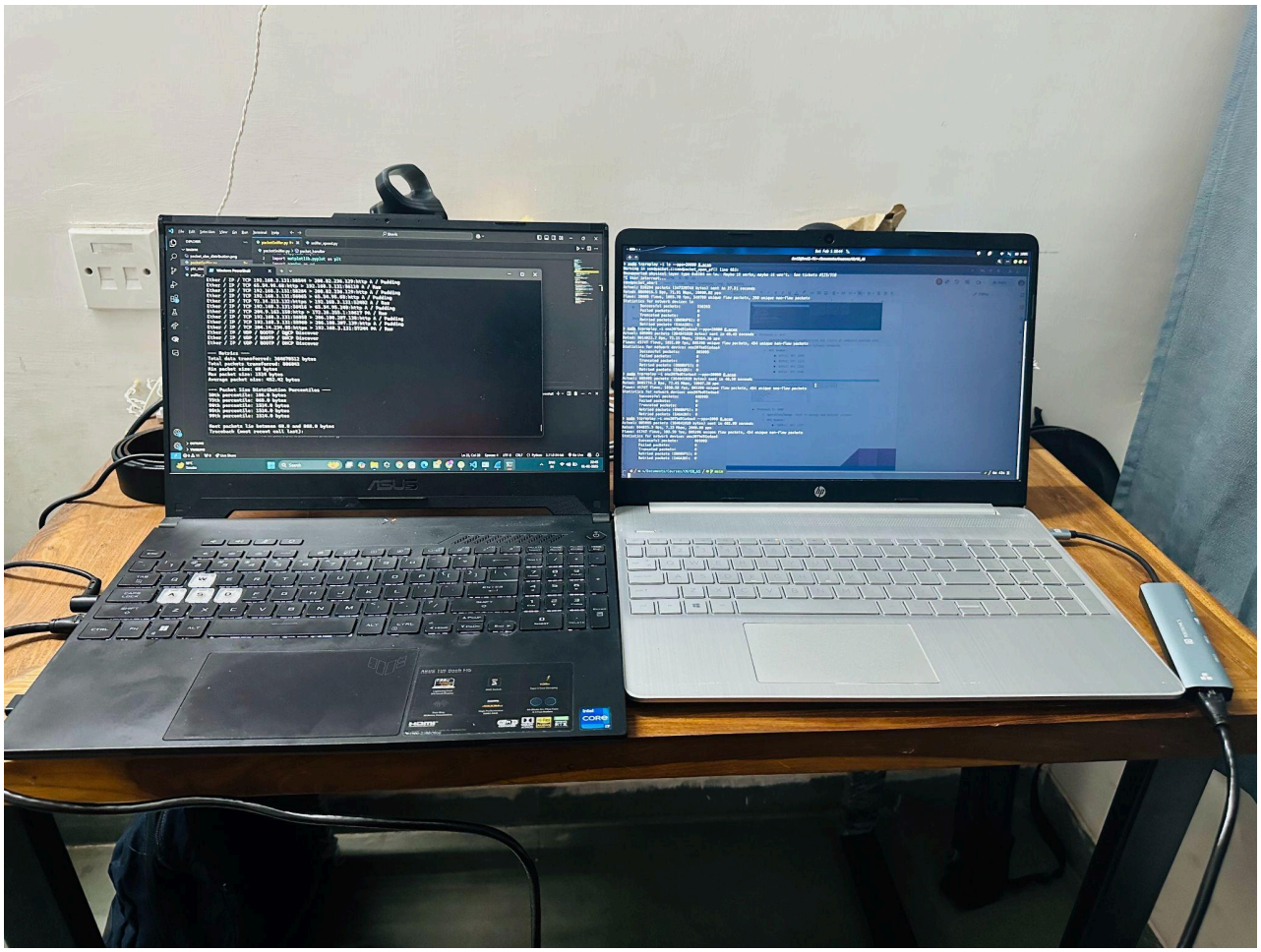
```python
# mDNS (Multicast DNS) uses 224.0.0.251 (IPv4) and ff02::fb (IPv6) on UDP port 5353.
    # To filter out mDNS packets, we add checks for:

    # IPv4: packet[IP].dst == "224.0.0.251"
    # IPv6: packet[IPv6].dst == "ff02::fb"
    # UDP Port 5353: packet[UDP].dport == 5353

def traffic_packet(packet):
    """Filters out localhost and multicast traffic"""
    if IP in packet and (packet[IP].src == "127.0.0.1" or packet[IP].dst == "127.0.0.1"):
        return True
    if IPv6 in packet and (packet[IPv6].src == "::1" or packet[IPv6].dst == "::1"):
        return True
    if (IP in packet and packet[IP].dst == "224.0.0.251") or (IPv6 in packet and packet[IPv6].dst == "ff02::fb"):
        return True
    if UDP in packet and packet[UDP].dport == 5353:
        return True
    return False
```

Fig: Code to filter out the traffic of Mac Os's LoopBack lo0

- **Case 2:** Running tcpreplay and sniffer on different machines (physical or VMs): Running on the Ethernet interface on two different hosts using an Ethernet Cable - We achieved similar speed itself - only a marginal increase to `--pps=2000`

```
~/Documents/Courses/CN/CN_A1 / main
sudo tcpreplay -i enx207bd51a4aa4 --pps=2000 0.pcap
```

```
Windows PowerShell
PS C:\Users\91942\Downloads\Bhavik> python .\sniffer_speed.py -i Ethernet -q 1 -t 430
```



Part 2: Catch Me If You Can

PCAP Specific Questions

```
----------Summary-----------
Q1: Unique Packets Destined to IMS server: 30
Q2: Course registered on IMS is:
course = Embedded_system
Q3: Total data transferred on port 4321: 2970 bytes
Q4: Total number of SuperUsers: 69

---------------------------
```

