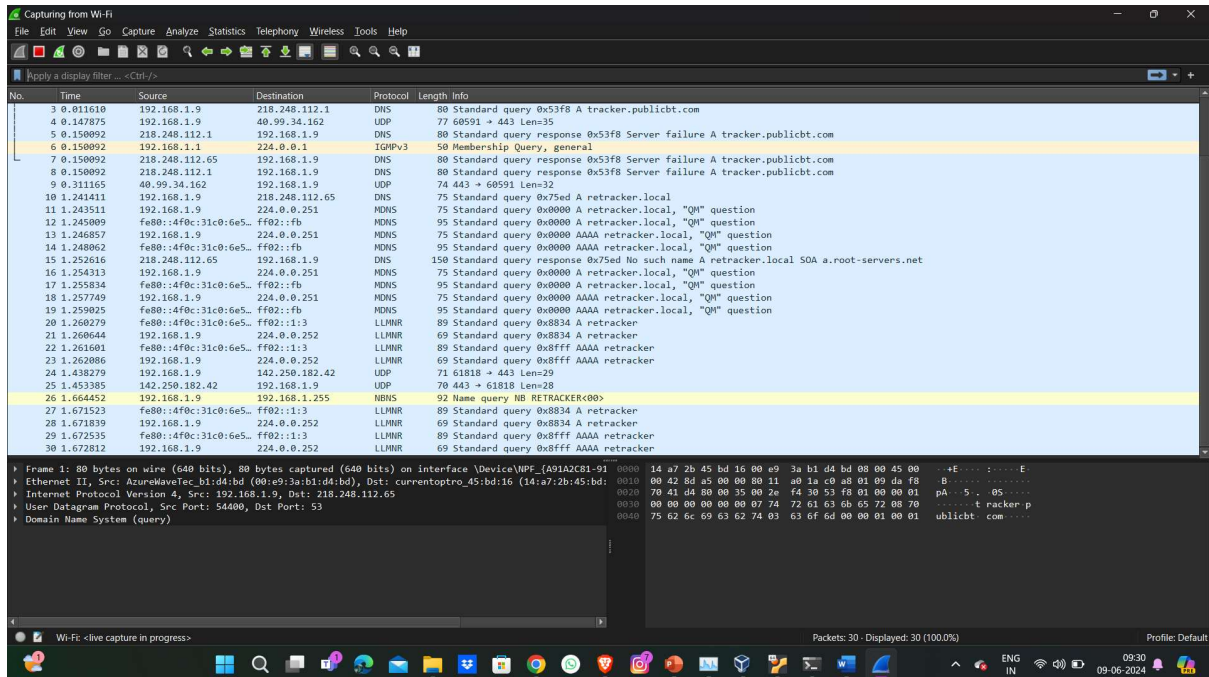


Assignment -2 (wireshark) solutions:

1) Install Wireshark, take capture on WiFi interface

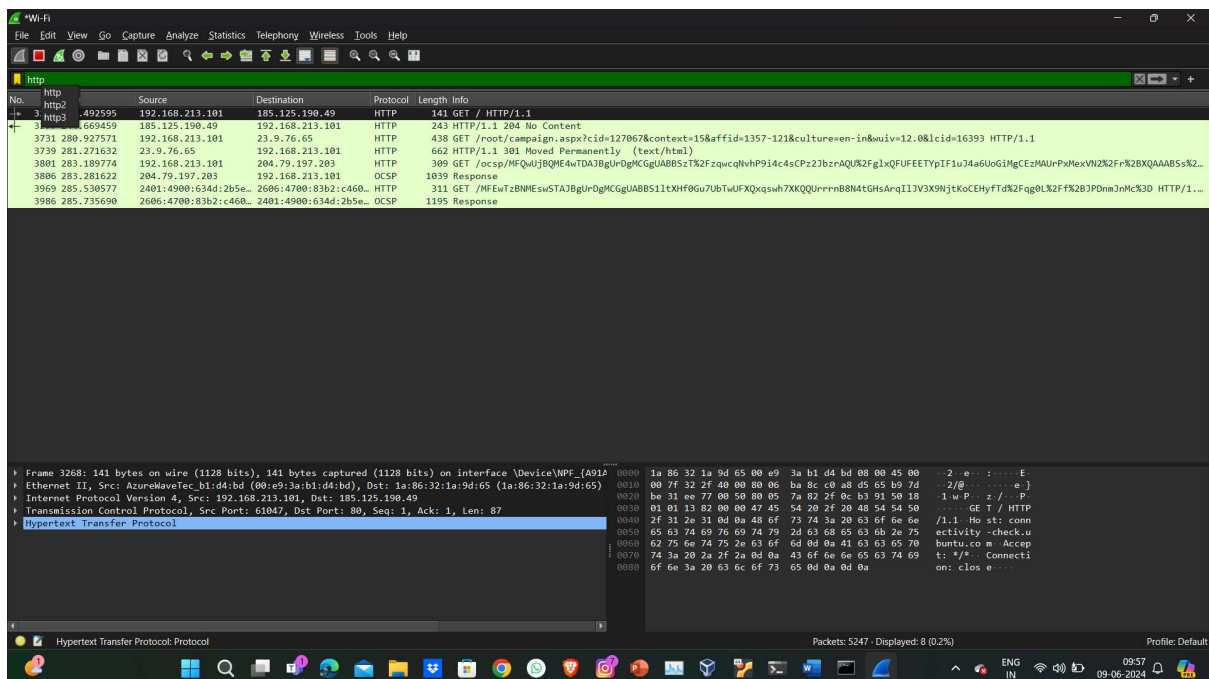
Capture on wifi interface.



1. Identify the beacon frame using filter.

2. Apply filters to view specific packet.

HTTP PACKETS



TCP PACKETS

Wireshark packet capture showing TCP traffic. The packet list pane displays a list of packets, with packet 6671 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 6, Transmission Control Protocol, and Transport Layer Security. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
6657	385.765182	192.168.213.101	13.107.42.12	TCP	54	61108 → 443 [ACK] Seq=270906 Ack=8035 Win=65024 Len=0
6658	386.887274	192.168.213.101	13.107.42.12	TLSv1.2	657	Application Data
6659	386.887447	192.168.213.101	13.107.42.12	TCP	305	Application Data
6660	387.016705	13.107.42.12	192.168.213.101	TCP	54	443 → 60838 [ACK] Seq=20030 Ack=18789 Win=16384 Len=0
6661	387.281560	13.107.42.12	192.168.213.101	TLSv1.2	948	Application Data
6662	387.281560	13.107.42.12	192.168.213.101	TLSv1.2	111	Application Data
6663	387.281635	192.168.213.101	13.107.42.12	TCP	54	60838 → 443 [ACK] Seq=18789 Ack=20981 Win=257 Len=0
6667	388.368803	2603:1063:2202:14::3	2401:4900:634d:2b5e::	TLSv1.2	107	Application Data
6668	388.409679	2401:4900:634d:2b5e::	2603:1063:2202:14::3	TCP	74	60752 → 443 [ACK] Seq=1 Ack=826 Win=257 Len=0
6669	388.746852	221.224.86.173	192.168.213.101	TCP	54	[TCP Keep-Alive] 1988 → 60929 [ACK] Seq=1 Ack=25 Win=502 Len=0
6670	388.746888	192.168.213.101	221.224.86.173	TCP	54	[TCP Keep-Alive ACK] 60929 → 1988 [ACK] Seq=25 Ack=2 Win=257 Len=0
6671	390.492930	2603:1063:2202:14::3	2401:4900:634d:2b5e::	TLSv1.2	107	Application Data
