

# Computer Networks CS 331

## Assignment-1

Gaurav Joshi (21110065) Husain Malwat (21110117)

**GitHub Repository:** [https://github.com/Gaurav17Joshi/CN\\_assignment1](https://github.com/Gaurav17Joshi/CN_assignment1)

---

### Part-1

---

In this part, we have made a sniffer called fast\_sniffer.py, and it can be run and used.

- Protocols of 2.pcap:-

Protocol	Percent Packets	packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	805997	100.0	364642055	6
Ethernet	100.0	805997	3.5	12800341	0
Internet Protocol Version 6	0.1	436	0.0	17712	0
> User Datagram Protocol	0.0	402	0.0	3216	0
Internet Control Message Protocol v6	0.0	34	0.0	2068	0
Internet Protocol Version 4	99.9	805543	4.4	16112460	0
> User Datagram Protocol	19.0	153234	0.3	1225872	0
> Transmission Control Protocol	80.4	647723	3.9	14239696	0
Internet Group Management Protocol	0.0	286	0.0	6884	0
Internet Control Message Protocol	0.5	4300	0.1	217975	0
Address Resolution Protocol	0.0	18	0.0	504	0

The transport layer protocols in the 2.pcap are:-

1. UDP
2. TCP
3. ICMP
4. IGMP

The information we need from each packet is:

1. Packet size (q1)
2. Source ip (q2, q3)
3. Source port (q2, q3)
4. Destination ip (q2, q3)
5. Destination port (q2, q3)

Based on the problem, and the 2.pcap file, these were the different transport layers we had and the information we needed, so to make our sniffer as fast as possible, we only sniffed and stored this information. Next, we run different python scripts to use the sniffed data and get the various statistical results.

We have given the instructions to run the code in the github repo also.

To run the sniffer with tcpreplay:-

**Steps:-**

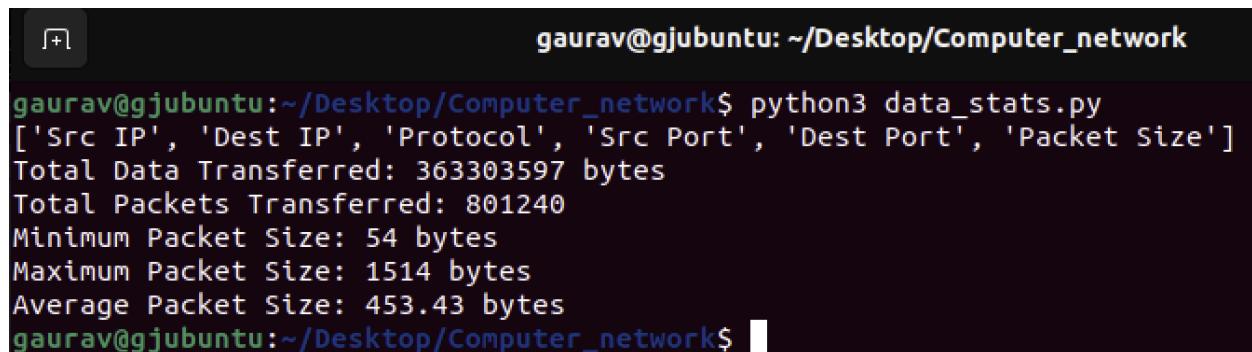
1. In python install the required libraries; pip install socket struct csv
2. Run the fast\_sniffer.py: sudo python3 fast\_sniffer.py
3. Run the tcpreplay of the 2.pcap in another terminal: sudo tcpreplay -i enp0s1 -M 10 2.pcap. (here enp0s1 can be replace by other ports "eth")

**Q1) Packet Capture and Analysis**

This program captures network packets using a raw socket and logs relevant details (source/destination IPs, protocol, ports, and packet sizes) into a CSV file. The captured data is then analyzed to determine total data transferred, packet count, and size distribution. A histogram visualizes the packet size distribution.

**Steps to Run:**

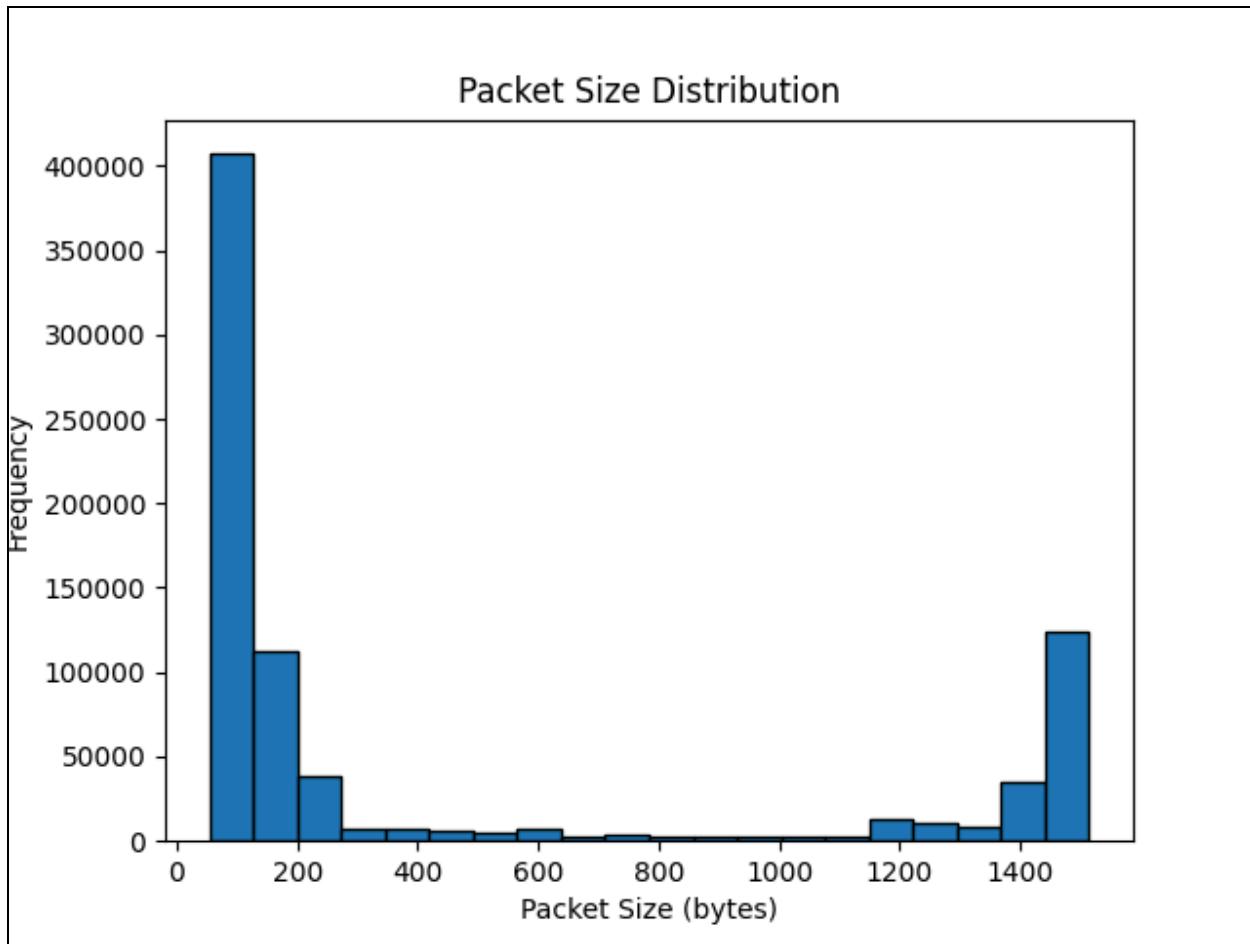
1. Run the packet capture script with superuser privileges (sudo python3 fast\_sniffer.py).
2. Stop capture using Ctrl+C, which saves packet data to fast\_captured\_packets\_info.csv.
3. Run the analysis script (python3 data\_stats.py) to generate statistics and a packet size histogram (Packet\_Size\_dist.png).