The code is to query all the CTF questions as we replay the packets.

```
IPv = IP if IP in packet else IPv6 if IPv6 in packet else None
if IPv and IPv in packet:
    src_ip = packet[IPv].src
    dst_ip = packet[IPv].dst

    if dst_ip == ims_ip:
        ims_dst_packets.append(packet)
        all_ims_packets.append(packet)

    if src_ip == ims_ip:
        all_ims_packets.append(packet)

    protocol = TCP if TCP in packet else UDP if UDP in packet else None
    if protocol:
        src_port = packet[protocol].sport
        dst_port = packet[protocol].dport
        if dst_ip == ims_ip:
            unique_conn_to_ims[f"{src_ip}:{src_port} -> {dst_ip}:{dst_port}"] += 1

    if protocol and (packet[protocol].sport == 4321 or packet[protocol].dport == 4321):
        port_packets.append(packet)

    if Raw in packet:
        payload = packet[Raw].load.decode(errors='ignore')
        if "superuser" in payload.lower():
            super_users += 1
            superuser_packets.append(packet)
```

Question 1: How many unique connections were made to the IMS server?

➔ **There's only 1 unique connection to the IMS server** (dst_ip = **10.0.137.79**). However, in all, **30** such connections were made.

```
Unique connections to IMS server (with their connection counts):
defaultdict(<class 'int'>, {'10.1.12.123:1234 -> 10.0.137.79:4321': 30})
```

```
All packets destined to IMS server:
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
```

Question 2: I have registered for a course in IMS. What course did I register for?

➔ The course was ***Embedded System.*** The packet is listed below:

➔ <Ether dst=66:77:88:99:aa:bb src=00:11:22:33:44:55 type=IPv4 | <IP version=4 ihl=5 tos=0x0 len=64 id=1 flags= frag=0 ttl=64 proto=tcp chksum=0xd0ec src=10.0.137.79 dst=10.1.12.123 | <TCP sport=rwhois dport=search_agent seq=0 ack=0 dataofs=5 reserved=0 flags=S window=8192 chksum=0x5b9c urgptr=0 | <Raw load=b'**course = Embedded_system**' |>>>>

```
###[ Ethernet ]###
  dst       = 66:77:88:99:aa:bb
  src       = 00:11:22:33:44:55
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 64
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xd0ec
     src       = 10.0.137.79
     dst       = 10.1.12.123
     \options   \
###[ TCP ]###
        sport     = rwhois
        dport     = search_agent
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
...
        options   = []
###[ Raw ]###
           load      = b'course = Embedded_system'
```

Question 3: What is the total amount of data (in bytes) transferred over a port 4321?

- ➔ **2970 bytes** for **52 such packets.**

```
All packets transferred on port 4321 (both src and dst):
Ether / IP / UDP 172.16.128.169:rwhois > 172.16.133.248:snmp / SNMP
Ether / IP / UDP 172.16.133.248:snmp > 172.16.128.169:rwhois / SNMP
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S / Raw
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.1.12.123:search_agent > 10.0.137.79:rwhois S
Ether / IP / TCP 10.0.137.79:rwhois > 10.1.12.123:search_agent S
```

Question 4: There are many Superusers. Find how many SuperUsers are there.

→ 69 superusers.

```
0 |<Raw  load=b'I am superuser 35' |>>>>,
 |<Raw  load=b'I am superuser 30' |>>>>,
btr=0 |<Raw  load=b'I am superuser 33' |>>>>,
r=0 |<Raw  load=b'I am superuser 8' |>>>>,
0 |<Raw  load=b'I am superuser 6' |>>>>,
=0 |<Raw  load=b'I am superuser 39' |>>>>,
btr=0 |<Raw  load=b'I am superuser 17' |>>>>,
tr=0 |<Raw  load=b'I am superuser 61' |>>>>,
r=0 |<Raw  load=b'I am superuser 7' |>>>>,
=0 |<Raw  load=b'I am superuser 20' |>>>>,
r=0 |<Raw  load=b'I am superuser 21' |>>>>,
tr=0 |<Raw  load=b'I am superuser 27' |>>>>,
0 |<Raw  load=b'I am superuser 57' |>>>>,
=0 |<Raw  load=b'I am superuser 40' |>>>>,
r=0 |<Raw  load=b'I am superuser 25' |>>>>,
0 |<Raw  load=b'I am superuser 51' |>>>>,
tr=0 |<Raw  load=b'I am superuser 34' |>>>>,
0 |<Raw  load=b'I am superuser 18' |>>>>,
0 |<Raw  load=b'I am superuser 23' |>>>>,
tr=0 |<Raw  load=b'I am superuser 47' |>>>>,
=0 |<Raw  load=b'I am superuser 32' |>>>>,
0 |<Raw  load=b'I am superuser 56' |>>>>,
btr=0 |<Raw  load=b'I am superuser 37' |>>>>,
=0 |<Raw  load=b'I am superuser 53' |>>>>,
urgptr=0 |<Raw  load=b'I am superuser 65' |>>>>,
```

