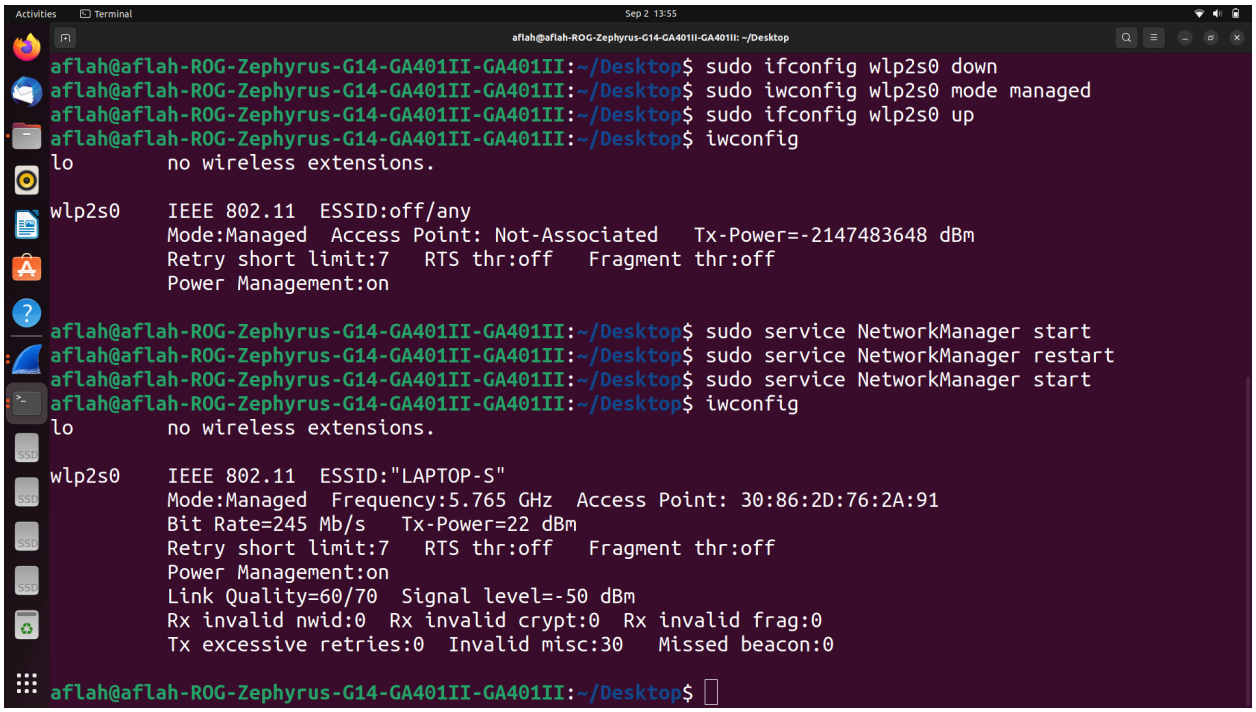
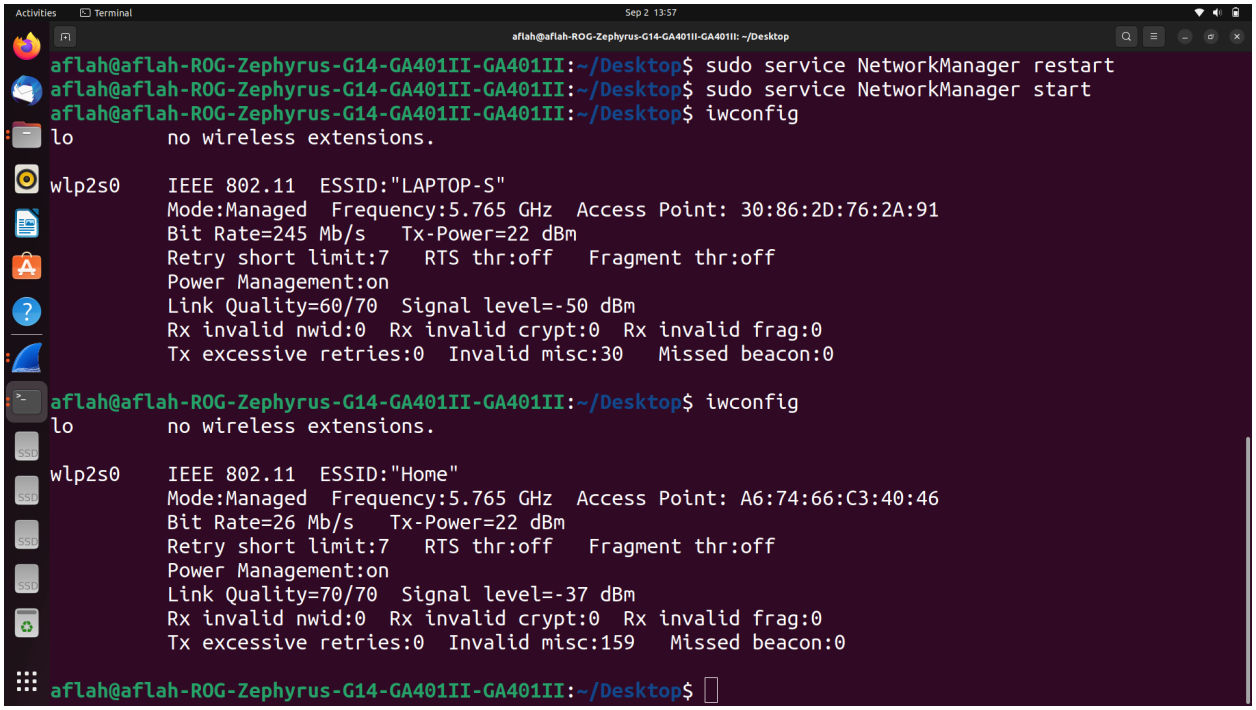
Wireless Networks
Assignment 1