6672	390.533474	2401:4900:634d:2b5e::	2603:1063:2202:14::3	TCP	74	60749 → 443 [ACK] Seq=789 Ack=908 Win=257 Len=0
6673	392.230879	2401:4900:634d:2b5e::	2603:1040:a06:6::	TLSv1.2	117	Application Data
6676	392.345645	2603:1040:a06:6::	2401:4900:634d:2b5e::	TLSv1.2	248	Application Data
6677	392.386910	2401:4900:634d:2b5e::	2603:1040:a06:6::	TCP	74	60763 → 443 [ACK] Seq=653 Ack=4305 Win=258 Len=0
6678	392.462631	2401:4900:634d:2b5e::	2404:6800:4003:c04::	TCP	75	[TCP Keep-Alive] 60781 → 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1
6679	392.520271	2404:6800:4003:c04::	2401:4900:634d:2b5e::	TCP	86	[TCP Keep-Alive ACK] 5228 → 60781 [ACK] Seq=1 Ack=2 Win=289 Len=0 SLE=1 SRE=2
6684	395.285992	192.168.213.101	13.107.42.12	TLSv1.2	657	Application Data
6685	395.286178	192.168.213.101	13.107.42.12	TCP	305	Application Data
6686	395.390579	13.107.42.12	192.168.213.101	TCP	54	443 → 60838 [ACK] Seq=20981 Ack=19392 Win=16382 Len=0
6687	395.390579	13.107.42.12	192.168.213.101	TCP	54	443 → 60838 [ACK] Seq=20981 Ack=19643 Win=16381 Len=0
6690	395.656722	13.107.42.12	192.168.213.101	TLSv1.2	948	Application Data
6691	395.656722	13.107.42.12	192.168.213.101	TLSv1.2	111	Application Data
6692	395.656809	192.168.213.101	13.107.42.12	TCP	54	60838 → 443 [ACK] Seq=19643 Ack=21932 Win=253 Len=0
6693	397.629805	192.168.213.101	40.70.77.100	TCP	54	61079 → 443 [FIN, ACK] Seq=1301 Ack=1302 Win=58024 Len=0
6695	397.926103	40.70.77.100	192.168.213.101	TCP	54	443 → 61079 [FIN, ACK] Seq=3102 Ack=1302 Win=523520 Len=0
6696	397.926147	192.168.213.101	40.70.77.100	TCP	54	61079 → 443 [ACK] Seq=1302 Ack=3103 Win=58024 Len=0

