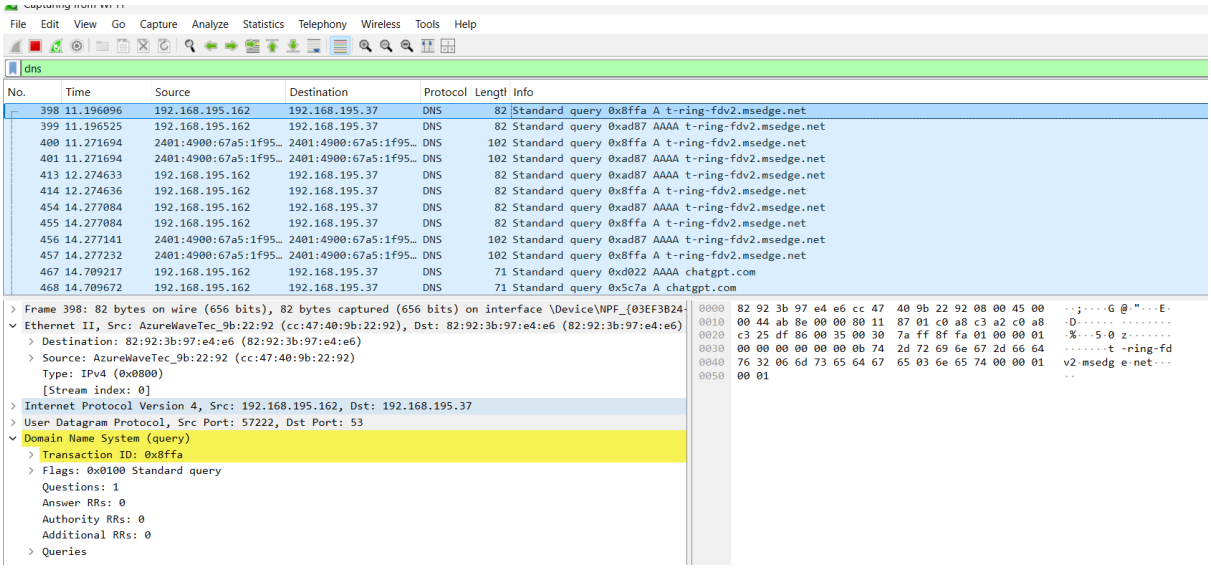
Q2. Use Wireshark to capture and analyze DNS, TCP, UDP traffic and packet head packet flow, options and flags

DNS:



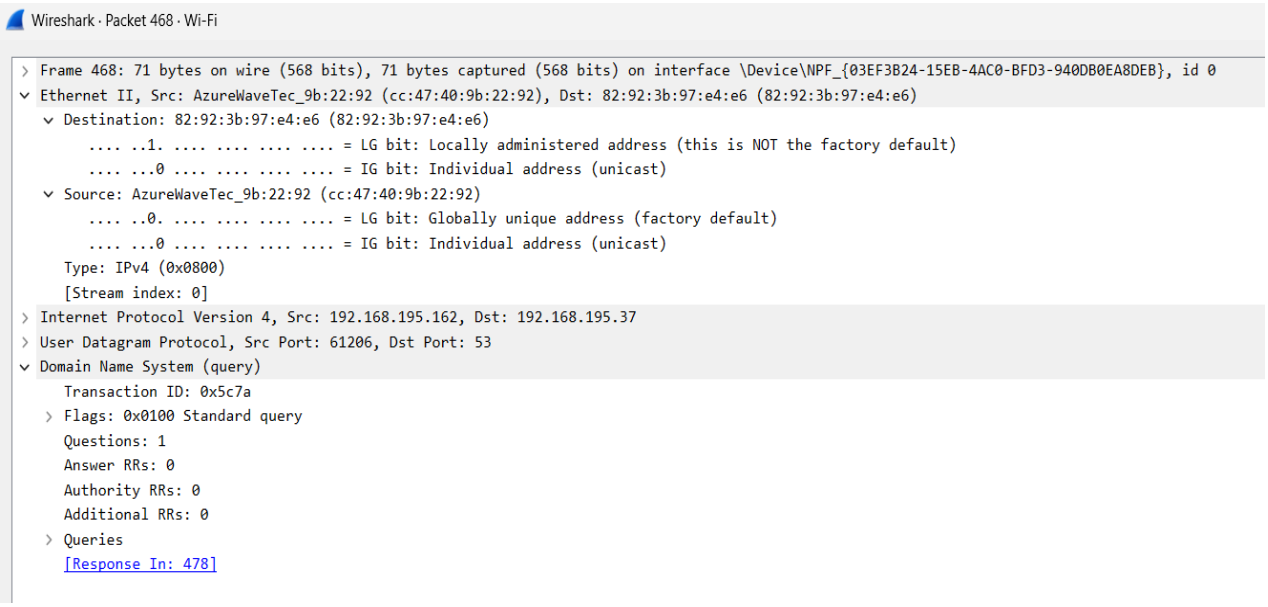
Source MAC: AzureWaveTec_9b:22:92

Destination MAC: 82:92:3b:97:e4:e6

Type: IPv4 (0x0800)

Flags: 0x0100

DNS Request:



DNS Response:

Wireshark · Packet 478 · Wi-Fi

```
> Frame 478: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{03EF3B24-15EB-4AC0-BFD3-940DB0EA8DEB}, id 0
v Ethernet II, Src: 82:92:3b:97:e4:e6 (82:92:3b:97:e4:e6), Dst: AzureWaveTec_9b:22:92 (cc:47:40:9b:22:92)
  v Destination: AzureWaveTec_9b:22:92 (cc:47:40:9b:22:92)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: 82:92:3b:97:e4:e6 (82:92:3b:97:e4:e6)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.195.37, Dst: 192.168.195.162
> User Datagram Protocol, Src Port: 53, Dst Port: 61206
v Domain Name System (response)
    Transaction ID: 0x5c7a
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 468]
    [Time: 0.011302000 seconds]
```

TCP:

SYN (Client → Server, Request to start connection).

SYN-ACK (Server → Client, Acknowledges connection).

ACK (Client → Server, Final handshake confirmation).