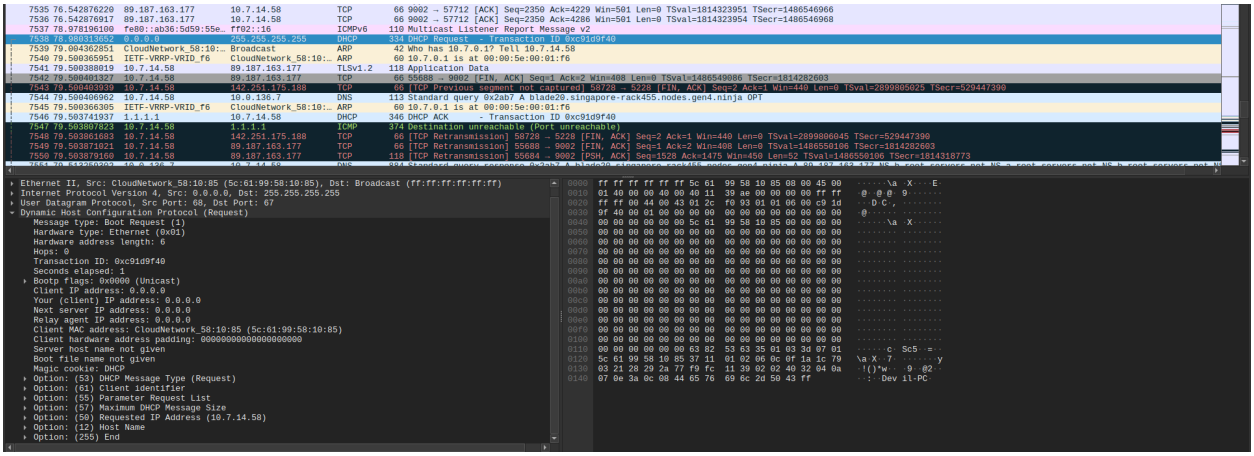
```
###[ Ethernet ]###
  dst       = 66:77:88:99:aa:bb
  src       = 00:11:22:33:44:55
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 57
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xfc7a
     src       = 192.168.67.2
     dst       = 192.168.185.240
     \options   \
###[ TCP ]###
        sport     = 35083
        dport     = idrs
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
...
        options   = []
###[ Raw ]###
           load      = b'I am superuser 35'
```

Part 3: Capture the Packets

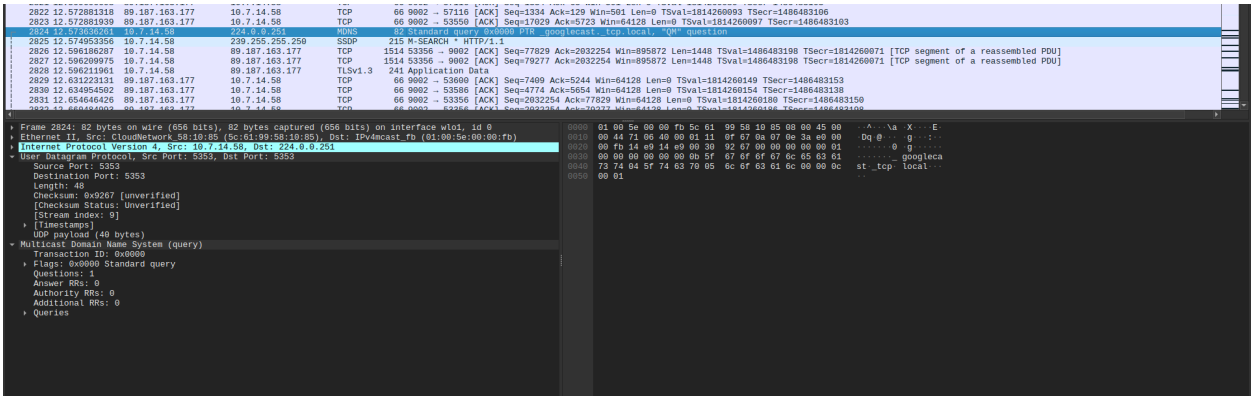
1. Wireshark Capture and Analysis

List of 5 Different Application Layer Protocols:

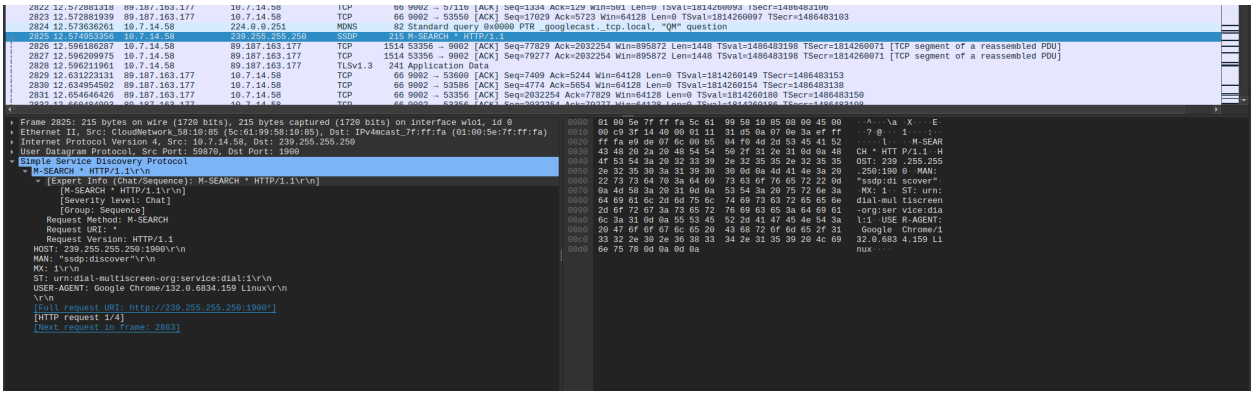
- Protocol 1: **DHCP (Dynamic Host Configuration Protocol)**
  - **Operation/Usage:** Dynamically assigns IP addresses and network configuration parameters to hosts.
  - **RFC Number:** RFC 2131