Frame 6671: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface \Device\NPF_{A91A2C...} Ethernet II, Src: 1a:86:32:1a:9d:65 (1a:86:32:1a:9d:65), Dst: AzureWaveTec_b1:d4:bd (00:e9:3a:b1:d4:bd)

Internet Protocol Version 6, Src: 2603:1063:2202:14::3, Dst: 2401:4900:634d:2b5e::9959:22a4:ec87:97c4

Transmission Control Protocol, Src Port: 443, Dst Port: 60749, Seq: 875, Ack: 789, Len: 33

Transport Layer Security

Packets specifically from or to the ip address “192.168.213.101”

Wireshark packet capture showing TCP traffic filtered by IP address 192.168.213.101. The packet list pane displays a list of packets, with packet 6662 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
6653	385.419114	192.168.213.101	13.107.42.12	TLSv1.3	967	Application Data
6654	385.454337	13.107.42.12	192.168.213.101	TCP	54	443 → 61108 [ACK] Seq=7268 Ack=269993 Win=4194304 Len=0
6655	385.459924	13.107.42.12	192.168.213.101	TCP	54	443 → 61108 [ACK] Seq=7268 Ack=270906 Win=4193280 Len=0
6656	385.723418	13.107.42.12	192.168.213.101	TLSv1.3	821	Application Data
6657	385.765182	192.168.213.101	13.107.42.12	TCP	54	61108 → 443 [ACK] Seq=270906 Ack=8035 Win=65024 Len=0
6658	386.887274	192.168.213.101	13.107.42.12	TLSv1.2	657	Application Data
6659	386.887447	192.168.213.101	13.107.42.12	TCP	305	Application Data
6660	387.016705	13.107.42.12	192.168.213.101	TCP	54	443 → 60838 [ACK] Seq=20030 Ack=18789 Win=16384 Len=0
6661	387.281560	13.107.42.12	192.168.213.101	TLSv1.2	948	Application Data
6662	387.281560	13.107.42.12	192.168.213.101	TLSv1.2	111	Application Data
6663	387.281635	192.168.213.101	13.107.42.12	TCP	54	60838 → 443 [ACK] Seq=18789 Ack=20981 Win=257 Len=0
6664	387.714318	192.168.213.101	94.41.238.199	BT-DHT	146	Get_peers Info_hash=5da1a960b6a5766e02b3e8f816229eca45607390
6665	388.056884	94.41.238.199	192.168.213.101	BT-DHT	359	Response Nodes=8
6669	388.746852	221.224.86.173	192.168.213.101	TCP	54	[TCP Keep-Alive] 1988 → 60929 [ACK] Seq=1 Ack=25 Win=502 Len=0
6670	388.746888	192.168.213.101	221.224.86.173	TCP	54	[TCP Keep-Alive ACK] 60929 → 1988 [ACK] Seq=25 Ack=2 Win=257 Len=0
6680	392.715153	192.168.213.101	18.223.137.220	BT-DHT	146	Get_peers Info_hash=5dalaalcea46ced3dfb86139404e3323eb0424e0
6681	394.011571	18.223.137.220	192.168.213.101	BT-DHT	118	Response Nodes=0
6682	394.651494	94.41.238.199	192.168.213.101	BT-DHT	145	Find_node Target=5da1a9d0f00000f710000149c00007a00000002389
6683	394.651829	192.168.213.101	94.41.238.199	BT-DHT	341	Response Nodes=8
6684	395.285992	192.168.213.101	13.107.42.12	TLSv1.2	657	Application Data
6685	395.286178	192.168.213.101	13.107.42.12	TLSv1.2	305	Application Data
6686	395.390579	13.107.42.12	192.168.213.101	TCP	54	443 → 60838 [ACK] Seq=20981 Ack=19392 Win=16382 Len=0
6687	395.390579	13.107.42.12	192.168.213.101	TCP	54	443 → 60838 [ACK] Seq=20981 Ack=19643 Win=16381 Len=0
6690	395.656722	13.107.42.12	192.168.213.101	TLSv1.2	948	Application Data
6691	395.656722	13.107.42.12	192.168.213.101	TLSv1.2	111	Application Data
6692	395.656809	192.168.213.101	13.107.42.12	TCP	54	60838 → 443 [ACK] Seq=19643 Ack=21932 Win=253 Len=0
6693	397.629805	192.168.213.101	40.70.77.100	TCP	54	61079 → 443 [FIN, ACK] Seq=1301 Ack=3102 Win=58024 Len=0
6694	397.715802	192.168.213.101	177.245.155.47	BT-DHT	146	Get_peers Info_hash=5da1a9421afdd65b442d4bcb19453a87bb310a0