A screenshot of a terminal window titled 'gaurav@gjubuntu: ~/Desktop/Computer\_network'. The terminal shows the execution of the 'data\_stats.py' script. The output provides network statistics: Total Data Transferred (363303597 bytes), Total Packets Transferred (801240), Minimum Packet Size (54 bytes), Maximum Packet Size (1514 bytes), and Average Packet Size (453.43 bytes). The terminal prompt 'gaurav@gjubuntu:~/Desktop/Computer\_network\$' is visible at the bottom right.

```
gaurav@gjubuntu:~/Desktop/Computer_network$ python3 data_stats.py
['Src IP', 'Dest IP', 'Protocol', 'Src Port', 'Dest Port', 'Packet Size']
Total Data Transferred: 363303597 bytes
Total Packets Transferred: 801240
Minimum Packet Size: 54 bytes
Maximum Packet Size: 1514 bytes
Average Packet Size: 453.43 bytes
gaurav@gjubuntu:~/Desktop/Computer_network$
```

Here, are the statistics of the data, including a histogram:-



x axis = packet size, and the y-axis = number of packets.

## Q2.) Unique Source-Destination Pairs Extraction

This script (`pair_stats.py`) extracts and identifies unique source-destination pairs (IP:port combinations) from captured packet data stored in `captured_packets_info.csv`. The program reads the CSV file, locates the necessary columns, and stores unique (source IP, source port, destination IP, destination port) pairs in a set to eliminate duplicates.

Steps to Run:

1. Ensure `captured_packets_info.csv` exists with proper packet data.
2. Run the script:  
`"python3 pair_stats.py"`

3. The script outputs the total number of unique pairs.

```
gaurav@gjubuntu:~/Desktop/Computer_network$ python3 pair_stats.py
['Src IP', 'Dest IP', 'Protocol', 'Src Port', 'Dest Port', 'Packet Size']
0 , 1 , 3 , 4
Number of unique pairs: 41791
gaurav@gjubuntu:~/Desktop/Computer_network$
```

- Here, we have 41791 unique Source destination pairs.

4. Set print\_all = True to list them. We can also print out all of them:-

```
gaurav@gjubuntu:~/Desktop/Computer_network$ python3 pair_stats.py --print-all
Source: 172.16.133.234:49151 -> Destination: 108.59.243.196:65435
Source: 172.16.133.42:57377 -> Destination: 172.16.139.250:5440
Source: 172.16.133.73:60766 -> Destination: 172.16.139.250:5440
Source: 172.16.133.28:49407 -> Destination: 63.97.94.126:80
Source: 172.16.133.66:54338 -> Destination: 23.67.242.80:443
Source: 172.16.133.109:49151 -> Destination: 4.69.132.85:49654
```

### Q3. Flow Calculation and Data Transfer Analysis

This script calculates flow statistics for each source and destination IP, as well as identifies the source-destination pair with the most data transferred. It reads the captured packet data from `fast_captured_packets_info.csv` and processes it to populate dictionaries that track:

1. Source flows: Number of flows initiated by each source IP.
2. Destination flows: Number of flows received by each destination IP.
3. Data transferred: Total data transferred for each unique source-destination IP:port pair.

The script also prints the total number of source and destination flows and identifies the source-destination pair with the maximum data transfer.

Steps to Run:

1. Ensure the file `fast_captured_packets_info.csv` contains the relevant packet data.
2. Run the script:

“`python3 flow_calculation.py`”

3. The script outputs:
  - Number of source and destination flows.
  - A dictionary of source flows.
  - A dictionary of destination flows.
  - The source-destination pair with the most data transferred.

The total number of unique outgoing and incoming flows, and the pair with most data transferred.

```
gaurav@gjubuntu:~/Desktop/Computer_network$ python3 flow_stats.py
['Src IP', 'Dest IP', 'Protocol', 'Src Port', 'Dest Port', 'Packet Size']
0 , 1 , 3 , 4
Source IP Flows:
Total Number of Ip address outgoing flows 2078

Destination IP Flows:
Total Number of Ip address incoming flows 2004

Source-Destination Pair with Most Data Transferred: ('172.16.133.95', '49358', '157.56.240.102'
, '443')
Total Data Transferred: 17341946 bytes
gaurav@gjubuntu:~/Desktop/Computer_network$
```

4. Setting the print\_all flag to True will display all the source and destination flows.

#### Source Flows:-

```
gaurav@gjubuntu:~/Desktop/Computer_network$ python3 flow_stats.py
['Src IP', 'Dest IP', 'Protocol', 'Src Port', 'Dest Port', 'Packet Size']
0 , 1 , 3 , 4
Source IP Flows:
Total Number of Ip address source flows 2078
192.168.64.1: 4 flows
65.54.95.68: 1275 flows
65.54.95.75: 766 flows
65.54.95.140: 658 flows
204.14.234.85: 1036 flows
65.54.186.19: 66 flows
192.168.3.131: 4294 flows
```

#### Destination Flows:-

```
Destination IP Flows:
Total Number of Ip address destination flows 2004
224.0.0.251: 29 flows
192.168.3.131: 6184 flows
10.0.2.15: 808 flows
207.46.0.109: 29 flows
65.54.95.68: 664 flows
172.16.255.1: 1219 flows
204.14.234.85: 740 flows
65.54.95.140: 495 flows
172.16.0.1: 10 flows
147.31.122.1: 90 flows
```

## Q4. Sniffer Timing

PART1: Self

We will run tcpreplay with a speed cap for 'mbps' and 'pps'

Tcpreplay commands:-

Run :

sudo tcpreplay -i enp0s1 -M 10 2.pcap (for 10 mbps)

**30 Mbps**

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -M 30 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 97.23 seconds
Rated: 3749997.9 Bps, 29.99 Mbps, 8288.91 pps
Flows: 41719 flows, 429.04 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu: ~/Desktop/Computer_network$
```

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
Packet: 65.54.95.140:80 -> 192.168.3.131:56415, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56417 -> 65.54.95.140:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
^C
Sniffing stopped.

Total captured Packets: 805752 and Total saved Packets: 805290
gaurav@gjubuntu: ~/Desktop/Computer_network$
```

**40 Mbps**

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -M 40 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 72.92 seconds
Rated: 4999999.3 Bps, 39.99 Mbps, 11051.89 pps
Flows: 41719 flows, 572.05 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
```

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
Packet: 65.54.95.140:80 -> 192.168.3.131:56415, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56417 -> 65.54.95.140:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
^C
Sniffing stopped.

Total captured Packets: 801268 and Total saved Packets: 800814
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
```

50 Mbps

```
gaurav@gjubuntu:~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -M 50 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 58.34 seconds
Rated: 6249994.9 Bps, 49.99 Mbps, 13814.85 pps
Flows: 41719 flows, 715.06 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu:~/Desktop/Computer_network$
```

```
gaurav@gjubuntu:~/Desktop/Computer_network$ 
Packet: 192.168.3.131:56417 -> 65.54.95.140:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
^C
Sniffing stopped.

Total captured Packets: 805838 and Total saved Packets: 805378
gaurav@gjubuntu:~/Desktop/Computer_network$
```

60 Mbps

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -M 60 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 48.61 seconds
Rated: 7499995.6 Bps, 59.99 Mbps, 16577.82 pps
Flows: 41719 flows, 858.08 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu: ~/Desktop/Computer_network$
```

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
Packet: 192.168.3.131:56417 -> 65.54.95.140:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
^C
Sniffing stopped.

Total captured Packets: 805672 and Total saved Packets: 805207
gaurav@gjubuntu: ~/Desktop/Computer_network$
```