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

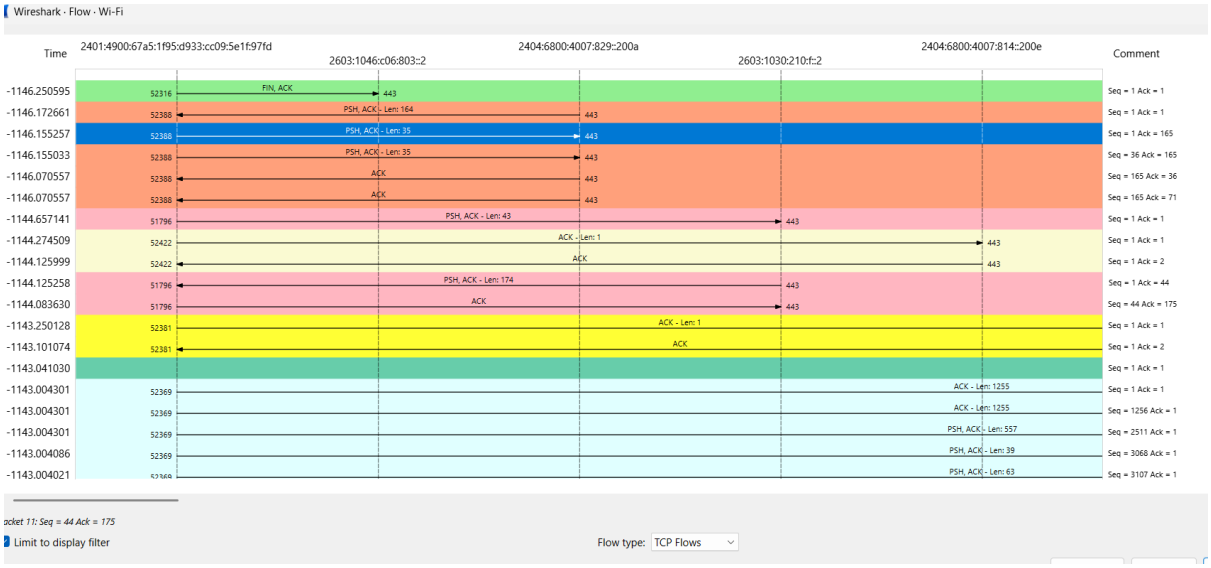
tcp

No.	Time	Source	Destination	Protocol	Length	Info
29	3.563086	2404:6800:4007:809:…	2401:4900:67a5:1f95…	TLSv1.2	403	Application Data
30	3.563256	2401:4900:67a5:1f95…	2404:6800:4007:809:…	TCP	74	52369 → 443 [ACK] Seq=3170 Ack=1341 Win=255 Len=0
31	3.563371	2404:6800:4007:809:…	2401:4900:67a5:1f95…	TLSv1.2	113	Application Data
32	3.564124	2401:4900:67a5:1f95…	2404:6800:4007:809:…	TLSv1.2	109	Application Data
33	3.564216	2401:4900:67a5:1f95…	2404:6800:4007:809:…	TLSv1.2	113	Application Data
34	3.662132	2404:6800:4007:809:…	2401:4900:67a5:1f95…	TCP	74	443 → 52369 [ACK] Seq=1380 Ack=3205 Win=560 Len=0
35	3.662132	2404:6800:4007:809:…	2401:4900:67a5:1f95…	TCP	74	443 → 52369 [ACK] Seq=1380 Ack=3244 Win=560 Len=0
36	7.607814	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TCP	86	52440 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
37	7.756592	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TCP	86	443 → 52440 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1255 SACK_PERM WS=256
38	7.756771	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TCP	74	52440 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
39	7.757406	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TCP	1329	52440 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1255 [TCP PDU reassembled in 40]
40	7.757406	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TLSv1.3	543	Client Hello (SNI=www.google.com)
41	7.858959	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TCP	74	443 → 52440 [ACK] Seq=1 Ack=1256 Win=268032 Len=0
42	7.859047	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TCP	74	443 → 52440 [ACK] Seq=1 Ack=1725 Win=267776 Len=0
43	7.860321	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TLSv1.3	1294	Server Hello
44	7.860321	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TLSv1.3	1294	Change Cipher Spec
45	7.860321	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TCP	1294	443 → 52440 [ACK] Seq=2441 Ack=1725 Win=267776 Len=1220 [TCP PDU reassembled in 46]
46	7.860321	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TLSv1.3	491	Application Data
47	7.860486	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TCP	74	52440 → 443 [ACK] Seq=1725 Ack=4078 Win=65280 Len=0
48	7.861715	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TLSv1.3	148	Change Cipher Spec, Application Data
49	7.862077	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TLSv1.3	166	Application Data
50	7.862535	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TCP	1329	52440 → 443 [ACK] Seq=1891 Ack=4078 Win=65280 Len=1255 [TCP PDU reassembled in 51]
51	7.862535	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TLSv1.3	958	Application Data
52	7.862713	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TLSv1.3	158	Application Data
53	7.862822	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TLSv1.3	167	Application Data
54	7.872376	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TLSv1.3	165	Application Data
55	7.881423	2401:4900:67a5:1f95…	2600:1417:20::17cd:…	TCP	74	52317 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	7.889656	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TCP	74	443 → 52440 [ACK] Seq=4078 Ack=1891 Win=267776 Len=0
57	7.889656	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TLSv1.3	1090	Application Data, Application Data
58	7.889656	2404:6800:4007:82b:…	2401:4900:67a5:1f95…	TLSv1.3	105	Application Data
59	7.889856	2401:4900:67a5:1f95…	2404:6800:4007:82b:…	TCP	74	52440 → 443 [ACK] Seq=4298 Ack=5125 Win=64256 Len=0

```
> Frame 36: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{03EF3B24-1
> Ethernet II, Src: AzureWaveTec_9b:22:92 (cc:47:40:9b:22:92), Dst: 82:92:3b:97:e4:e6 (82:92:3b:97:e4:e6)
> Internet Protocol Version 6, Src: 2401:4900:67a5:1f95:d933:cc09:5e1f:97fd, Dst: 2404:6800:4007:82b::2004

0000  82 92 3b 97 e4 e6 cc 47  40 9b 22 92 86 dd 60 05   ··;····G @·"···`·
0010  15 8b 00 20 06 3f 24 01  49 00 67 a5 1f 95 d9 33   ··· ·?$· I·g····3
0020  cc 09 5e 1f 97 fd 24 04  68 00 40 07 08 2b 00 00   ··^···$· h·@··+··
0030  00 00 00 00 20 04 cc d8  01 bb 67 8d 27 fe 00 00   ···· ··· ··g·'···
```