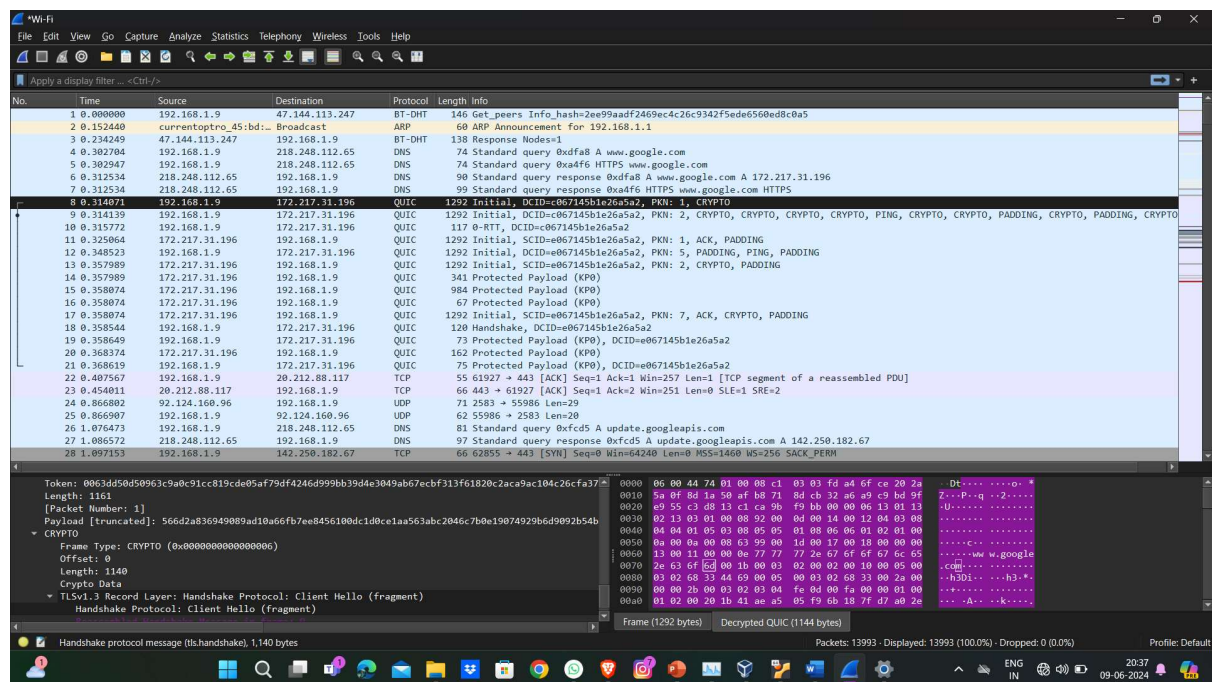
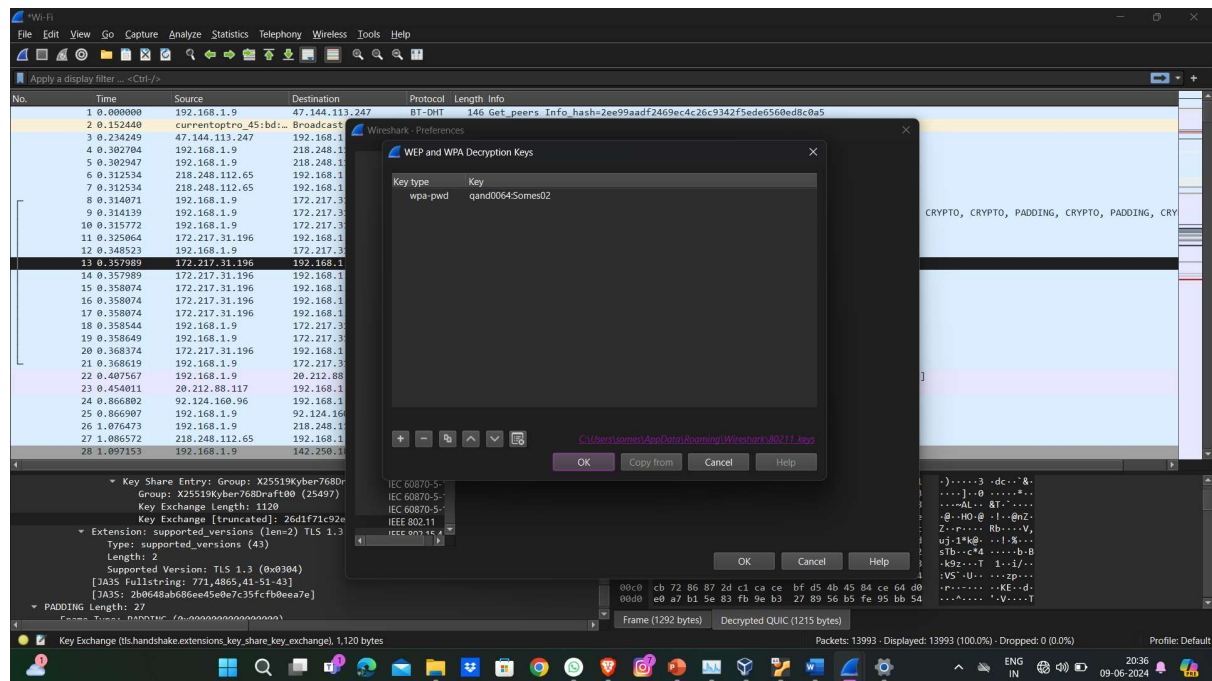
Frame 6662: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface \Device\NPF_{A91A2C...} Ethernet II, Src: 1a:86:32:1a:9d:65 (1a:86:32:1a:9d:65), Dst: AzureWaveTec_b1:d4:bd (00:e9:3a:b1:d4:bd)