**80 Mbps** (It now captures almost all packets)

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -M 80 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 36.46 seconds
Rated: 9999997.9 Bps, 79.99 Mbps, 22103.78 pps
Flows: 41719 flows, 1144.10 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
```

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
Packet: 192.168.64.1:5353 -> 224.0.0.251:5353, Protocol: UDP, Size: 79
^C
Sniffing stopped.

Total captured Packets: 802458 and Total saved Packets: 802006
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
```

**100 Mbps** (This has a significant loss)

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -M 100 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 29.17 seconds
Rated: 12499988.6 Bps, 99.99 Mbps, 27629.70 pps
Flows: 41719 flows, 1430.13 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
```

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
Packet: 192.168.3.131:56417 -> 65.54.95.140:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
^C
Sniffing stopped.

Total captured Packets: 786111 and Total saved Packets: 785682
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
```

**Hence, the TOP SPEED = 60 Mbps (over that, there is some loss)**

Using packet rate:-

sudo tcpreplay -i enp0s1 -p 1000 2.pca (for 1000 packets per second)

**10000 Packets per second** (Collects all packets)

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -p 10000 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 80.59 seconds
Rated: 4524115.9 Bps, 36.19 Mbps, 10000.00 pps
Flows: 41719 flows, 517.60 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu: ~/Desktop/Computer_network$ 

gaurav@gjubuntu: ~/Desktop/Computer_network$ 
Packet: 192.168.3.131:56417 -> 65.54.95.140:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
^C
Sniffing stopped.

Total captured Packets: 805975 and Total saved Packets: 805518
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
```

**20000 Packets per second** (Collects all packets, but has some losses)

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -p 20000 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 40.29 seconds
Rated: 9048225.2 Bps, 72.38 Mbps, 20000.00 pps
Flows: 41719 flows, 1035.21 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu: ~/Desktop/Computer_network$ 

gaurav@gjubuntu: ~/Desktop/Computer_network$ 
Packet: 192.168.3.131:56417 -> 65.54.95.140:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
^C
Sniffing stopped.

Total captured Packets: 785706 and Total saved Packets: 785253
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
```

**30000 Packets per second** (Collects all packets, but has some losses)

```
gaurav@gjubuntu: ~/Desktop/Computer_network$ sudo tcpreplay -i enp0s1 -p 30000 2.pcap
Actual: 805997 packets (364642055 bytes) sent in 26.86 seconds
Rated: 13572351.9 Bps, 108.57 Mbps, 30000.03 pps
Flows: 41719 flows, 1552.82 fps, 805298 flow packets, 454 non-flow
Statistics for network device: enp0s1
    Successful packets:      805997
    Failed packets:          0
    Truncated packets:       0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
gaurav@gjubuntu: ~/Desktop/Computer_network$ ^C
gaurav@gjubuntu: ~/Desktop/Computer_network$ 
Packet: 192.168.3.131:56417 -> 65.54.95.140:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57244 -> 204.14.234.85:443, Protocol: TCP, Size: 54
Packet: 65.54.95.140:80 -> 192.168.3.131:56027, Protocol: TCP, Size: 530
Packet: 192.168.3.131:56214 -> 65.54.95.75:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:56428 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.3.131:57011 -> 72.14.213.138:80, Protocol: TCP, Size: 997
Packet: 84.197.9.59:44808 -> 172.16.255.1:50983, Protocol: UDP, Size: 62
Packet: 192.168.3.90:139 -> 10.0.2.15:1095, Protocol: TCP, Size: 107
Packet: 204.14.234.85:443 -> 192.168.3.131:57247, Protocol: TCP, Size: 222
Packet: 184.85.226.161:443 -> 172.16.255.1:10650, Protocol: TCP, Size: 1514
Packet: 204.14.234.85:8443 -> 192.168.3.131:57248, Protocol: TCP, Size: 60
Packet: 172.16.255.1:10638 -> 130.117.72.100:443, Protocol: TCP, Size: 54
Packet: 65.54.95.68:80 -> 192.168.3.131:56065, Protocol: TCP, Size: 1514
Packet: 192.168.3.131:56457 -> 65.54.95.68:80, Protocol: TCP, Size: 54
Packet: 192.168.2.96:56872 -> 192.168.145.198:31821, Protocol: TCP, Size: 83
Packet: 192.168.3.131:57245 -> 204.14.234.85:8443, Protocol: TCP, Size: 54
Packet: 209.17.73.30:80 -> 192.168.3.131:58789, Protocol: TCP, Size: 1514
Packet: 204.9.163.181:443 -> 172.16.255.1:10640, Protocol: TCP, Size: 1514
^C
Sniffing stopped.

Total captured Packets: 799823 and Total saved Packets: 799367
gaurav@gjubuntu: ~/Desktop/Computer_network$
```

Hence, the TOP SPEED = 10000 Pps (over that, there is some loss)

ii)

---

## Part-2

---

### Sniffing Specific Packet Information

Our script captures packets using a raw socket and processes them to answer specific questions regarding a network traffic capture. It looks for specific information in TCP packets, including an IP address, laptop name, checksum, and specific messages. The script answers the following questions:

1. Find the IP Address: Searches for a message containing "my ip address = " in the payload of TCP packets.
2. Count Packets with IP: Counts the number of packets where the captured IP address appears either as a source or destination.
3. Laptop Name and TCP Checksum: Extracts the laptop name and its corresponding TCP checksum from packets.
4. Order Successful Messages: Counts number packets contain the phrase "Order successful".

Steps to Run:

1. Set the variable found\_ip to the IP address you are looking for and run the script with the following command:  
"sudo python3 sniff\_packets.py".
  - o Note: Here, we first ran the code to get the ip, and then saved it. We had to do this as the ip address was being used before its location.
2. The script listens for packets and checks for the specified conditions.
3. Once you stop the script (with Ctrl+C), it will print the results for all the questions:
  - o The extracted IP address.
  - o The number of packets with the given IP.
  - o The laptop name and TCP checksum.
  - o The count of packets containing "Order successful".

The answers for the questions are:-

1. 10.1.2.200
2. 80
3. a. lenovo , b, 8192
4. 40

```
gaurav@gjubuntu:~/Desktop/Computer_network$ sudo python3 adv_data_sniff.py
[sudo] password for gaurav:
the name of laptop = lenovo
✓ Found Laptop
my ip address = <10.1.2.200>
✓ Found IP Address in TCP Packet
^C
● Sniffing stopped.

Total packets checked = 806014

Q1. Extracted IP Address: 10.1.2.200
Q2. Number of packets with IP 10.1.2.200: 80
Q3a. Laptop Name: the name of laptop = lenovo
Q3b. TCP Checksum of laptop name packet: 8192
Q4. Number of packets with 'Order successful': 40
gaurav@gjubuntu:~/Desktop/Computer_network$
```

---

## Part-3

---

“””

### **Part 3: Capture the packets (20 points)**

- 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.
- 1) 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.
  - 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.
  - 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.

“””

### **Wireshark Experiments**

#### **Q 1.a) Application Layer Protocols Captured Using Wireshark:**

## 1. Multicast Domain Name System (mDNS)

- mDNS is a zero-configuration networking protocol that enables devices to resolve hostnames to IP addresses without relying on a central DNS server.
  - It is used for device discovery in local networks and is commonly found in applications such as Apple AirPlay, Google Chromecast, and various smart home and IoT devices.
  - mDNS operates at the Application Layer and uses UDP (port 5353), meaning data is sent without connection setup, making it fast but unreliable.