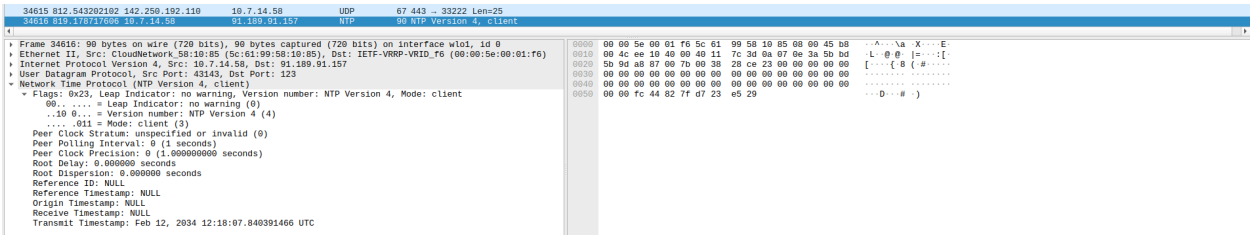
- Protocol 2: **mDNS (Multicast Domain Name System)**
  - **Operation/Usage:** Resolves hostnames to IP addresses on local networks without requiring a dedicated DNS server.
  - **RFC Number:** RFC 6762



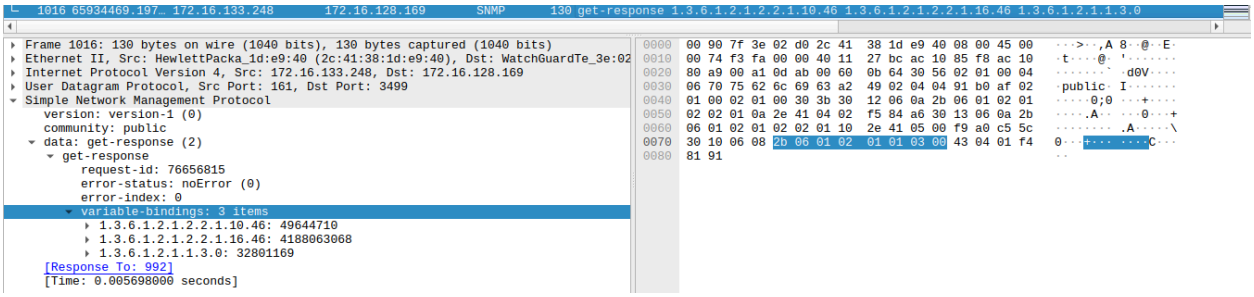
- Protocol 3: **SSDP (Simple Service Discovery Protocol)**
  - **Operation/Usage:** Discovers and advertises network services and devices, typically used in UPnP environments.
  - **RFC Number:** [RFC]



- Protocol 4: **NTP (Network Time Protocol)**
  - **Operation/Usage:** Synchronizes the clocks of computer systems over packet-switched, variable-latency networks.
  - **RFC Number:** NTPv4: [RFC 5905]



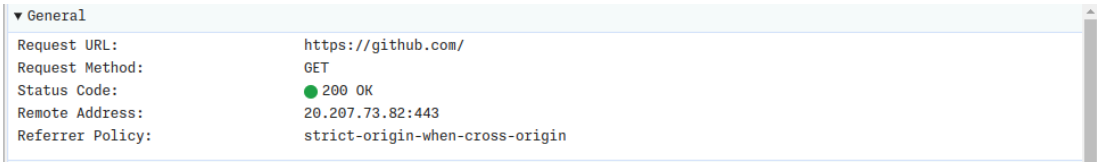
- Protocol 5: **SNMP (Simple Network Management Protocol)**
  - **Operation/Usage:** Used to manage and monitor network
  - **RFC Number:** SNMPv1: [RFC 1157]