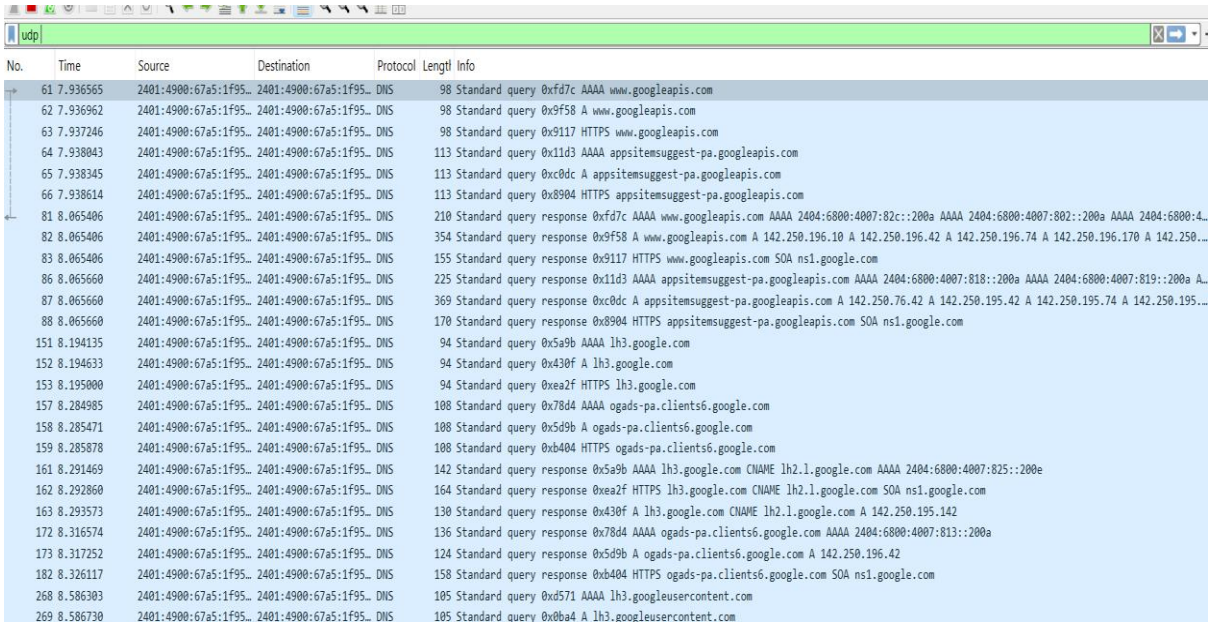
TCP Flow:



The graph shows multiple ongoing TCP conversations between different endpoints.

Some connections are actively transferring data, while others are just sending ACKs.