Mohammad Aflah Khan
2020082

Q1.



SSID - Laptop-S
BSSID - 30:86:2D:76:2A:91
Signal Strength - (-50) dBm
Bit-Rate - 245 Mbps
Transmission Power - 22 dBm
Operating Frequency Band - 5.765 GHz



```
aflah@aflah-ROG-Zephyrus-G14-GA401II-GA401II:~/Desktop$ sudo service NetworkManager restart
aflah@aflah-ROG-Zephyrus-G14-GA401II-GA401II:~/Desktop$ sudo service NetworkManager start
aflah@aflah-ROG-Zephyrus-G14-GA401II-GA401II:~/Desktop$ iwconfig
lo        no wireless extensions.

wlp2s0    IEEE 802.11  ESSID:"LAPTOP-S"
          Mode:Managed  Frequency:5.765 GHz  Access Point: 30:86:2D:76:2A:91
          Bit Rate=245 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=60/70  Signal level=-50 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:30   Missed beacon:0

aflah@aflah-ROG-Zephyrus-G14-GA401II-GA401II:~/Desktop$ iwconfig
lo        no wireless extensions.

wlp2s0    IEEE 802.11  ESSID:"Home"
          Mode:Managed  Frequency:5.765 GHz  Access Point: A6:74:66:C3:40:46
          Bit Rate=26 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=70/70  Signal level=-37 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:159   Missed beacon:0

aflah@aflah-ROG-Zephyrus-G14-GA401II-GA401II:~/Desktop$
```

(Refer to second command, first command was run when connected to different WiFi)

SSID - Home
BSSID - A6:74:66:C3:40:46
Signal Strength - (-37) dBm
Bit-Rate - 26 Mbps
Transmission Power - 22 dBm
Operating Frequency Band - 5.765 GHz

Analysis of Different Fields:

- SSID & BSSID: Different as we're connected to 2 different WiFis
- Signal Strength: Different and lower for mobile hotspot as it is not a dedicated access point as compared to IIIT's WiFi Routers. Note that even though the mobile is closer than access point, the access point reading is still stronger
- Bit-Rate: IIIT's access point uses better modulation and coding schemes which probably reads to elevated BitRates there

Q2.

a.) Count of Unique MAC Addresses: 12792
Count of Unique Access Points: 142
Count of Unique Clients: 12757

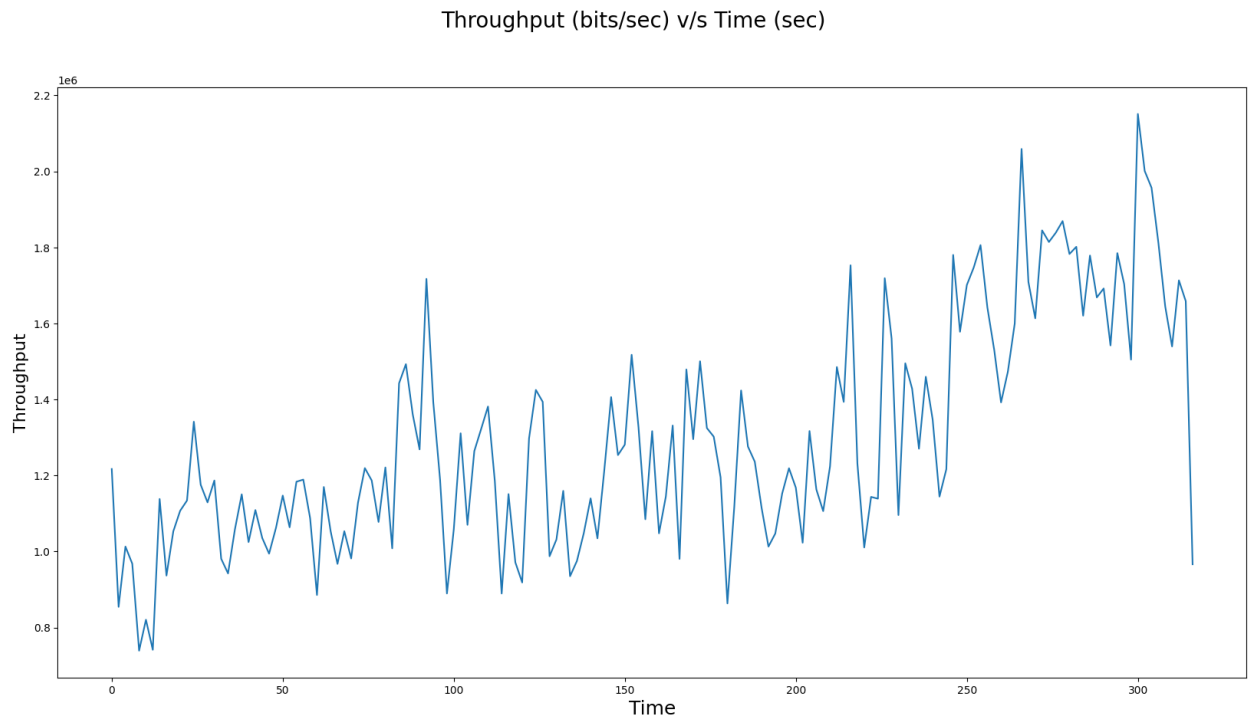
b.) Average Signal Strength details in the attached client_data.csv file

c.) Average Bitrate details in the attached client_data.csv file

d.) Number of Clients per Standard:

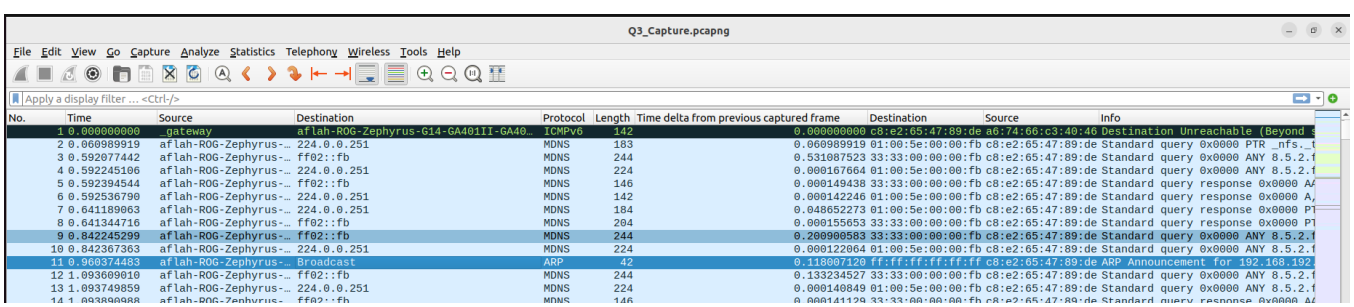
- 802.11g: 203018
- 802.11b: 5373
- 802.11n: 18320

e.) Aggregate Throughput:



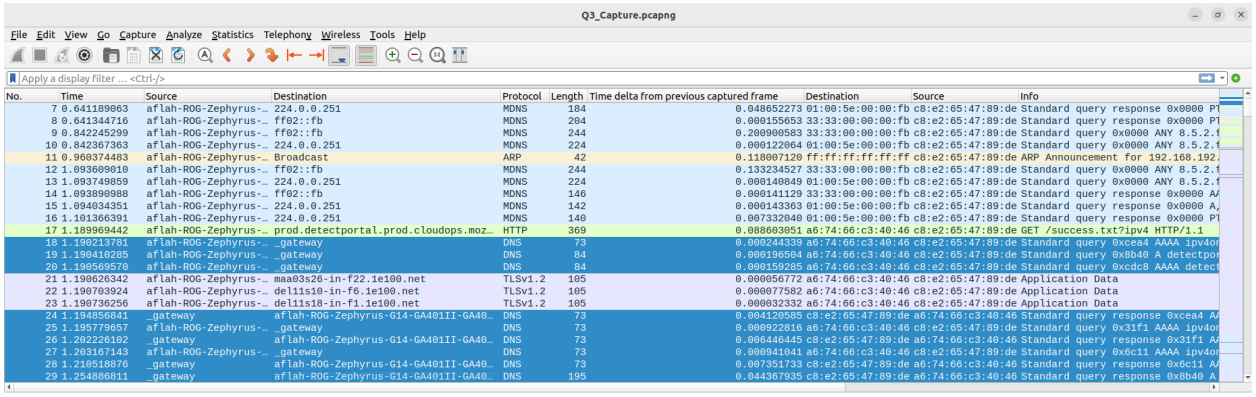
Q3.

a.) Upon the initial connection to a hotspot, Wireshark captures an ARP broadcast with the purpose of identifying the addresses associated with the access point (mobile) within the network.



