Name: Abdurrahman Qureshi

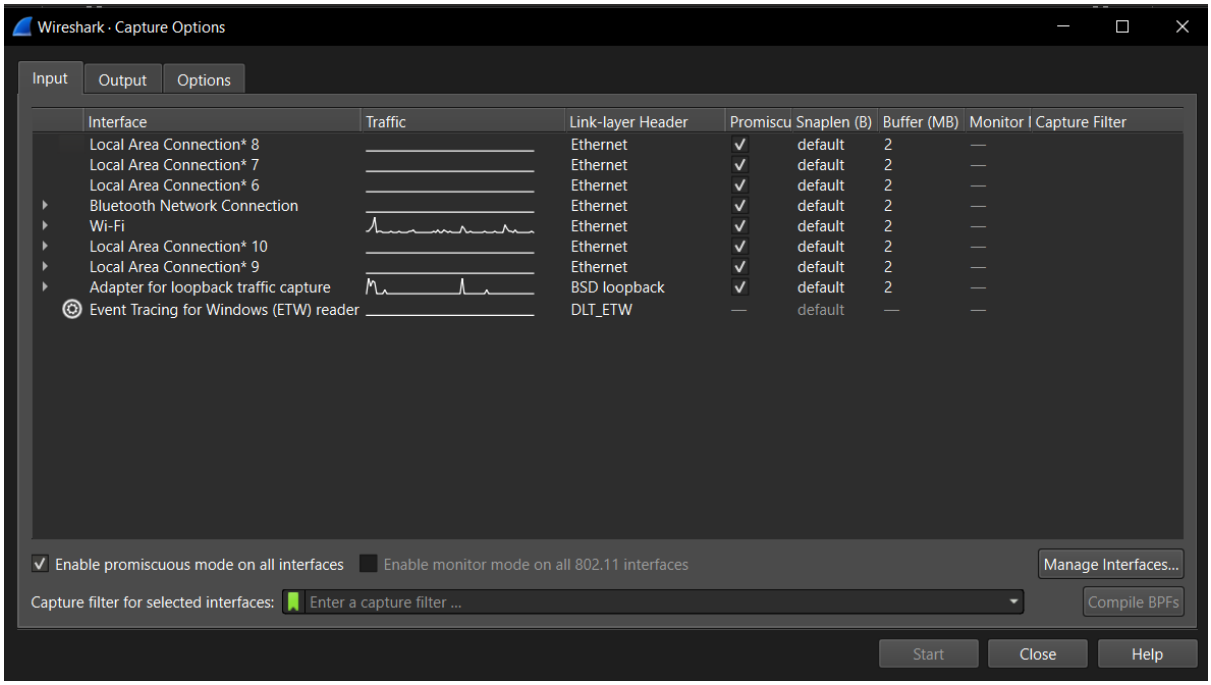
Roll No: 242466

Practical No: 3

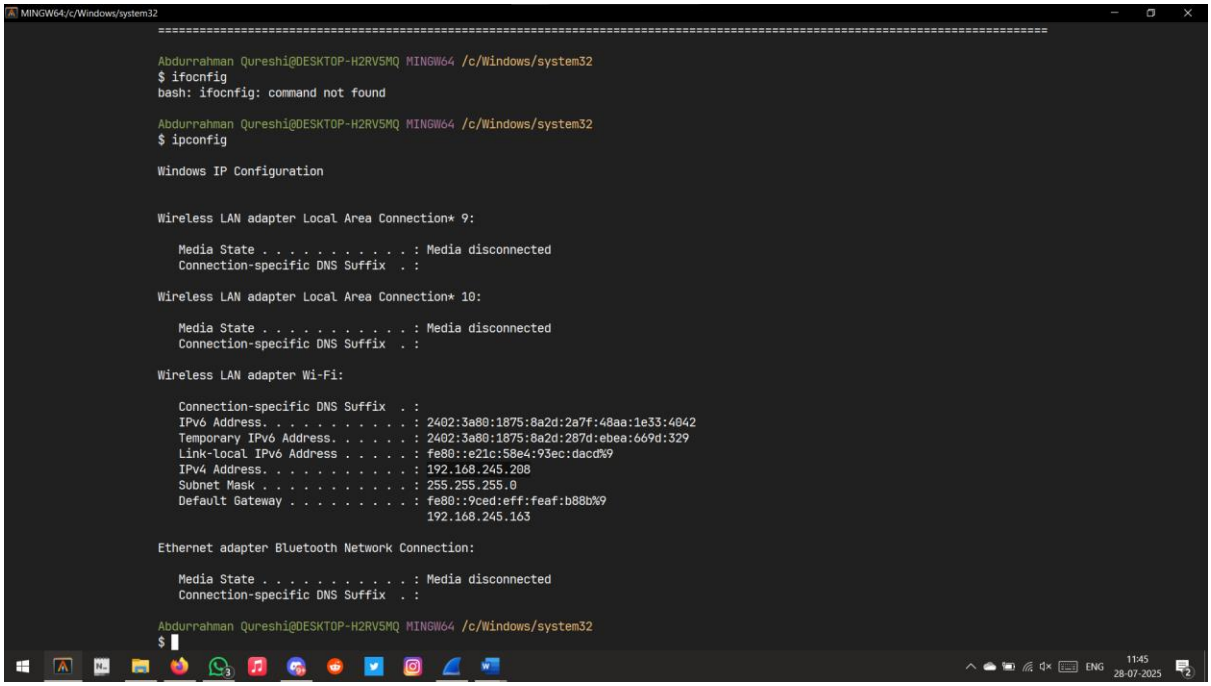