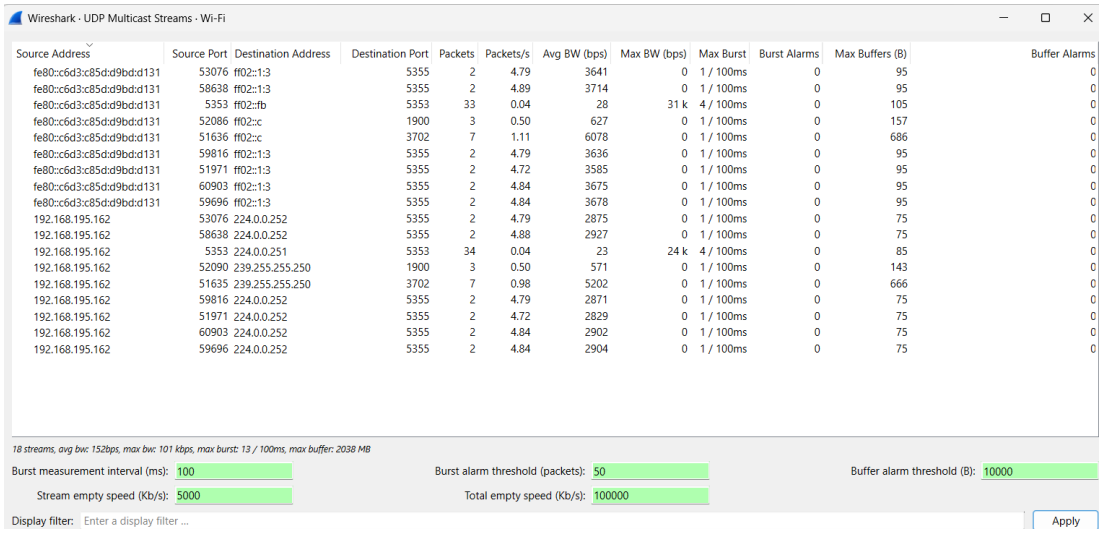
UDP:



udp

No.	Time	Source	Destination	Protocol	Length	Info
61	7.936565	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	98	Standard query 0xfd7c AAAA www.googleapis.com
62	7.936962	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	98	Standard query 0x9f58 A www.googleapis.com
63	7.937246	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	98	Standard query 0x9117 HTTPS www.googleapis.com
64	7.938043	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	113	Standard query 0x11d3 AAAA appsitemsuggest-pa.googleapis.com
65	7.938345	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	113	Standard query 0xc0dc A appsitemsuggest-pa.googleapis.com
66	7.938614	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	113	Standard query 0x8904 HTTPS appsitemsuggest-pa.googleapis.com
81	8.065406	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	210	Standard query response 0xfd7c AAAA www.googleapis.com AAAA 2404:6800:4007:82c::200a AAAA 2404:6800:4007:802::200a AAAA 2404:6800:4…
82	8.065406	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	354	Standard query response 0x9f58 A www.googleapis.com A 142.250.196.10 A 142.250.196.42 A 142.250.196.74 A 142.250.196.170 A 142.250.…
83	8.065406	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	155	Standard query response 0x9117 HTTPS www.googleapis.com SOA ns1.google.com
86	8.065660	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	225	Standard query response 0x11d3 AAAA appsitemsuggest-pa.googleapis.com AAAA 2404:6800:4007:818::200a AAAA 2404:6800:4007:819::200a A…
87	8.065660	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	369	Standard query response 0xc0dc A appsitemsuggest-pa.googleapis.com A 142.250.76.42 A 142.250.195.42 A 142.250.195.74 A 142.250.195.…
88	8.065660	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	170	Standard query response 0x8904 HTTPS appsitemsuggest-pa.googleapis.com SOA ns1.google.com
151	8.194135	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	94	Standard query 0x5a9b AAAA lh3.google.com
152	8.194633	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	94	Standard query 0x430f A lh3.google.com
153	8.195000	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	94	Standard query 0xea2f HTTPS lh3.google.com
157	8.284985	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	108	Standard query 0x78d4 AAAA ogads-pa.clients6.google.com
158	8.285471	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	108	Standard query 0x5d9b A ogads-pa.clients6.google.com
159	8.285878	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	108	Standard query 0xb404 HTTPS ogads-pa.clients6.google.com
161	8.291469	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	142	Standard query response 0x5a9b AAAA lh3.google.com CNAME lh2.l.google.com AAAA 2404:6800:4007:825::200e
162	8.292860	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	164	Standard query response 0xea2f HTTPS lh3.google.com CNAME lh2.l.google.com SOA ns1.google.com
163	8.293573	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	130	Standard query response 0x430f A lh3.google.com CNAME lh2.l.google.com A 142.250.195.142
172	8.316574	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	136	Standard query response 0x78d4 AAAA ogads-pa.clients6.google.com AAAA 2404:6800:4007:813::200a
173	8.317252	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	124	Standard query response 0x5d9b A ogads-pa.clients6.google.com A 142.250.196.42
182	8.326117	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	158	Standard query response 0xb404 HTTPS ogads-pa.clients6.google.com SOA ns1.google.com
268	8.586303	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	105	Standard query 0xd571 AAAA lh3.googleusercontent.com
269	8.586730	2401:4900:67a5:1f95…	2401:4900:67a5:1f95…	DNS	105	Standard query 0x0ba4 A lh3.googleusercontent.com