**RFC:** <https://datatracker.ietf.org/doc/html/rfc6762>

## 2. Network Time Protocol (NTP)

- NTP protocol is used to synchronize the clocks of computers and network devices over a network.
  - It operates using UDP (port 123) for its communication.

**RFC:** <https://datatracker.ietf.org/doc/html/rfc5905>

No.	Time	Source	Destination	Protocol	Length	Info
13	2.543912	10.7.34.194	17.253.18.131	NTP	90	NTP Version 4, client
19	4.633144	10.7.34.194	17.253.18.131	NTP	90	NTP Version 4, client
32	6.736026	10.7.34.194	17.253.84.251	NTP	90	NTP Version 4, client
33	6.845389	17.253.84.251	10.7.34.194	NTP	90	NTP Version 4, server
947	902.500561	10.7.34.194	17.253.18.99	NTP	90	NTP Version 4, client
948	904.602217	10.7.34.194	17.253.18.99	NTP	90	NTP Version 4, client
949	906.707025	10.7.34.194	17.253.18.131	NTP	90	NTP Version 4, client

Frame 13: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface en0, id 0  
 Ethernet II, Src: fe:d9:20:18:57:5d (fe:d9:20:18:57:5d), Dst: IETF-VRRP-VRID\_6 (00:00:5e:00:01:f6)  
 > Destination: IETF-VRRP-VRID\_6 (00:00:5e:00:01:f6)  
 > Source: fe:d9:20:18:57:5d (fe:d9:20:18:57:5d)  
 Type: IPv4 (0x0800)  
 [Stream index: 0]  
> Internet Protocol Version 4, Src: 10.7.34.194, Dst: 17.253.18.131  
 > UDP Port: 123 [Protocol], Src Port: 123, Dst Port: 123  
 Source Port: 123  
 Destination Port: 123  
 Length: 56  
 Checksum: 0x1545 [unverified]  
 [Checksum Status: Unverified]  
 [Stream index: 4]  
 [Stream Packet Number: 1]  
 [Timestamps]  
 UDP payload (48 bytes)  
 Network Time Protocol (NTP Version 4, client)  
 > Flags: 0x23, Leap Indicator: no warning, Version number: NTP Version 4, Mode: client  
 Peer Clock Stratum: unspecified or invalid (0)  
 Peer Polling Interval: 0 (1 seconds)  
 Peer Clock Precision: 0 (1.000000000 seconds)  
 Root Delay: 0.000000 seconds  
 Root Dispersion: 0.000000 seconds  
 Reference ID: NULL  
 Reference Timestamp: NULL  
 Origin Timestamp: NULL

0000 00 00 5e 00 01 f6 fe d9 20 18 57 5d 00 00 45 00 .^.....  
0001 00 4c 10 36 00 00 40 1f 19 23 00 07 22 c2 11 fd L...@.  
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..@.6.  
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....6.  
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....6.  
0050 00 00 a5 17 dc 05 36 d4 bd 08 .....6.

### 3. Real-Time Messaging Protocol (RTMP)

- RTMP is used for delivering streaming audio, video, and data to a Flash player, commonly for live streaming media applications.

<https://datatracker.ietf.org/doc/html/rfc7826>

No.	Time	Source	Destination	Protocol	Length	Info
3771	65934467.89...	67.69.196.212	172.16.133.93	RTMP	64	Unknown (0x0)

Frame 3771: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface unknown, id 0  
 Ethernet II, Src: WatchGuardTe\_3e:02:d0 (00:90:7f:3e:02:d0), Dst: Dell\_67:15:9f (00:21:70:67:15:9f)  
 > Destination: Dell\_67:15:9f (00:21:70:67:15:9f)  
 > Source: WatchGuardTe\_3e:02:d0 (00:90:7f:3e:02:d0)  
 Type: IPv4 (0x0800)  
 [Stream index: 62]  
 Internet Protocol Version 4, Src: 67.69.196.212, Dst: 172.16.133.93  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 > Differentiated Services Field: 0x20 (DS2: CS1, ECN: Not-ECT)  
 Total Length: 50  
 Identification: 0x52f4 (2136)  
 Identification: 0x52f4 (2136)  
 > 010.... = Flags: 0x2 Don't fragment  
 ..0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 64  
 Protocol: TCP (6)  
 Header Checksum: 0x792a [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 67.69.196.212  
 Destination Address: 172.16.133.93  
 [Stream index: 368]  
 Transmission Control Protocol, Src Port: 1935, Dst Port: 60584, Seq: 129, Ack: 1, Len: 10  
 Real Time Messaging Protocol (Unknown (0x0))

0000 00 21 70 67 15 9f 00 90 7f 3e 02 d0 00 00 45 20 !pg.....  
0010 00 32 52 04 40 98 00 00 20 28 43 45 01 d0 00 00 2R@u.y  
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..C.....  
0030 ff ff 1d 43 00 00 82 00 05 83 00 01 00 00 00 01 ..C.....

## 4. SSH Protocol (Secure Shell)

- SSH is a cryptographic network protocol that allows secure remote login and command execution over an unsecured network, providing encryption and authentication. <https://datatracker.ietf.org/doc/html/rfc4253>

No.	Time	Source	Destination	Protocol	Length	Info
734	65934466.78	172.16.128.233	172.16.133.233	SSH	198	Client: Encrypted packet (len=144)
907	65934466.85	172.16.133.233	172.16.128.233	SSH	592	Server: Encrypted packet (len=448)
908	65934466.85	172.16.133.233	172.16.128.233	SSH	78	Server: Encrypted packet (len=6)
1000	65934467.35	172.16.133.233	172.16.128.233	SSH	106	Client: Encrypted packet (len=52)
2580	65934467.35	172.16.133.233	172.16.128.233	SSH	106	Server: Encrypted packet (len=52)
2510	65934467.35	172.16.133.233	172.16.128.233	SSH	122	Client: Encrypted packet (len=68)
2830	65934467.35	172.16.133.233	172.16.128.233	SSH	138	Server: Encrypted packet (len=84)
2832	65934467.35	172.16.133.233	172.16.128.233	SSH	138	Client: Encrypted packet (len=84)
3043	65934467.57	172.16.133.233	172.16.128.233	SSH	96	Server: Encrypted packet (len=60)
3044	65934467.57	172.16.133.233	172.16.128.233	SSH	122	Client: Encrypted packet (len=68)
3303	65934467.67	172.16.133.233	172.16.128.233	SSH	106	Server: Encrypted packet (len=52)
3310	65934467.67	172.16.133.233	172.16.128.233	SSH	154	Client: Encrypted packet (len=100)
3555	65934467.77	172.16.133.233	172.16.128.233	SSH	98	Server: Encrypted packet (len=36)
3716	65934467.87	172.16.133.233	172.16.133.233	SSH	106	Client: Encrypted packet (len=52)
3737	65934467.87	172.16.133.233	172.16.128.233	SSH	96	Server: Encrypted packet (len=52)
3726	65934467.87	172.16.133.233	172.16.128.233	SSH	106	Client: Encrypted packet (len=52)
9298	65934469.97	172.16.133.233	172.16.133.233	SSH	106	Client: Encrypted packet (len=52)
9291	65934469.97	172.16.133.233	172.16.128.233	SSH	106	Server: Encrypted packet (len=52)
9292	65934469.97	172.16.133.233	172.16.128.233	SSH	106	Client: Encrypted packet (len=52)
147-	65934470.97	172.16.133.233	172.16.133.233	SSH	106	Server: Encrypted packet (len=52)
148-	65934471.98	172.16.133.233	172.16.128.233	SSH	106	Client: Encrypted packet (len=52)
147-	65934472.98	172.16.133.233	172.16.128.233	SSH	106	Server: Encrypted packet (len=52)
149-	65934472.98	172.16.133.233	172.16.128.233	SSH	106	Client: Encrypted packet (len=52)
149-	65934472.98	172.16.133.233	172.16.128.233	SSH	106	Server: Encrypted packet (len=52)
> Frame 907: 592 bytes on wire (4616 bits), 592 bytes captured (4616 bits) on interface unknown, id 0						
Ethernet II, Src: Cisco_b1:15:80 (08:04:db:b1:58:60), Dst: WatchGuardTe_3e:02:d0 (00:90:7f:3e:02:d0)						
Destination: WatchGuardTe_3e:02:d0 (00:90:7f:3e:02:d0)						
Source: Cisco_b1:15:80 (08:04:db:b1:58:60)						
Type: IPv4 (8888)						
[Stream index: 14]						
Internet Protocol Version 4, Src: 172.16.133.233, Dst: 172.16.128.233						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 255						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 119]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
HeaderChecksum: 0x477b [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 172.16.133.233						
Destination Address: 172.16.128.233						
[Stream index: 143]						
Transmission Control Protocol, Src Port: 22, Dst Port: 55208, Seq: 1, Ack: 145, Len: 448						
Identification: 0x12e1 (4833)						
Flags: 0x0						
Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)			</td			