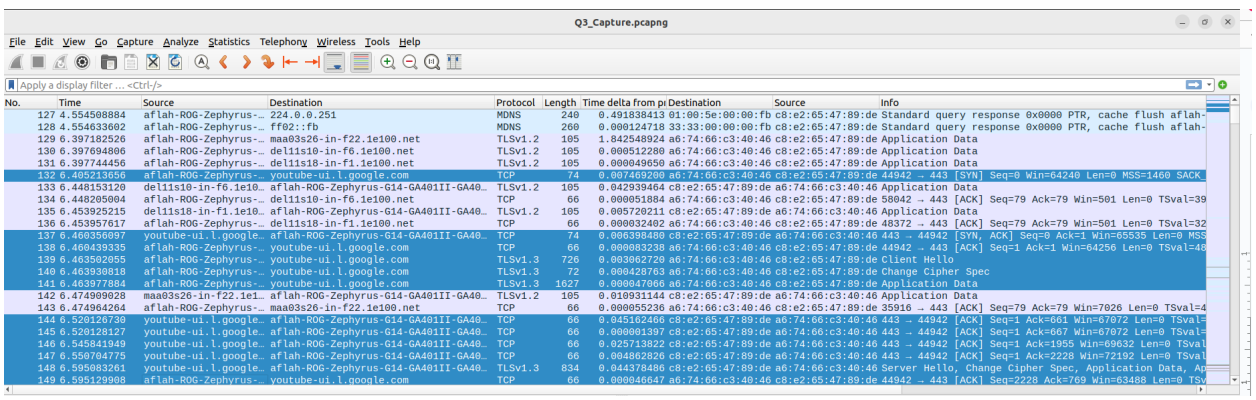
No.	Time	Source	Destination	Protocol	Length	Time delta from previous captured frame	Destination	Source	Info
1	0.000000000	_gateway	aflah-ROG-Zephyrus-G14-GA401II-GA40…	ICMPv6	142	0.000000000	c8:e2:65:47:89:de	a0:74:66:c3:40:46	Destination Unreachable (Beyond S
2	0.060989919	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	183	0.060989919	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 PTR _nfs._t
3	0.592077442	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	244	0.531987523	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
4	0.592245106	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	224	0.000167664	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
5	0.592394544	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	146	0.000149438	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 A
6	0.592536790	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	142	0.000142246	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 A,
7	0.641189063	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	184	0.048652273	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 PT
8	0.641344716	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	204	0.000155653	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 PT
9	0.842245299	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	244	0.200900583	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
10	0.842367363	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	224	0.000122064	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
11	0.960374483	aflah-ROG-Zephyrus-…	Broadcast	ARP	42	0.118007120	ff:ff:ff:ff:ff:ff	c8:e2:65:47:89:de	ARP Announcement for 192.168.192
12	1.093609010	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	244	0.133234527	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
13	1.093749859	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	224	0.000140849	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
14	1.093890988	aflah-ROG-Zephyrus-	ff02::fb	MDNS	146	0.000141129	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 A

This is followed by DNS Resolution. Since mobile's hotspot will also be in use by it's internal services like app updates etc. which run in the background there are several DNS requests. One of them will correspond to our youtube request -