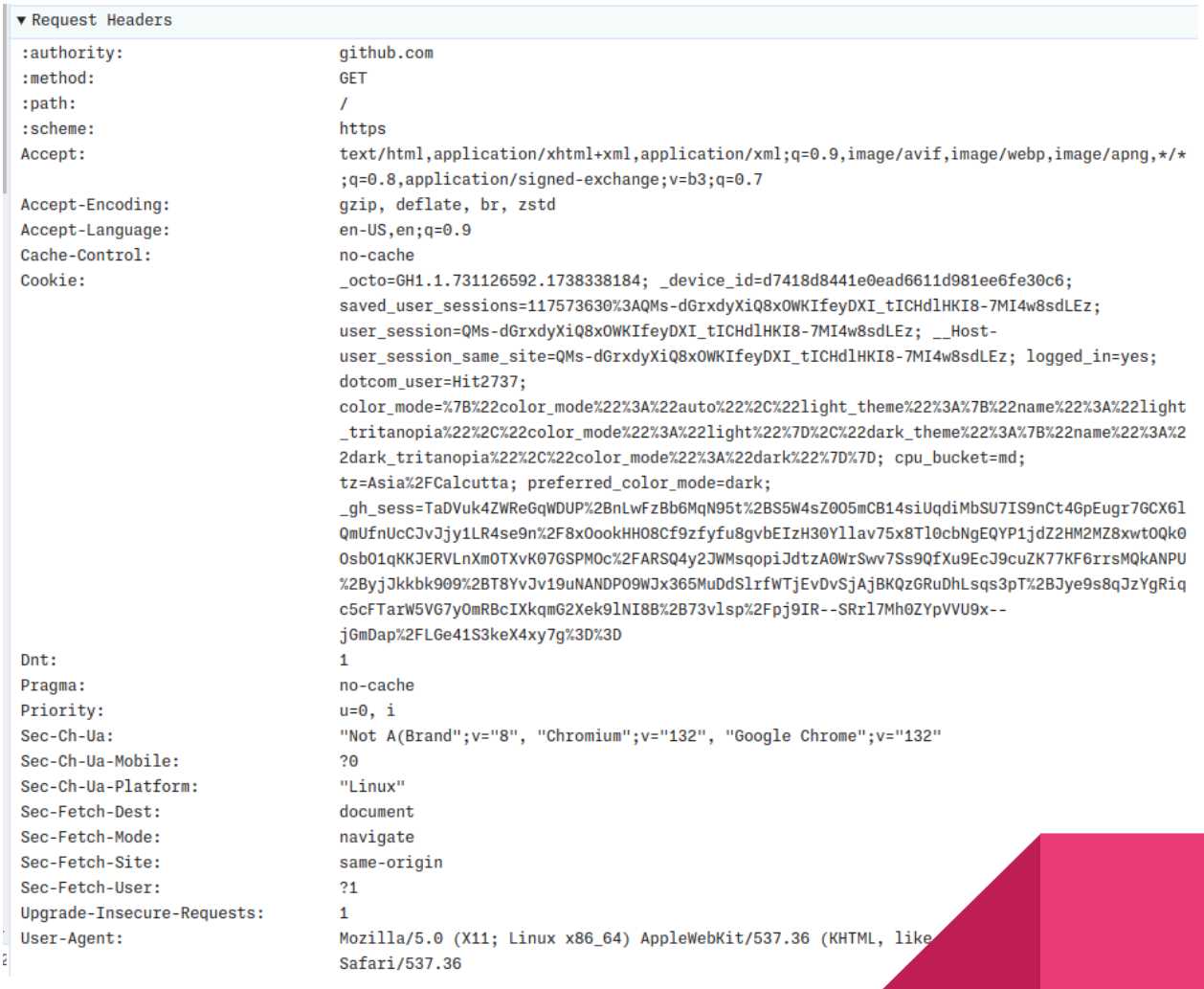
2. Website Analysis

Browser Used: **Google Chrome**

- **Website 1: github.com (20.207.73.82)**
    - Request Line:



    - Connection Type: Persistent
    - Header Fields:
        - Request Header:



- **Response Header:**

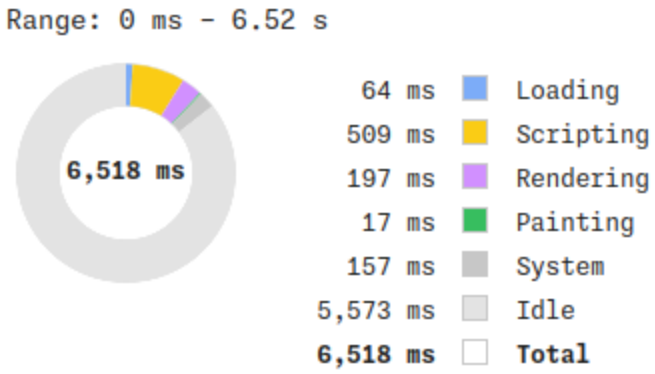
▼ Response Headers

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/

...

Content-Type:	text/html; charset=utf-8
Date:	Sat, 01 Feb 2025 12:17:27 GMT
Etag:	W/"1152c5cddfc9a24fb56c6935c3f50ad3"
Referrer-Policy:	origin-when-cross-origin, strict-origin-when-cross-origin
Server:	GitHub.com
Set-Cookie:	_gh_sess=OlOCnrw8vbi6uGg89ix9dbZbBrd90Cv8adcxI%2BGAPCCPnbutuPMco7mhTVp1AAyaQFpu%2BrtnGdCWEW1yg9X0jxt4Cu%2F6Guqo17iO9XNKbehuTWAs%2FAeUYgLtBG0ce6u53zPQJHvh%2Bt6X0fKXWP%2BzprHGTFiS0W7hznRIMHhCgceCsxuGGz7c9xNCoUa53mhMAum32bvGrUbANjfX8lFxFZEbBmSXEe7zhY3QSJRXty0Z%2FoxG54DLSznh7J%2FSsctvYbq3W5TCYeYEO%2Bj4LVU1p8uJ4T2bFHPIoE7ubwSwloLnsMsv1ish74uLDH%2BEvauY8JjcgEI2ZkG9wvQssaZNZfD5Ywfr28M4hZJw31LL2x%2F%2BQdhCauNnPwF%2FLG96KPgo--q9HxriwYFw77GBOd--himlYDzrvT9s%2BL2AKGm07w%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
X-Content-Type-Options:	nosniff
X-Frame-Options:	deny
X-Github-Request-Id:	9325:0A3C:109E50D:149CF38:679E10D5
X-Xss-Protection:	0

- **Performance Metrics:**



- ## Cookies and Flags:

Request Cookies ☐ show filtered out request cookies

Name ▲	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Partiti…	Cross…	Priority
__Host-user_session_same_site	QMs-dGrxdyXiQ8xOWKIfeyDXI_tICHdlHKI8-7MI4w8sdLEz	github.c…	/	2025-02-14T22:12:03.864Z	77	✓	✓	Strict			Medium
_device_id	d7418d8441e0ead6611d981ee6fe30c6	github.c…	/	2026-01-31T22:11:41.357Z	42	✓	✓	Lax			Medium
_gh_sess	TaDVuk4ZWReGqWDUP%2BnLwFzBb6MqN95t%2BS5W4sZOO5mCB14…	github.c…	/	Session	460	✓	✓	Lax			Medium
_octo	GH1.1.731126592.1738338184	.github.…	/	2026-01-31T15:43:04.388Z	31		✓	Lax			Medium
color_mode	%7B%22color_mode%22%3A%22auto%22%2C%22light_theme%2…	.github.…	/	Session	236		✓	Lax			Medium
cpu_bucket	md	.github.…	/	Session	12		✓	Lax			Medium
dotcom_user	Hit2737	.github.…	/	2026-01-31T22:12:03.864Z	18	✓	✓	Lax			Medium
logged_in	yes	.github.…	/	2026-01-31T22:12:03.864Z	12	✓	✓	Lax			Medium
preferred_color_mode	dark	.github.…	/	Session	24		✓	Lax			Medium
saved_user_sessions	117573630%3AQMs-dGrxdyXiQ8xOWKIfeyDXI_tICHdlHKI8-7M…	github.c…	/	2025-05-01T22:12:03.864Z	79	✓	✓	Lax			Medium
tz	Asia%2FCalcutta	.github.…	/	Session	17		✓	Lax			Medium
user_session	QMs-dGrxdyXiQ8xOWKIfeyDXI_tICHdlHKI8-7MI4w8sdLEz	github.c…	/	2025-02-14T22:12:03.864Z	60	✓	✓	Lax			Medium

Response Cookies

Name ▲	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Partiti…	Cross…	Priority
_gh_sess	OlOCnrw8vbi6uGg89ix9dbZbBrd90Cv8adcxI%2BGAPCCPnbutu…	github.c…	/	Session	509	✓	✓	Lax			Medium

- **Website 2: netflix.com (3.251.50.149)**
    - Request Line:
        - For the first request ⟶
        - For the other requests to get the js, css, files and images etc.