## 6. Yahoo YMSG Messenger Protocol

- YMSG is the messaging protocol used by Yahoo Messenger for sending instant messages and supporting features like file transfers, presence, and notifications.

Frame 91866: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface unknown, id 0  
Ethernet II, Src: LiteonTechno\_3f:fb:dd (9c:b7:8d:3f:fb:dd), Dst: WatchGuardTe\_3e:02:d0 (00:90:7f:e3:02:d0)  
Destination: WatchGuardTe\_3e:02:d0 (00:90:7f:e3:02:d0)  
Source: LiteonTechno\_3f:fb:dd (9c:b7:8c:3f:fb:dd)  
Type: IPv4 (0x0800)  
[Stream index: 12]  
Internet Protocol Version 4, Src: 172.16.133.114, Dst: 67.195.187.234  
 0100 00 90 7f e3 02 d0 9c b7 8d 3f fb dd 08 00 45 00 ...  
 0101 .. 0101 .. Header Length: 20 bytes (5)  
 0102 .. Differentiated Service Field: 0x00 (DSSCP: CS0, EON: Not-ECT)  
 0103 Total Length: 72  
Identification: 0x0100 (24843)  
 0104 .0.0.0.0.0.0.0.0 = Fragment Offset: 0  
 0105 Time to Live: 128  
Protocol: TCP (62)  
Header Checksum: 0x6874 (Validation disabled)  
Message Checksum: Unverified  
Source Address: 172.16.133.114  
Destination Address: 67.195.187.234  
[Stream index: 1738]  
Transmission Control Protocol, Src Port: 53723, Dst Port: 5050, Seq: 1, Ack: 1, Len: 32  
Yahoo YM56 Messenger Protocol (Keep Alive)

## 7. Domain Name System (DNS)

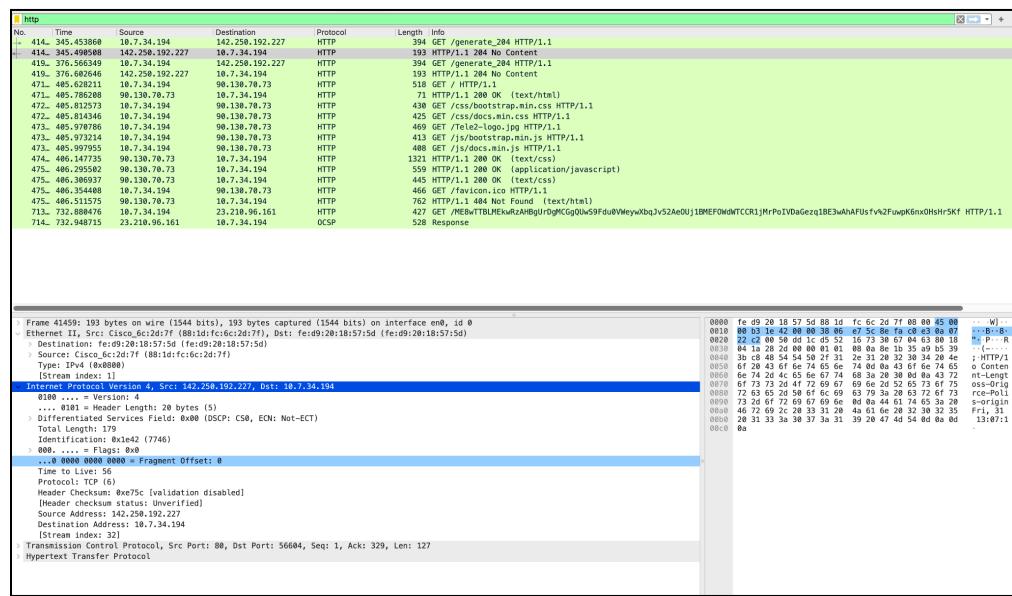
DNS is a protocol that translates human-readable domain names into IP addresses, allowing browsers to locate web servers. It operates over TCP/UDP (port 53) and is essential for the functioning of the internet.

RFC: <https://www.ietf.org/rfc/rfc1035.txt>

## 8. Hypertext Transfer Protocol (HTTP)

HTTP is the foundational protocol for transferring data across the web. It defines how messages are formatted and transmitted, operating over TCP (port 80) and often using encryption (HTTPS) over port 443.

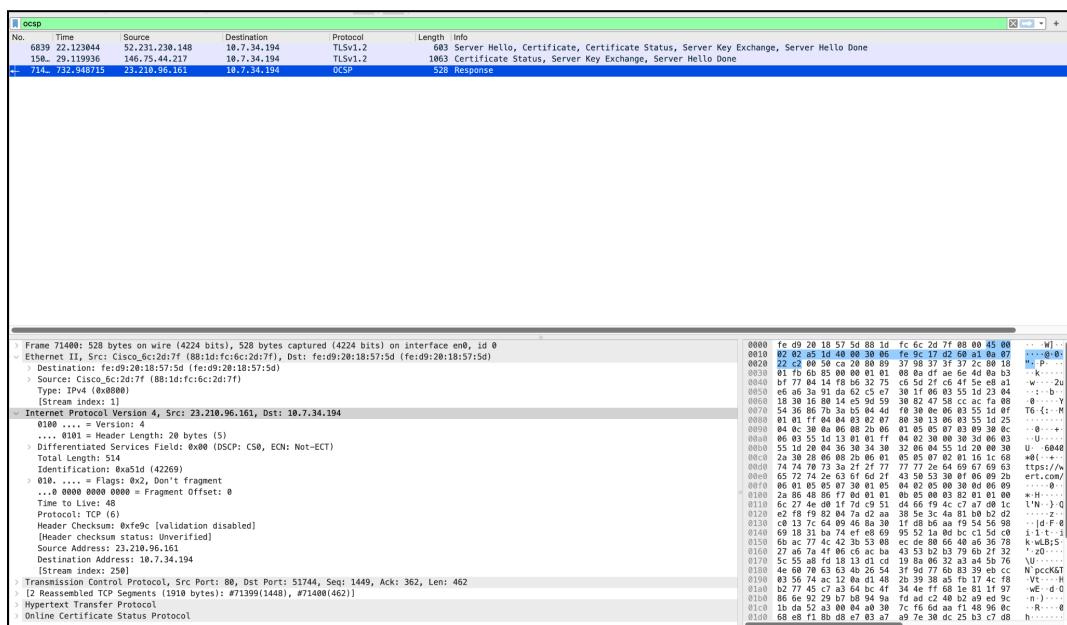
RFC: <from slides>



## 9. Online Certificate Status Protocol (OCSP)

OCSP is a protocol used to check the revocation status of an X.509 digital certificate, providing real-time verification to enhance the security of communications. It operates over HTTP (port 80).