No.	Time	Source	Destination	Protocol	Length	Time delta from previous captured frame	Destination	Source	Info
7	0.641189063	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	184	0.048652273	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 PT
8	0.641344716	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	204	0.000155653	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 PT
9	0.842245299	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	244	0.200900583	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
10	0.842367363	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	224	0.000122064	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
11	0.960374483	aflah-ROG-Zephyrus-…	Broadcast	ARP	42	0.118007120	ff:ff:ff:ff:ff:ff	c8:e2:65:47:89:de	ARP Announcement for 192.168.192.
12	1.093609010	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	244	0.133234527	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
13	1.093749859	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	224	0.000140849	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query 0x0000 ANY 8.5.2.1
14	1.093899988	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	146	0.000141129	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 A/
15	1.094034351	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	142	0.000143363	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 A,
16	1.101366391	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	140	0.007332040	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 PT
17	1.189969442	aflah-ROG-Zephyrus-…	prod.detectportal.prod.cloudops.moz…	HTTP	369	0.088603051	a6:74:66:c3:40:46	c8:e2:65:47:89:de	GET /success.txt?ipv4 HTTP/1.1
18	1.190213781	aflah-ROG-Zephyrus-…	_gateway	DNS	73	0.000244339	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Standard query 0xcea4 AAAA ipv4or
19	1.190410285	aflah-ROG-Zephyrus-…	_gateway	DNS	84	0.000196504	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Standard query 0x8b40 A detectpor
20	1.190569570	aflah-ROG-Zephyrus-…	_gateway	DNS	84	0.000159285	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Standard query 0xcdc8 AAAA detect
21	1.190626342	aflah-ROG-Zephyrus-…	maa03s26-in-f22.1e100.net	TLSv1.2	105	0.000056772	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Application Data
22	1.190703924	aflah-ROG-Zephyrus-…	del11s10-in-f6.1e100.net	TLSv1.2	105	0.000077582	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Application Data
23	1.190736256	aflah-ROG-Zephyrus-…	del11s18-in-f1.1e100.net	TLSv1.2	105	0.000032332	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Application Data
24	1.194856841	_gateway	aflah-ROG-Zephyrus-G14-GA401II-GA40…	DNS	73	0.004120585	c8:e2:65:47:89:de	a6:74:66:c3:40:46	Standard query response 0xcea4 AA
25	1.195779657	aflah-ROG-Zephyrus-…	_gateway	DNS	73	0.000922816	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Standard query 0x31f1 AAAA ipv4or
26	1.202226102	_gateway	aflah-ROG-Zephyrus-G14-GA401II-GA40…	DNS	73	0.006446445	c8:e2:65:47:89:de	a6:74:66:c3:40:46	Standard query response 0x31f1 AA
27	1.203167143	aflah-ROG-Zephyrus-…	_gateway	DNS	73	0.000941041	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Standard query 0x6c11 AAAA ipv4or
28	1.210518876	_gateway	aflah-ROG-Zephyrus-G14-GA401II-GA40…	DNS	73	0.007351733	c8:e2:65:47:89:de	a6:74:66:c3:40:46	Standard query response 0x6c11 AA
29	1.254886811	_gateway	aflah-ROG-Zephyrus-G14-GA401II-GA40…	DNS	195	0.044367935	c8:e2:65:47:89:de	a6:74:66:c3:40:46	Standard query response 0x8b40 A

After this we can see a SYN packet being sent and a SYN ACK being received which corresponds to connection establishment with Youtube. We see a Client Hello using TLSv1.3, some exchange of data for presumably starting actual transfer and then we start to receive actual data frames as seen below -