Shows details of UDP multicast streams like source,destination addresses, ports, packet rates, and bandwidth usage.



Wireshark · UDP Multicast Streams · Wi-Fi

Source Address	Source Port	Destination Address	Destination Port	Packets	Packets/s	Avg BW (bps)	Max BW (bps)	Max Burst	Burst Alarms	Max Buffers (B)	Buffer Alarms
fe80::c6d3:c85d:d9bd:d131	53076	ff02::1:3	5355	2	4.79	3641	0	1 / 100ms	0	95	0
fe80::c6d3:c85d:d9bd:d131	58638	ff02::1:3	5355	2	4.89	3714	0	1 / 100ms	0	95	0
fe80::c6d3:c85d:d9bd:d131	5353	ff02::fb	5353	33	0.04	28	31 k	4 / 100ms	0	105	0
fe80::c6d3:c85d:d9bd:d131	52086	ff02::c	1900	3	0.50	627	0	1 / 100ms	0	157	0
fe80::c6d3:c85d:d9bd:d131	51636	ff02::c	3702	7	1.11	6078	0	1 / 100ms	0	686	0
fe80::c6d3:c85d:d9bd:d131	59816	ff02::1:3	5355	2	4.79	3636	0	1 / 100ms	0	95	0
fe80::c6d3:c85d:d9bd:d131	51971	ff02::1:3	5355	2	4.72	3585	0	1 / 100ms	0	95	0
fe80::c6d3:c85d:d9bd:d131	60903	ff02::1:3	5355	2	4.84	3675	0	1 / 100ms	0	95	0
fe80::c6d3:c85d:d9bd:d131	59696	ff02::1:3	5355	2	4.84	3678	0	1 / 100ms	0	95	0
192.168.195.162	53076	224.0.0.252	5355	2	4.79	2875	0	1 / 100ms	0	75	0
192.168.195.162	58638	224.0.0.252	5355	2	4.88	2927	0	1 / 100ms	0	75	0
192.168.195.162	5353	224.0.0.251	5353	34	0.04	23	24 k	4 / 100ms	0	85	0
192.168.195.162	52090	239.255.255.250	1900	3	0.50	571	0	1 / 100ms	0	143	0
192.168.195.162	51635	239.255.255.250	3702	7	0.98	5202	0	1 / 100ms	0	666	0
192.168.195.162	59816	224.0.0.252	5355	2	4.79	2871	0	1 / 100ms	0	75	0
192.168.195.162	51971	224.0.0.252	5355	2	4.72	2829	0	1 / 100ms	0	75	0
192.168.195.162	60903	224.0.0.252	5355	2	4.84	2902	0	1 / 100ms	0	75	0
192.168.195.162	59696	224.0.0.252	5355	2	4.84	2904	0	1 / 100ms	0	75	0

18 streams, avg bw: 152bps, max bw: 101 kbps, max burst: 13 / 100ms, max buffer: 2038 MB

Burst measurement interval (ms): 100
Burst alarm threshold (packets): 50
Buffer alarm threshold (B): 10000
Stream empty speed (Kb/s): 5000
Total empty speed (Kb/s): 100000

Display filter: Enter a display filter ...
Apply