Date Of Performance: 28/07/2025

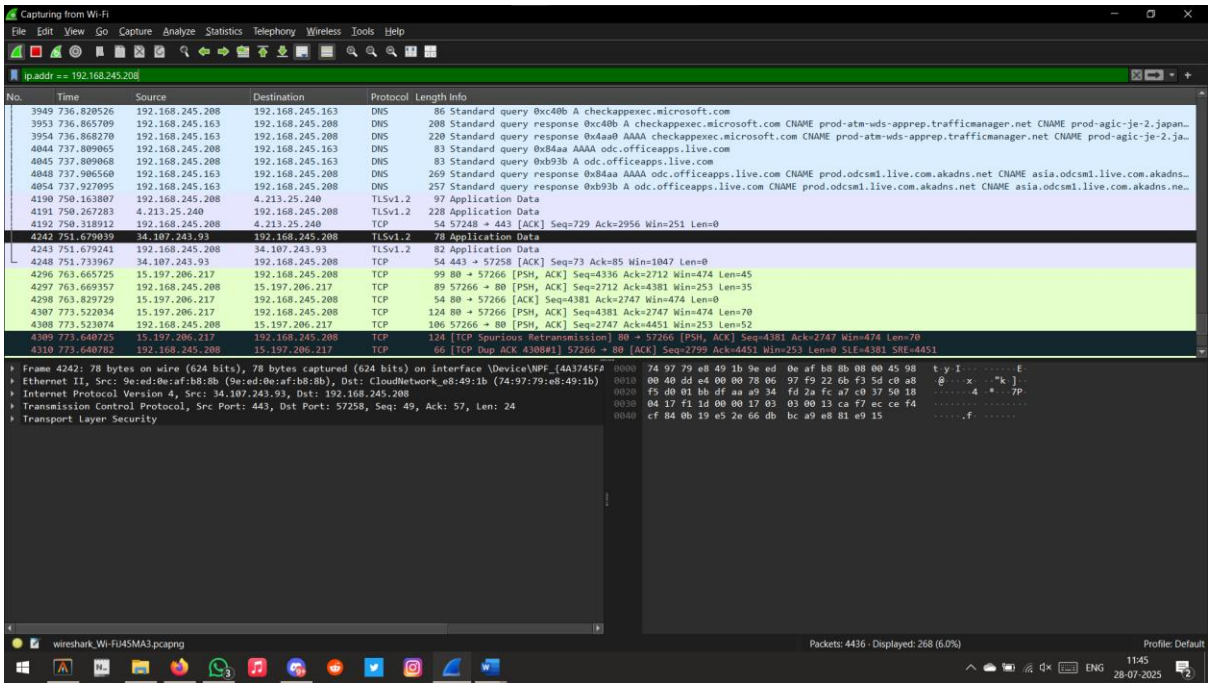
Aim: Study of packet sniffer tool WireShark via different network filters