Internet Protocol Version 4, Src: 13.107.42.12, Dst: 192.168.213.101

Transmission Control Protocol, Src Port: 443, Dst Port: 60838, Seq: 20924, Ack: 18789, Len: 57

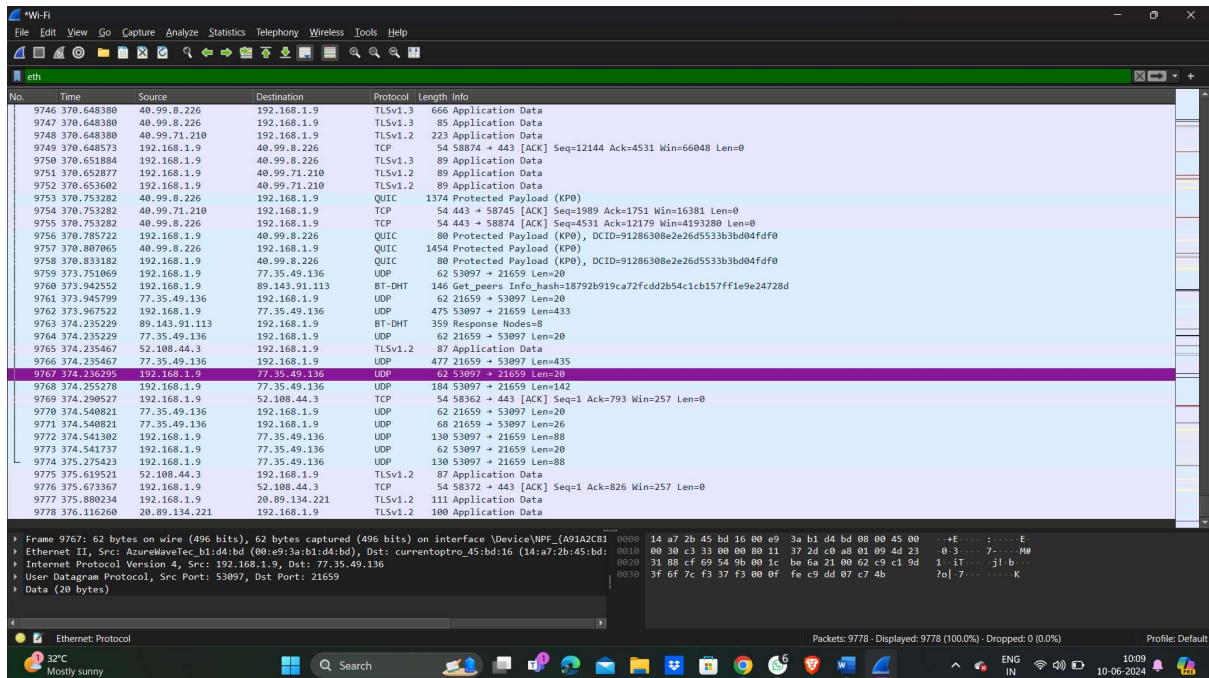
Transport Layer Security

3. Decrypt the wireshark pcap using passphrase, to view the encrypted packets.



5. Point out ethernet and 802.11 frames.

Ethernet frames



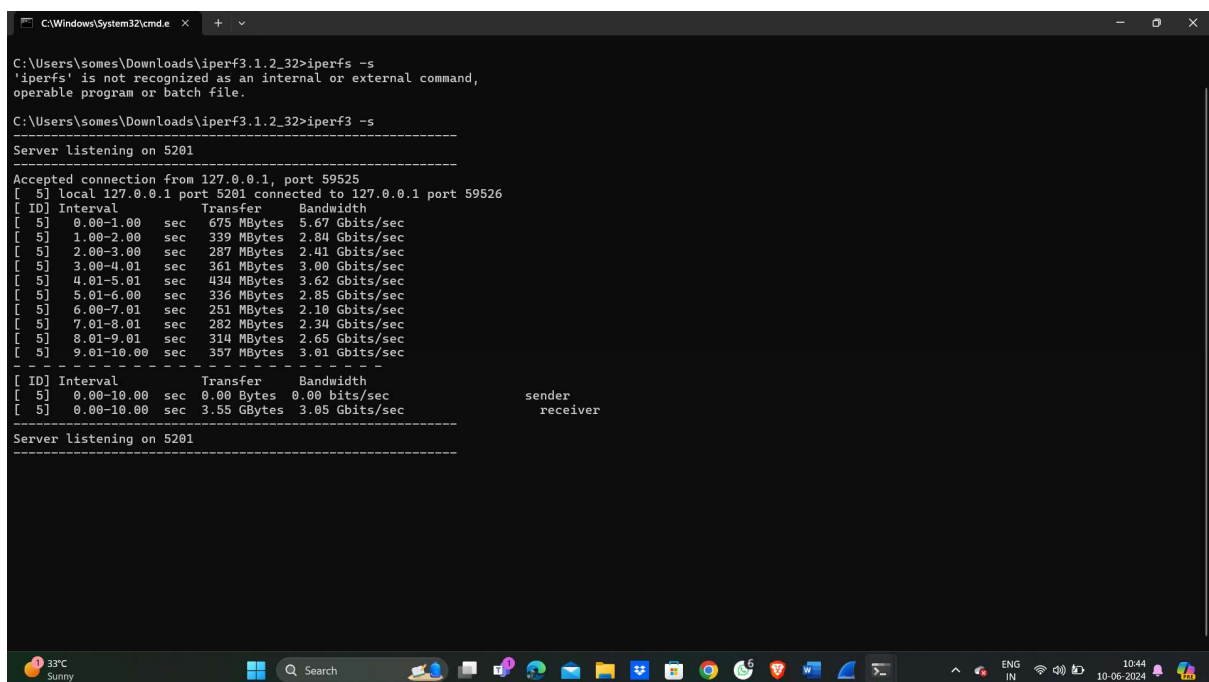
2) Install Iperf on client and server device

1. Run TCP traffic

2. Run UDP traffic

Check for the bandwidth and drops reported in the results.

TCP traffic - server



TCP traffic – client.

```
Command Prompt
Microsoft Windows [Version 10.0.22631.3593]
(c) Microsoft Corporation. All rights reserved.

C:\Users\somes>cd C:\Users\somes\Downloads\iperf3.1.2_32

C:\Users\somes\Downloads\iperf3.1.2_32>iperf3 -c 127.0.0.1