Request URL:	https://www.netflix.com/in/
Request Method:	GET
Status Code:	200 OK
Remote Address:	207.45.73.1:443
Referrer Policy:	strict-origin-when-cross-origin

```
GET /dnm/api/v6/mAcAr9TxZIVbINe88xb3Teg5_OA/AAAABcBQAzZgCcAJyLKGf0x3EjJHKr1h1oCRUQDfVspaHXampP-RjiOkIRlWBz7ViFOvUI1EdPSRcxoOPmB7paPLi52W4OmQZJ4NDMQ.webp?r=a92 HTTP/1.1
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cache-Control: no-cache
Connection: keep-alive
DNT: 1
Host: occ-0-4875-2164.1.nflxso.net
Pragma: no-cache
Referer: https://www.netflix.com/
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
```

- **Connection Type:** Persistent (keep-alive)
- **Header Fields:**
    - **Request Header:**

▼ Request Headers

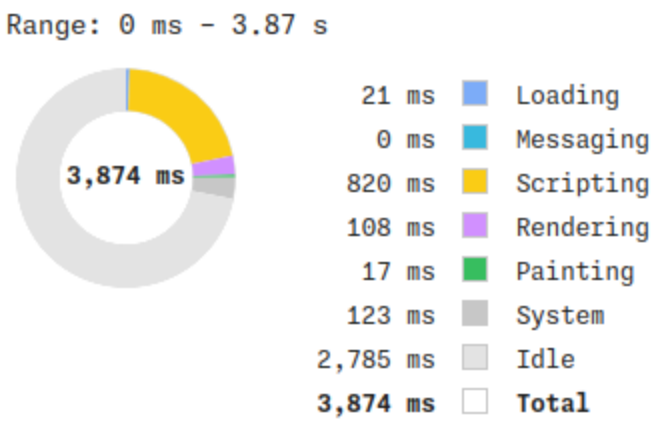
:authority:	www.netflix.com
:method:	GET
:path:	/in/
:scheme:	https
Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-US,en;q=0.9
Cache-Control:	no-cache
Cookie:	nfvdid=BQFmAAEBEOw8mOf0gaZf4-JKjud9XQ9A1X82lCLhbaKjCfH7i3DJfJSyH9LVDazi9AqNfL_KZaL07BRbtgicFyvSJcWvMOZviwn4MhseFyDlAuC3d-GCow%3D%3D; SecureNetflixId=v%3D3%26mac%3DAQEAEQABABTYrN-j6ykCuaLNnbTjf5IRS-TD4cUwTpU.%26dt%3D1738414512377; NetflixId=v%3D3%26ct%3DBgjHlOvcAxLAAch-wff20XTjx6xEUJ6a0oSWDlXUUEhc5by3cCP1ar5HVSK6cteoNEkSi8Mteey3kuMIx80Fxbteb3ttgTPd1PKNwZysKSGH9SOtrfkC94lEWgZicdYiAxUcUD_bOY9ayYV9zskfMdp1NJn8NbGQUd8BPCaobJOkiBAv_TLUTNZQelqmTCaWvo1wdX59TJgtamfAimdhO9AZ2fXeyhl_cYT5UF7lWE3X4x0u1fjHKtybZQu-D8PQpFWahd4uyINCChgGIg4KDL9Z1iYFJYVs93kPDQ..; flwssn=ebf561a5-1363-42f6-901f-c7938913d5bc; OptanonConsent=isGpcEnabled=0&datestamp=Sat+Feb+01+2025+18%3A25%3A17+GMT%2B0530+(India+Standard+Time)&version=202411.1.0&browserGpcFlag=0&isIABGlobal=false&hosts=&consentId=04f13e0c-cdb5-41a0-a117-2b600e06e89f&interactionCount=1&isAnonUser=1&landingPath=https%3A%2F%2Fwww.netflix.com%2Fin%2F&groups=C0001%3A1%2CC0002%3A1%2CC0003%3A1%2CC0004%3A1
Dnt:	1
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-Model:	""
Sec-Ch-Ua-Platform:	"Linux"
Sec-Ch-Ua-Platform-Version:	"6.8.0"
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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36

- **Response Header:**

▼ 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 12:55:19 GMT
Expires:	0
Pragma:	no-cache
Server:	envoy
Set-Cookie:	flwssn=ebf561a5-1363-42f6-901f-c7938913d5bc; Max-Age=10800; Domain=.netflix.com; Path=/
Strict-Transport-Security:	max-age=31536000; includeSubDomains
Via:	2 i-04a5f5e547b131765 (eu-west-1)
X-B3-Traceid:	679e19b6ccab91fdddb3485b7effff0e
X-Content-Type-Options:	nosniff
X-Envoy-Decorator-Operation:	lo_svc
X-Envoy-Upstream-Service-Time:	229
X-Frame-Options:	DENY
X-Netflix.Nfstatus:	1_1
X-Netflix.Proxy.Execution-Time:	232
X-Netflix.Zuul.Netty.Content.Compressor.Target:	gzip
X-Originating-Url:	http://www.netflix.com/in/
X-Request-Id:	daf03d32-cb81-40db-a3bc-e558cdcb983f
X-Robots-Tag:	index
X-Xss-Protection:	1; mode=block; report=https://www.netflix.com/ichnaea/log/freeform/xssreport