RFC: 6960



Q 2)

## i. canarabank.in

### a. Request Line and Connection Information:

Name	Method	Status	Protocol	Remote Address	Type	Initiator	Size	Time
canarabank/	GET	200	http/1.1	124.153.118.169:443	document	(index):731	1.4 kB	183 ms
chatbot.html?hostedDomain=ht...	GET	200	http/1.1	20.235.192.10:443	document	(disk cache)	1 ms	
mdown1.gif	GET	200	http/1.1	124.153.118.169:443	gif	canarabank/25	(memory ca...	0 ms
shareprice.css	GET	200	http/1.1	124.153.118.169:443	stylesheet	canarabank/9	(memory ca...	0 ms
canarabank.com	GET	200	http/1.1	107.162.160.8:443	document	Other	58.7 kB	734 ms
languageMapping.json	GET	200	http/1.1	20.235.192.10:443	xhr	jquery.js?2	(ServiceWor...	10 ms
en	GET	200	http/1.1	20.235.192.10:443	xhr	jquery.js?2	1.0 kB	104 ms
webSdkEvents.js	GET	200	http/1.1	20.235.192.10:443	xhr	jquery.js?2	(disk cache)	2 ms
splash-icon.png	GET	200	http/1.1	20.235.192.10:443	png	chatbot.html?hostedDom...	(memory ca...	0 ms
sw.js	GET	200	http/1.1	20.235.192.10:443	script	chatbot.html?hostedDom...	(memory ca...	0 ms
index.js	GET	200	http/1.1	20.235.192.10:443	script	chatbot.html?hostedDom...	(memory ca...	0 ms
chatBotFrame.js	GET	200	http/1.1	20.235.192.10:443	script	chatbot.html?hostedDom...	(memory ca...	0 ms
chatBot.js	GET	200	http/1.1	20.235.192.10:443	script	chatbot.html?hostedDom...	(memory ca...	0 ms
sdk.js	GET	200	http/1.1	20.235.192.10:443	script	chatbot.html?hostedDom...	(memory ca...	0 ms
jquery.js	GET	200	http/1.1	20.235.192.10:443	script	chatbot.html?hostedDom...	(memory ca...	0 ms
pdf.gif	GET	200	http/1.1	107.162.160.8:443	gif	jquery.min.js?2	(memory ca...	0 ms
RBI_Banner_2_English.webp	GET	200	http/1.1	107.162.160.8:443	webp	custom.js?v=USKOx_rj-bl	(memory ca...	0 ms
EVAL JS 2D enabled.webp	GET	200	http/1.1	107.162.160.8:443	webp	custom.js?v=USKOx_rj-bl	(memory ca...	0 ms

#### 1. Request Line:

- **GET / HTTP/1.1**
- **Version of Application Layer Protocol: HTTP/1.1**
- **IP Address: 107.162.160.8**

```
PS C:\Users\3malw> ping canarabank.com

Pinging canarabank.com [107.162.160.8] with 32 bytes of data:
Reply from 107.162.160.8: bytes=32 time=72ms TTL=241
Reply from 107.162.160.8: bytes=32 time=74ms TTL=241
Reply from 107.162.160.8: bytes=32 time=71ms TTL=241
Reply from 107.162.160.8: bytes=32 time=72ms TTL=241

Ping statistics for 107.162.160.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 71ms, Maximum = 74ms, Average = 72ms
PS C:\Users\3malw> |
```

## 2. Connection Type:

- Persistent Connection: NO

The screenshot shows the NetworkMiner tool interface. On the left, a tree view lists various network requests, including 'canarabank/' and 'canarabank.com'. On the right, the 'Headers' tab is selected, showing detailed information for the 'canarabank.com' request. Under the 'General' section, the 'Request URL' is https://canarabank.com/, 'Request Method' is GET, 'Status Code' is 200 OK, and 'Remote Address' is 107.162.160.8:443. Under the 'Response Headers' section, 'Cache-Control' is public, max-age=36000, and 'Connection' is close.

[Connection: keep-alive indicates a persistent connection, while Connection: close indicates a non-persistent connection]

## ii. github.com

### a. Request Line and Connection Information:

The screenshot shows the Network tab in the Chrome DevTools performance panel. The main area displays a timeline of network requests for the GitHub homepage. Below the timeline, a table provides detailed information for each request, including the name, method, status, protocol, remote address, type, initiator, size, and time. The table shows numerous requests from the domain 185.199.110.154:443, primarily using the h2 protocol.

Name	Method	Status	Protocol	Remote Address	Remote Address Sp...	Type	Initiator	Size	Time
github.com	GET	200	h2	20.205.243.166:443	Public	document	Other	51.8 kB	78 ms
global-banner-disable-f988...	GET	200	h2	185.199.110.154:443		script	(index):29	(memory ...	0 ms
mona-sans-d1bf285e9b9b...	GET	200	h2	185.199.110.154:443		font	(index):31	(memory ...	0 ms
wp-runtime-0344c458bf5c.js	GET	200	h2	185.199.110.154:443		script	(index):48	(memory ...	0 ms
vendors-node_modules_0d...	GET	200	h2	185.199.110.154:443		script	(index):49	(memory ...	0 ms
vendors-node_modules_git...	GET	200	h2	185.199.110.154:443		script	(index):50	(memory ...	0 ms
ui_packages_failbot_failb...	GET	200	h2	185.199.110.154:443		script	(index):51	(memory ...	0 ms
environment-04ca94cb6e8...	GET	200	h2	185.199.110.154:443		script	(index):52	(memory ...	0 ms
vendors-node_modules_pri...	GET	200	h2	185.199.110.154:443		script	(index):53	(memory ...	0 ms
vendors-node_modules_git...	GET	200	h2	185.199.110.154:443		script	(index):54	(memory ...	0 ms
vendors-node_modules_git...	GET	200	h2	185.199.110.154:443		script	(index):55	(memory ...	0 ms
vendors-node_modules_git...	GET	200	h2	185.199.110.154:443		script	(index):56	(memory ...	0 ms
vendors-node_modules_git...	GET	200	h2	185.199.110.154:443		script	(index):57	(memory ...	0 ms
vendors-node_modules_git...	GET	200	h2	185.199.110.154:443		script	(index):58	(memory ...	0 ms
vendors-node_modules_git...	GET	200	h2	185.199.110.154:443		script	(index):59	(memory ...	0 ms
vendors-node_modules_git...	GET	200	h2	185.199.110.154:443		script	(index):60	(memory ...	0 ms
light-7aa84bbf711e.css	GET	200	h2	185.199.110.154:443		stylesheet	(index):34	(disk cache)	5 ms
oithub-elements-b487d4d...	GET	200	h2	185.199.110.154:443		script	(index):61	(memory ...	0 ms

## 1. Request Line:

- **GET / HTTP/2**
- **Version of Application Layer Protocol: HTTP/2**
- **IP Address: 20.207.73.82**