Connecting to host 127.0.0.1, port 5201
[ 4] local 127.0.0.1 port 59526 connected to 127.0.0.1 port 5201
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-1.00 sec    676 MBytes  5.67 Gbits/sec
[ 4] 1.00-2.00 sec    338 MBytes  2.84 Gbits/sec
[ 4] 2.00-3.00 sec    287 MBytes  2.41 Gbits/sec
[ 4] 3.00-4.01 sec    360 MBytes  3.00 Gbits/sec
[ 4] 4.01-5.01 sec    434 MBytes  3.62 Gbits/sec
[ 4] 5.01-6.00 sec    336 MBytes  2.85 Gbits/sec
[ 4] 6.00-7.01 sec    251 MBytes  2.10 Gbits/sec
[ 4] 7.01-8.00 sec    282 MBytes  2.38 Gbits/sec
[ 4] 8.00-9.01 sec    314 MBytes  2.61 Gbits/sec
[ 4] 9.01-10.00 sec   357 MBytes  3.01 Gbits/sec
-----
[ ID] Interval      Transfer    Bandwidth          sender
[ 4] 0.00-10.00 sec  3.55 GBytes  3.05 Gbits/sec      receiver
[ 4] 0.00-10.00 sec  3.55 GBytes  3.05 Gbits/sec

iperf Done.

C:\Users\somes\Downloads\iperf3.1.2_32>
```