- **Performance Metrics:**



- **Cookies and Flags:**

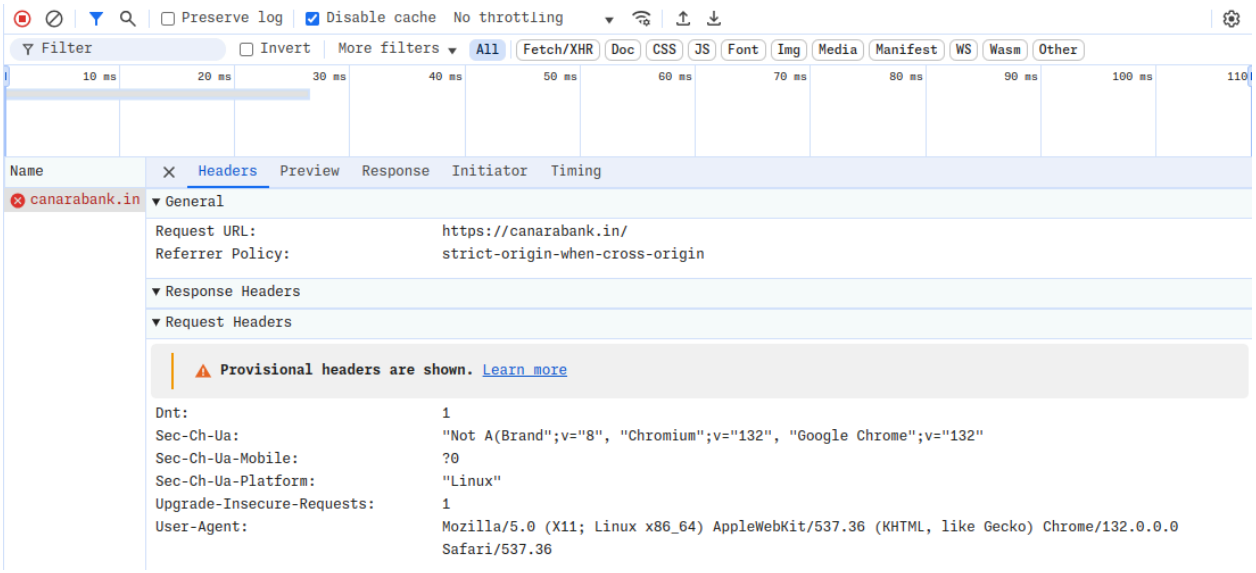
Request Cookies ☐ show filtered out request cookies

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite ▲	Par…	Cro…	Prior…
NetflixId	v%3D3%26ct%3DBgjHlOvcAxLAAch-wff…	.netflix.c…	/	2026-02-01T12:55:…	318	✓	✓	Lax			Medium
OptanonConsent	isGpcEnabled=0&datestamp=Sat+Feb…	.netflix.c…	/	2026-02-01T12:55:…	343			Lax			Medium
SecureNetflixId	v%3D3%26mac%3DAQEAEQABABTYrN-j6y…	.netflix.c…	/	2026-02-01T12:55:…	94	✓	✓	Strict			Medium
nfvdid	BQFmAAEBEOw8mOf0gaZf4-JKjud9XQ9A…	.netflix.c…	/	2026-02-01T12:55:…	130						Medium
flwssn	ebf561a5-1363-42f6-901f-c7938913…	.netflix.c…	/	2025-02-01T15:55:…	42						Medium

Response Cookies

Name ▲	Value	Domain	Path	Expires / Max-Age	Si…	HttpOn…	Sec…	SameSi…	Part…	Cro…	Prior…
flwssn	ebf561a5-1363-42f6-901f-c7938913d5bc	.netf…	/	3 hr	87						Medium

Website 3: canarabank.in (No IP Found)



No response header is received as the site is not working.

This task is then performed on an alternative site, i.e. **canarabank.com**

- **Website 3': canarabank.com (107.162.160.8)**
  - **Request Line:**

```
GET /Assets/images/exclusive-1.webp HTTP/1.1
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cache-Control: no-cache
Connection: keep-alive
Cookie: NSC_10.14.241.15_TTM=ffffffff0906ef1445525d5f4f58455e445a4a4216cb; TS019d7cd7=019ffc8db97b64a6f85511683db1ab5987595cb9735f72861794ffb14aeddb145dae648d1c838a89818210730d767c85c5ef893d63; _ga=GA1.1.1978269069.1738419340; _ga_MD86BV0YCY=GS1.1.1738419339.1.1.1738419384.15.0.0; TSbefe164a027=08c7d6d253ab2000314b7a2af894eff5189dff89c666aabd42ad934850308af9eacea7cb3141fda408ec3d86e0113000 6b8a5f60b0f931f98a883b3c63c1a49e49ad54b082f9add7938f24015a46da1aed44c1cdf23a3164bc6bf854af6bb183
DNT: 1
Host: canarabank.com
Pragma: no-cache
Referer: https://canarabank.com/assets/css/custom.css
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
```

  - **Connection Type:** Persistent (keep-alive)

- Header Fields:
  - Request Header:

▼ Request Headers ☐ Raw

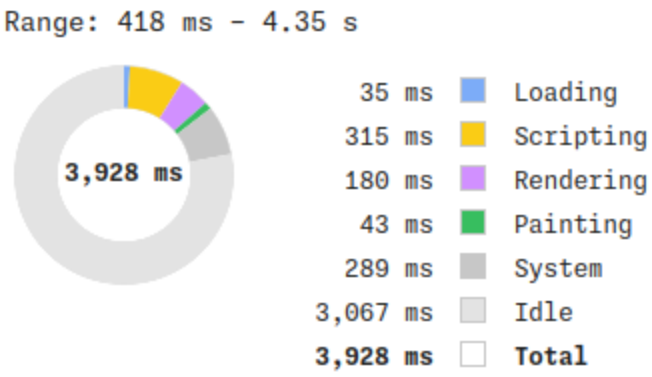
Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-US,en;q=0.9
Cache-Control:	no-cache
Connection:	keep-alive
Cookie:	_ga=GA1.1.1978269069.1738419340; _ga_MD86BV0YCY=GS1.1.1738424767.2.1.1738424925.60.0.0; NSC_10.14.241.15_TTM=ffffffff0906ef1445525d5f4f58455e445a4a4216cb; TS019d7cd7=019ffc8db9fd2ec5903e2e8550b07f9322b0476cd9631bcf1a8479185aa5207d336c1b292e1bd292143a76b6033b5a499ae92b7290; TSbefe164a027=08c7d6d253ab20005a6732297f64dcf326a9995798622a0a66212109f348894001baf7f53d37c46808f1921c5f113000a65265e1c8932a8de12484352f7e4ab0d348baa5df2d3a5d94eb5162c0c46473493f0d88e04bbf8f80d8901c5b75c5f0
Dnt:	1
Host:	canarabank.com
Pragma:	no-cache
Sec-Ch-Ua:	"Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Linux"
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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36

  - Response Header:

▼ 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 cabprod.gupshup.io code.highcharts.com 'unsafe-inline' 'unsafe-eval';
Content-Type:	text/html; charset=utf-8
Date:	Sat, 01 Feb 2025 15:48:55 GMT
Referrer-Policy:	no-referrer-when-downgrade
Set-Cookie:	NSC_10.14.241.15_TTM=ffffffff0906ef1445525d5f4f58455e445a4a4216cb;expires=Sat, 01-Feb-2025 16:21:19 GMT;path=/;secure;httponly
Set-Cookie:	TS019d7cd7=019ffc8db9fd2ec5903e2e8550b07f9322b0476cd9631bcf1a8479185aa5207d336c1b292e1bd292143a76b6033b5a499ae92b7290; Path=/; Secure; HTTPOnly
Set-Cookie:	TSbefe164a027=08c7d6d253ab2000cbd6bbe822ddd6130ebe746a8d690ffea52dddea78b39ba2fc238d01513c9b440830665e8b113000304d75394a3399b736c78017e3a7df19c4bbd195809ca16238b260620315615 80ec3da7a86c62c7da16dac7c88b4b40f; Path=/
Strict-Transport-Security:	max-age=31536000; includeSubDomains; preload
Transfer-Encoding:	chunked
Via:	1.1 sin1-bit15020
X-Content-Type-Options:	nosniff
X-F5-Cache:	MEM_MISS
X-Frame-Options:	SAMEORIGIN
X-Xss-Protection:	1; mode=block

- Performance Metrics:



- Cookies and Flags:

Request Cookies ☐ show filtered out request cookies

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Part…	Cros…	Priori…
NSC_10.14.241.15_T…	ffffffff0906ef1445525d5f4f58455e445a…	canarabank.…	/	2025-02-01T16:21:13…	64	✓	✓				Medium
TS019d7cd7	019ffc8db9fd2ec5903e2e8550b07f9322b0…	canarabank.…	/	Session	116	✓	✓				Medium
TSbefe164a027	08c7d6d253ab20005a6732297f64dcf326a9…	canarabank.…	/	Session	205						Medium
_ga	GA1.1.1978269069.1738419340	.canarabank…	/	2026-03-08T15:48:45…	30						Medium
_ga_MD86BV0YCY	GS1.1.1738424767.2.1.1738424925.60.0…	.canarabank…	/	2026-03-08T15:48:45…	52						Medium

Response Cookies

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Part…	Cros…	Priori…
NSC_10.14.241.15_T…	ffffffff0906ef1445525d5f4f58455e445a…	canarabank.…	/	2025-02-01T16:21:19…	127	✓	✓				Medium
TS019d7cd7	019ffc8db9fd2ec5903e2e8550b07f9322b0…	canarabank.…	/	Session	144	✓	✓				Medium
TSbefe164a027	08c7d6d253ab2000cbd6bbe822ddd6130ebe…	canarabank.…	/	Session	214						Medium

Error Codes

- Error 404: The requested resource does not exist on the server.

```
Request URL:            https://github.com/gregb/sublime-snazzy
Request Method:         GET
Status Code:            🔴 404 Not Found
Remote Address:         20.205.243.166:443
Referrer Policy:        strict-origin-when-cross-origin
```

- Error 401: Authentication is required, but the request lacks valid credentials, or they are incorrect.

```
Request URL:            https://api.github.com/user
Request Method:         GET
Status Code:            🔴 401 Unauthorized
Remote Address:         20.205.243.168:443
Referrer Policy:        strict-origin-when-cross-origin
```

- Error 409: The request conflicts with the current state of the resource, such as trying to create a duplicate entity.

```
Request URL:            https://github.com/Hit2737/Quiz_App/unstar
Request Method:         POST
Status Code:            🔴 409 Conflict
Remote Address:         20.207.73.82:443
Referrer Policy:        no-referrer-when-downgrade
```

References

- **Wireshark Documentation** - https://www.wireshark.org/docs/
  Official documentation for Wireshark, providing detailed information on packet capture and analysis.
- **TCPReplay Documentation** - https://tcpreplay.appneta.com/
  Documentation for TCPReplay, a tool used for replaying network traffic.
- **GitHub Repository for Assignment** - https://github.com/Hist2737/CN_A1
  The GitHub repository containing all the code, scripts, and documentation for this assignment.
- **Google Chrome Developer Tools** - https://developer.chrome.com/docs/devtools/
  Documentation for Chrome DevTools, used for analyzing network performance and HTTP headers.
- **Python Scapy Library** - https://scapy.net/
  Documentation for Scapy, a Python library used for packet manipulation and network analysis.