Promiscuos Mode:

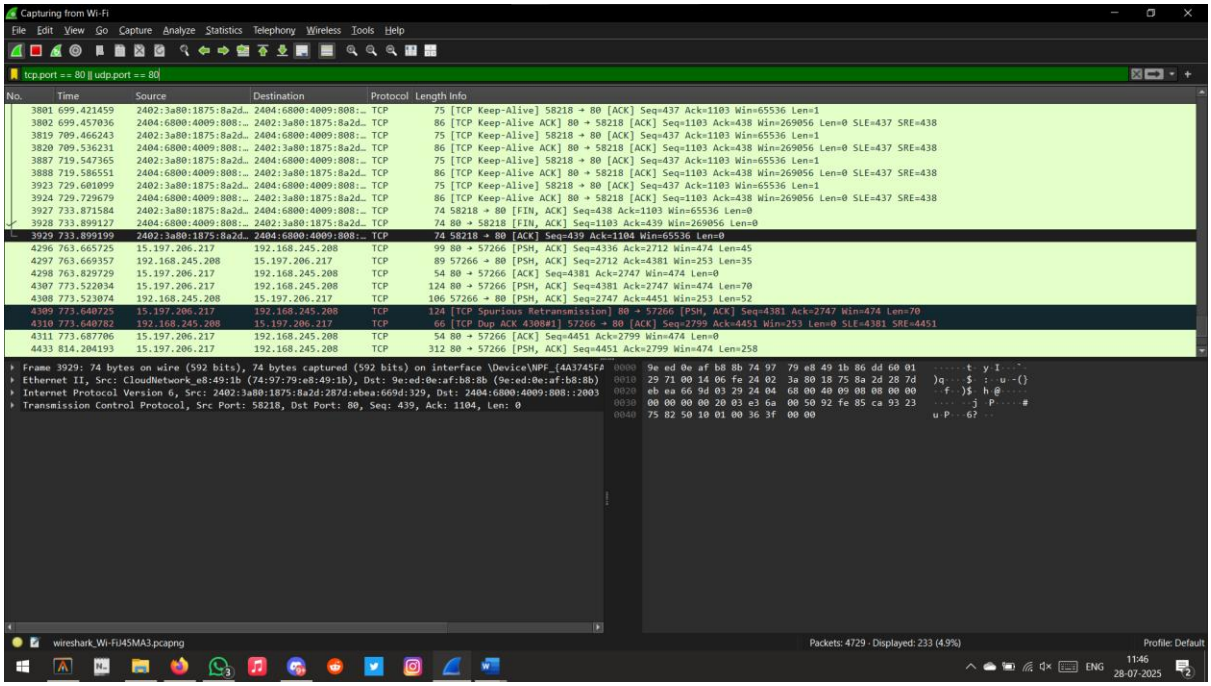


1) ip and ip.addr == ?