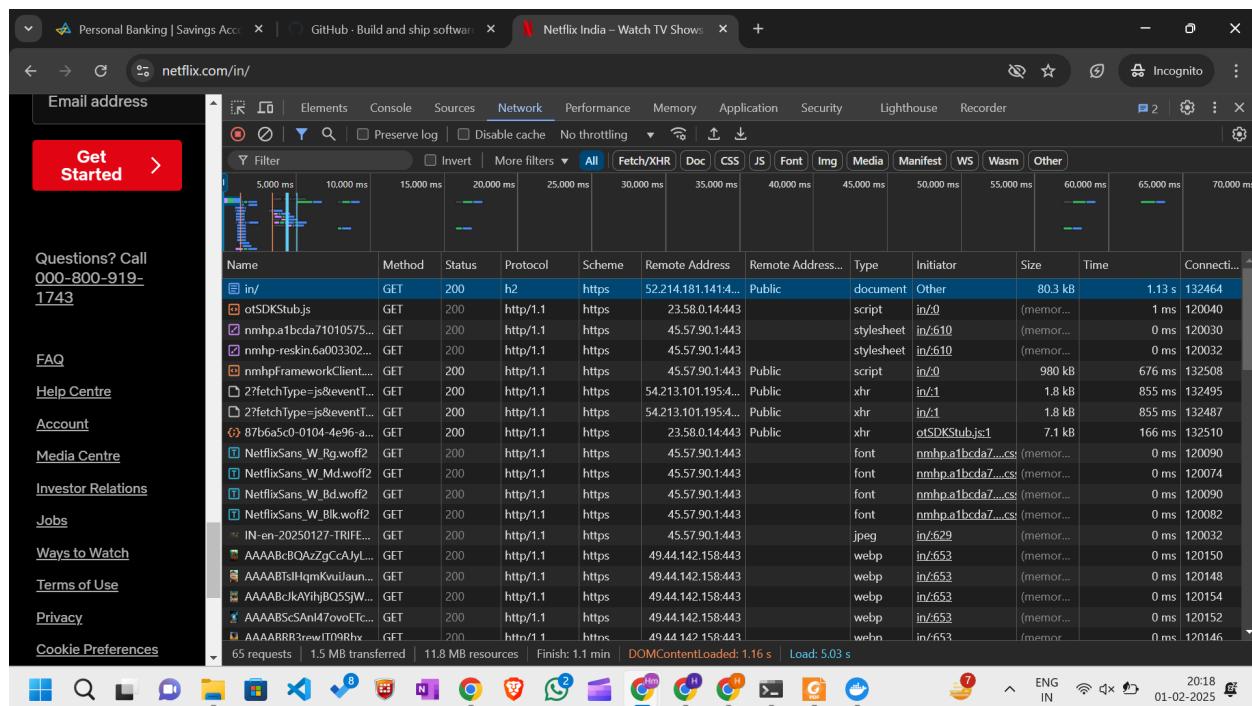
```
Pinging github.com [20.207.73.82] with 32 bytes of data:  
Reply from 20.207.73.82: bytes=32 time=16ms TTL=112  
Reply from 20.207.73.82: bytes=32 time=17ms TTL=112  
Reply from 20.207.73.82: bytes=32 time=39ms TTL=112  
Reply from 20.207.73.82: bytes=32 time=15ms TTL=112  
  
Ping statistics for 20.207.73.82:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 15ms, Maximum = 39ms, Average = 21ms  
PS C:\Users\3malw>
```

## 2. Connection Type:

- **Persistent Connection: NOT SPECIFIED**

## iii. netflix.com

### a. Request Line and Connection Information:



The screenshot shows the Network tab of the Chrome DevTools Performance panel. The left sidebar lists various navigation links for Netflix. The main area displays a timeline of network requests. A table below the timeline provides detailed information for each request, including Name, Method, Status, Protocol, Scheme, Remote Address, Type, Initiator, Size, Time, and Connecti... (partially visible). The table shows numerous requests, primarily GET requests for resources like JavaScript files (e.g., otSDKStub.js), CSS files, fonts (e.g., NetflixSans\_W\_Rg.woff2), and images (e.g., logo icons). Most requests are over HTTPS and return status codes such as 200 or 200 OK. The 'Protocol' column indicates the use of h2 for most requests.

Name	Method	Status	Protocol	Scheme	Remote Address	Type	Initiator	Size	Time	Connecti...	
otSDKStub.js	GET	200	h2	https	52.214.181.141...	Public	document	80.3 kB	1.13 s	132464	
nmhp.a1bcd71010575...	GET	200	http/1.1	https	23.58.0.144:443	script	in/0	(memor...	1 ms	120040	
nmhp-reskin.6a003302...	GET	200	http/1.1	https	45.57.90.1:443	stylesheet	in/610	(memor...	0 ms	120030	
nmhpframeworkClient...	GET	200	http/1.1	https	45.57.90.1:443	script	in/0	980 kB	676 ms	132508	
2?fetchType=js&eventT...	GET	200	http/1.1	https	54.213.101.195:4...	Public	xhr	in/1	1.8 kB	855 ms	132495
2?fetchType=js&eventT...	GET	200	http/1.1	https	54.213.101.195:4...	Public	xhr	in/1	1.8 kB	855 ms	132487
87b6a5c0-0104-4e96-a...	GET	200	http/1.1	https	23.58.0.144:443	Public	xhr	otSDKStub.js:1	7.1 kB	166 ms	132510
NetflixSans_W_Rg.woff2	GET	200	http/1.1	https	45.57.90.1:443	font	nmhp.a1bcd7...cs	(memor...	0 ms	120090	
NetflixSans_W_Md.woff2	GET	200	http/1.1	https	45.57.90.1:443	font	nmhp.a1bcd7...cs	(memor...	0 ms	120074	
NetflixSans_W_Bd.woff2	GET	200	http/1.1	https	45.57.90.1:443	font	nmhp.a1bcd7...cs	(memor...	0 ms	120090	
NetflixSans_W_Blkwoff2	GET	200	http/1.1	https	45.57.90.1:443	font	nmhp.a1bcd7...cs	(memor...	0 ms	120082	
iN-en-20250127-TRIFFE...	GET	200	http/1.1	https	45.57.90.1:443	jpeg	in/629	(memor...	0 ms	120032	
AAAAABcbQazzgcAjl...	GET	200	http/1.1	https	49.44.142.158:443	webp	in/653	(memor...	0 ms	120150	
AAAABTsIHqmKuiJaun...	GET	200	http/1.1	https	49.44.142.158:443	webp	in/653	(memor...	0 ms	120148	
AAAABcbkAyihB0SSJW...	GET	200	http/1.1	https	49.44.142.158:443	webp	in/652	(memor...	0 ms	120154	
AAAABcS-SAn47ovoEtc...	GET	200	http/1.1	https	49.44.142.158:443	webp	in/652	(memor...	0 ms	120152	
AAAARRR3rnewIT9rbx...	GET	200	http/1.1	https	49.44.142.158:443	webn	in/653	(memor...	0 ms	120146	

## 1. Request Line:

- **GET / HTTP/2**
- **Version of Application Layer Protocol:** HTTP/1.1 & HTTP/2 & HTTP/3
- **IP Address:** 52.214.181.141

## 2. Connection Type:

- **Persistent Connection:** Yes

Name	X	Headers	Preview	Response	Initiator	Timing
▼ Response Headers						
Accept-Ranges:		bytes				
Cache-Control:		max-age=604801				
Connection:		keep-alive				
Content-Length:		381520				
Content-Md5:		I/HFKDJPzvfRoBs9IB6BQ=				
Content-Type:		image/jpeg				
Date:		Sat, 01 Feb 2025 14:37:25 GMT				
Expires:		Sat, 08 Feb 2025 14:37:26 GMT				
Last-Modified:		Wed, 29 Jan 2025 16:39:29 GMT				
Server:		nginx				

---

### b. Request and Response Headers, and HTTP Error Codes:

#### Request Header Fields

**accept:**text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/\*/\*;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