No.	Time	Source	Destination	Protocol	Length	Time delta from pr	Destination	Source	Info
127	4.554508884	aflah-ROG-Zephyrus-…	224.0.0.251	MDNS	240	0.491838413	01:00:5e:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 PTR, cache flush aflah-
128	4.554633602	aflah-ROG-Zephyrus-…	ff02::fb	MDNS	260	0.000124718	33:33:00:00:00:fb	c8:e2:65:47:89:de	Standard query response 0x0000 PTR, cache flush aflah-
129	6.397182526	aflah-ROG-Zephyrus-…	maa03s26-in-f22.1e100.net	TLSv1.2	105	1.842548924	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Application Data
130	6.397694806	aflah-ROG-Zephyrus-…	del11s10-in-f6.1e100.net	TLSv1.2	105	0.000512280	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Application Data
131	6.397744456	aflah-ROG-Zephyrus-…	del11s18-in-f1.1e100.net	TLSv1.2	105	0.000049650	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Application Data
132	6.405213656	aflah-ROG-Zephyrus-…	youtube-ui.l.google.com	TCP	74	0.007663206	a6:74:66:c3:40:46	c8:e2:65:47:89:de	44942 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
133	6.448153120	del11s10-in-f6.1e10…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TLSv1.2	105	0.042939464	c8:e2:65:47:89:de	a6:74:66:c3:40:46	Application Data
134	6.448205004	aflah-ROG-Zephyrus-…	del11s10-in-f6.1e100.net	TCP	66	0.000051884	a6:74:66:c3:40:46	c8:e2:65:47:89:de	58042 → 443 [ACK] Seq=79 Ack=79 Win=501 Len=0 TSval=39
135	6.453925215	del11s18-in-f1.1e10…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TLSv1.2	105	0.005720211	c8:e2:65:47:89:de	a6:74:66:c3:40:46	Application Data
136	6.453957617	aflah-ROG-Zephyrus-…	del11s18-in-f1.1e100.net	TCP	66	0.000032402	a6:74:66:c3:40:46	c8:e2:65:47:89:de	48372 → 443 [ACK] Seq=79 Ack=79 Win=501 Len=0 TSval=32
137	6.460356097	youtube-ui.l.google…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TCP	74	0.006398480	c8:e2:65:47:89:de	a6:74:66:c3:40:46	443 → 44942 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
138	6.460439335	aflah-ROG-Zephyrus-…	youtube-ui.l.google.com	TCP	66	0.000083238	a6:74:66:c3:40:46	c8:e2:65:47:89:de	44942 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=48
139	6.463502855	aflah-ROG-Zephyrus-…	youtube-ui.l.google.com	TLSv1.3	726	0.003062720	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Client Hello
140	6.463930818	aflah-ROG-Zephyrus-…	youtube-ui.l.google.com	TLSv1.3	72	0.000428763	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Change Cipher Spec
141	6.463977884	aflah-ROG-Zephyrus-…	youtube-ui.l.google.com	TLSv1.3	1627	0.000047066	a6:74:66:c3:40:46	c8:e2:65:47:89:de	Application Data
142	6.474909028	maa03s26-in-f22.1e1…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TLSv1.2	105	0.010931144	c8:e2:65:47:89:de	a6:74:66:c3:40:46	Application Data
143	6.474964264	aflah-ROG-Zephyrus-…	maa03s26-in-f22.1e100.net	TCP	66	0.000055236	a6:74:66:c3:40:46	c8:e2:65:47:89:de	35916 → 443 [ACK] Seq=79 Ack=79 Win=7026 Len=0 TSval=4
144	6.520126730	youtube-ui.l.google…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TCP	66	0.045162466	c8:e2:65:47:89:de	a6:74:66:c3:40:46	443 → 44942 [ACK] Seq=1 Ack=661 Win=67072 Len=0 TSval=
145	6.520128127	youtube-ui.l.google…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TCP	66	0.000001397	c8:e2:65:47:89:de	a6:74:66:c3:40:46	443 → 44942 [ACK] Seq=1 Ack=667 Win=67072 Len=0 TSval=
146	6.545841949	youtube-ui.l.google…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TCP	66	0.025713822	c8:e2:65:47:89:de	a6:74:66:c3:40:46	443 → 44942 [ACK] Seq=1 Ack=1955 Win=69632 Len=0 TSval
147	6.550704775	youtube-ui.l.google…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TCP	66	0.004862826	c8:e2:65:47:89:de	a6:74:66:c3:40:46	443 → 44942 [ACK] Seq=1 Ack=2228 Win=72192 Len=0 TSval
148	6.595083261	youtube-ui.l.google…	aflah-ROG-Zephyrus-G14-GA401II-GA40…	TLSv1.3	834	0.044378486	c8:e2:65:47:89:de	a6:74:66:c3:40:46	Server Hello, Change Cipher Spec, Application Data, Ap
149	6.595129908	aflah-ROG-Zephyrus-…	youtube-ui.l.google.com	TCP	66	0.000046647	a6:74:66:c3:40:46	c8:e2:65:47:89:de	44942 → 443 [ACK] Seq=2228 Ack=769 Win=63488 Len=0 TSv

After this data starts to transfer!

b.) Total No. of TCP Packets - 1922

c.) Total No. of UDP Packets - 25746

Bonus:

The initial handshake with YouTube revealed the server's hardware address to be a6:74:66:c3:40:46. However, the IP address was not discernible in Wireshark.

A script was executed to analyze all packets and identify different YouTube servers. After running the script, it became evident that only the aforementioned address was utilized for communication throughout the session.

Therefore, the address of the YouTube server is confirmed to be a6:74:66:c3:40:46. da

Here are the packet counts:

- Source to Youtube TCP Packets: 1053
- Source to Youtube QUIC Packets: 5824
- Youtube to Source TCP Packets: 869
- Youtube to Source QUIC Packets: 19922