UDP traffic

UDP traffic server

```
C:\Windows\System32\cmd.exe
[HMKG] indicates options that support a K/M/G suffix for kilo-, mega-, or giga-

iperf3 homepage at: http://software.es.net/iperf/
Report bugs to: https://github.com/esnet/iperf

C:\Users\somes\Downloads\iperf3.1.2_32>iperf3 -s
Server listening on 5201
Accepted connection from 127.0.0.1, port 59567
[ 5] local 127.0.0.1 port 5201 connected to 127.0.0.1 port 59566
[ ID] Interval      Transfer    Bandwidth    Jitter    Lost/Total Datagrams
[ 5] 0.00-1.00 sec    120 KBytes  981 Kbits/sec  0.033 ms  0/15 (0%)
[ 5] 1.00-2.01 sec    128 KBytes  1.04 Mbits/sec  0.086 ms  0/16 (0%)
[ 5] 2.01-3.00 sec    128 KBytes  1.05 Mbits/sec  0.061 ms  0/16 (0%)
[ 5] 3.00-4.01 sec    128 KBytes  1.04 Mbits/sec  0.046 ms  0/16 (0%)
[ 5] 4.01-5.01 sec    128 KBytes  1.05 Mbits/sec  0.051 ms  0/16 (0%)
[ 5] 5.01-6.00 sec    128 KBytes  1.05 Mbits/sec  0.063 ms  0/16 (0%)
[ 5] 6.00-7.01 sec    128 KBytes  1.04 Mbits/sec  0.059 ms  0/16 (0%)
[ 5] 7.01-8.00 sec    128 KBytes  1.06 Mbits/sec  0.072 ms  0/16 (0%)
[ 5] 8.00-9.01 sec    128 KBytes  1.04 Mbits/sec  0.056 ms  0/16 (0%)
[ 5] 9.01-10.01 sec   128 KBytes  1.06 Mbits/sec  0.054 ms  0/16 (0%)
[ 5] 10.01-10.01 sec   0.00 Bytes  0.00 bits/sec  0.054 ms  0/0 (0%)
-----
[ ID] Interval      Transfer    Bandwidth    Jitter    Lost/Total Datagrams
[ 5] 0.00-10.01 sec   0.00 Bytes  0.00 bits/sec  0.054 ms  0/159 (0%)

Server listening on 5201
```

UDP traffic client

```
C:\Windows\System32\cmd.e
Microsoft Windows [Version 10.0.22631.3593]
(c) Microsoft Corporation. All rights reserved.

C:\Users\somes\Downloads\iperf3.1.2_32>iperf3 -c 127.0.0.1 -u
Connecting to host 127.0.0.1, port 5201
[ 4] local 127.0.0.1 port 50566 connected to 127.0.0.1 port 5201
[ ID] Interval      Transfer    Bandwidth  Total Datagrams
[ 4] 0.00-1.00 sec  128 KBytes  981 Kbits/sec  15
[ 4] 1.00-2.01 sec  128 KBytes  1.04 Mbits/sec  16
[ 4] 2.01-3.00 sec  128 KBytes  1.05 Mbits/sec  16
[ 4] 3.00-4.01 sec  128 KBytes  1.04 Mbits/sec  16
[ 4] 4.01-5.01 sec  128 KBytes  1.05 Mbits/sec  16
[ 4] 5.01-6.00 sec  128 KBytes  1.05 Mbits/sec  16
[ 4] 6.00-7.01 sec  128 KBytes  1.04 Mbits/sec  16
[ 4] 7.01-8.00 sec  128 KBytes  1.06 Mbits/sec  16
[ 4] 8.00-9.01 sec  128 KBytes  1.04 Mbits/sec  16
[ 4] 9.01-10.01 sec 128 KBytes  1.06 Mbits/sec  16
-----
[ ID] Interval      Transfer    Bandwidth  Jitter    Lost/Total Datagrams
[ 4] 0.00-10.01 sec 1.24 MBytes  1.04 Mbits/sec  0.054 ms  0/159 (0%)
[ 4] Sent 159 datagrams

iperf Done.

C:\Users\somes\Downloads\iperf3.1.2_32>
```