**host:** canarabank.com

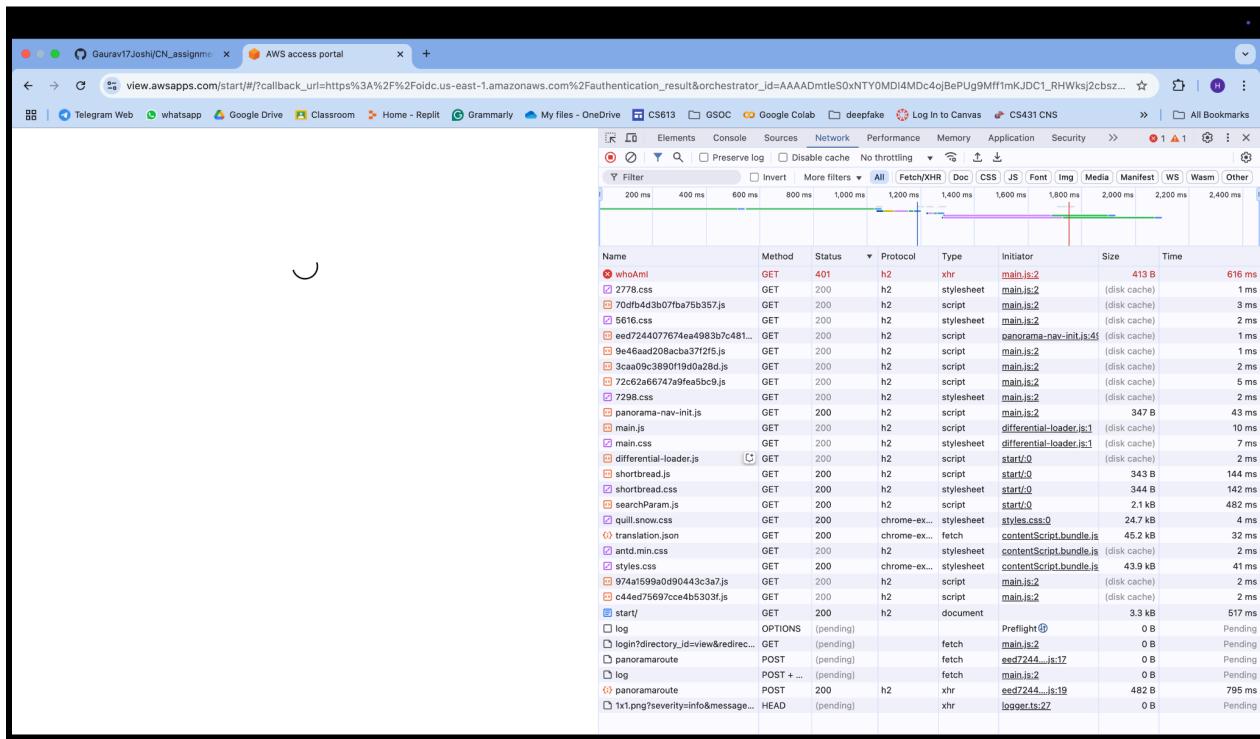
#### Response Header Fields

**cache-control:** public, max-age=36000

**connection:** close

content-type: text/html; charset=utf-8  
 date: Sat, 01 Feb 2025 15:06:44 GMT  
 referrer-policy: no-referrer-when-downgrade

### Error codes:



HTTP Error Codes	Description
401 Unauthorized	It occurs when authentication is required but has either failed or has not been provided. This typically happens when accessing protected resources without valid credentials.

### 307

The screenshot shows the NetworkMiner tool interface. On the left, a tree view lists files under 'Name' with 'canarabank.com' selected. On the right, the 'Headers' tab is active, displaying the following details:

Request URL	GET
Request Method	GET
Status Code	307 Internal Redirect
Referrer Policy	strict-origin-when-cross-origin

Temporary Redirect in HTTP status codes means that the requested resource has been temporarily moved to a different URL.

### 200 OK

The screenshot shows the NetworkMiner tool interface. On the left, a tree view lists files under 'Name' with 'canarabank.com' selected. On the right, the 'Headers' tab is active, displaying the following details:

Request URL	https://canarabank.com/
Request Method	GET
Status Code	200 OK
Remote Address	107.162.160.8:443
Referrer Policy	strict-origin-when-cross-origin

The request has been fulfilled, and the server has returned the requested data.

### 204 NO CONTENT

The screenshot shows the NetworkMiner tool interface. On the left, a tree view lists files under 'Name' with 'hero\_poster\_desktop-sat...'. On the right, the 'Headers' tab is active, displaying the following details:

Request URL	https://collector.github.com/github/collect
Request Method	POST
Status Code	204 No Content
Remote Address	140.82.113.21:443
Referrer Policy	strict-origin-when-cross-origin

No Content response in HTTP status codes indicates that the server has successfully processed the request, but there is no content to return in the response body.

## c. Performance Metrics and Cookies:

### 1. Performance Metrics:

The screenshot shows the Chrome DevTools Performance tab open for the URL `canarabank.com`. The main area displays three performance metrics: Largest Contentful Paint (LCP) at 1.53 s, Cumulative Layout Shift (CLS) at 0.05, and Interaction to Next Paint (INP) at 24 ms. The 'Local metrics' section also includes a table for 'Interactions' and 'Layout shifts'. On the right side, there are sections for 'Field data' and 'Environment settings' with options for CPU and Network throttling.

- **Browser Name:** Google Chrome
- **Website:** canarabank.com
- **Metrics Captured:**
  - **Largest Contentful Paint (LCP):** 1.53 s
  - **Cumulative Layout Shift (CLS):** 0.05
  - **Interaction to Next Paint (INP):** 24ms

### 2. Cookies Used:

- **Website:** canarabank.com

The screenshot shows the Chrome DevTools Application tab with the 'Cookies' section selected. It lists several cookies for the domain `canarabank.com`, including session cookies like `NSC_10.14.241.15_TTM`, `_ga`, and `_gat`, as well as other affinity and tracking cookies. The table includes columns for Name, Value, Domain, Path, Expires /..., Size, HttpOnly, Secure, SameSite, Partition, Cross-Site, and Priority.

Name	Value	Domain	Path	Expires /...	Size	HttpOnly	Secure	SameSite	Partition	Cross-Site	Priority
NSC_10.14.241.15_TTM	ffffffff0906ef154552...	canarabank.com	/	2025-02...	64	✓	✓				Medi...
appgw-affinity-ec53ae87...	d315eedd7310d482...	cabprod.gupshup.io	/	Session	83		✓	None			Medi...
_ga	GS1.1.173842405.1...	.canarabank.com	/	2026-03...	52						Medi...
_ga	GA1.1.1369761165.1...	.canarabank.com	/	2026-03...	30						Medi...
appgw-affinity-ec53a...	16fb91ff2936af0...	cabprod.gupshup.io	/	Session	83		✓	None			Medi...
appgw-affinity-ec53a...	16fbe91ff2936af0...	cabprod.gupshup.io	/	Session	79						Medi...
TSbef164a027	0805f09e8cab20001...	canarabank.com	/	Session	205						Medi...
TS019d7cd7	0162b8d0d9dd60fed...	canarabank.com	/	Session	116	✓	✓				Medi...

Cookie Name	Value	flag
TS019d7cd7	0162b8d0d9dd60fed8b8 046afbedbd7757d8125d cbe2ea466c47dcf9e418 b46f58b799f744cf4dbb6 5896a877cce75396b226 79df1	Secure, HTTPOnly
TSbefef164a027	0805f09e8cab200017ed f0db3fa546e7d430384b 5915088891915d47fe5d 6a06441731297b578b1 b0824f1b9e71130002c8 80b9d77251dee91b82fc 524de55633ff328d10a8 5dc50e3b8cc17a8679d6 3791328f073cebe78178 463d4c305a4f4	
NSC_10.14.241.15_TTM	ffffffff0906ef1545525d5f4f 58455e445a4a4216cb	Secure, HTTPOnly
_ga_MD86BV0YCY	GS1.1.1738422405.1.1.1 738423752.53.0.0	
_ga	GA1.1.1369761165.1738 422405	