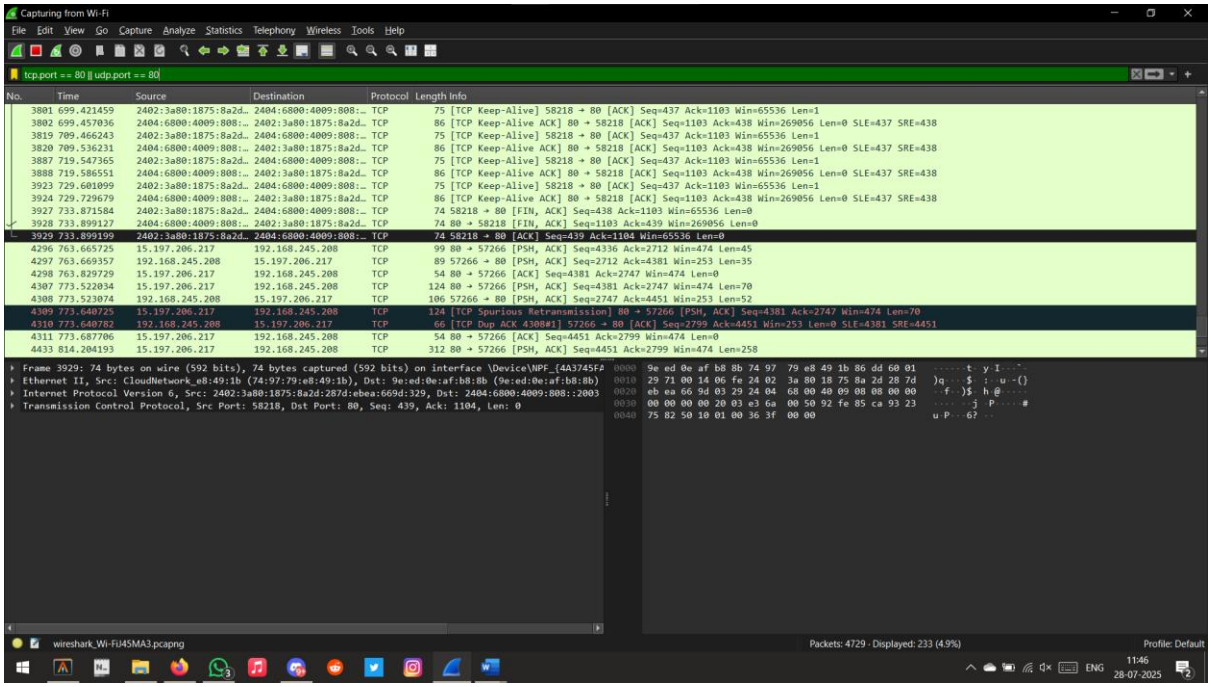




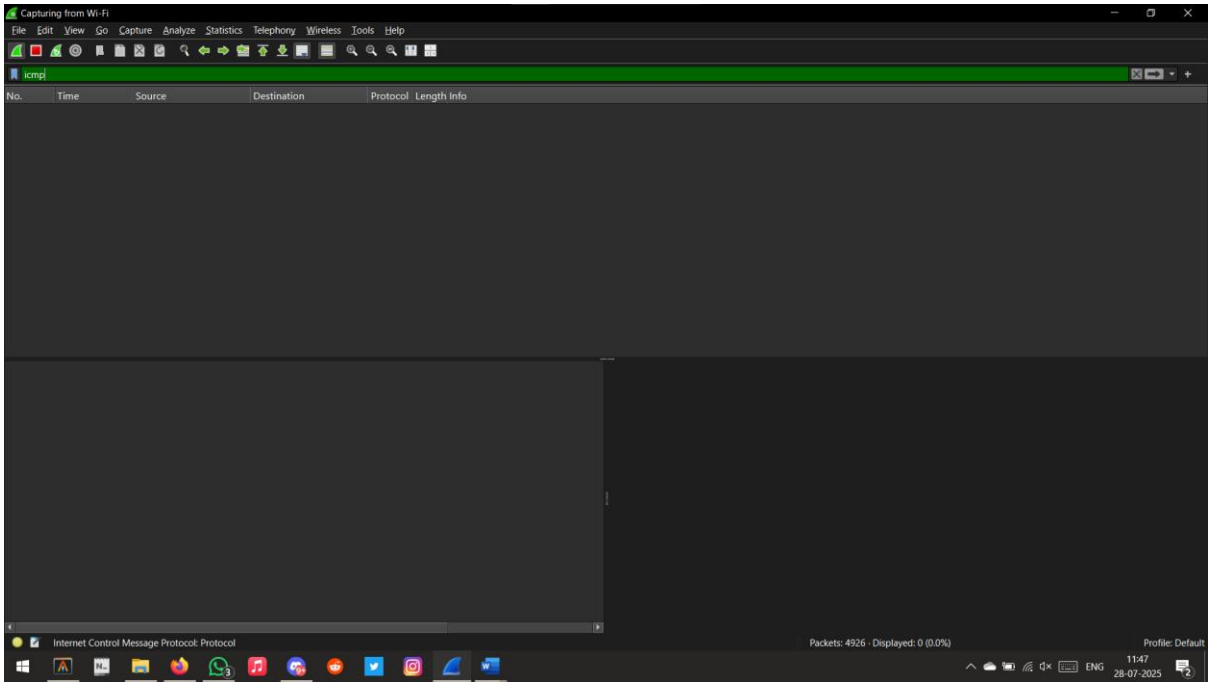
2) tcp.port == 80



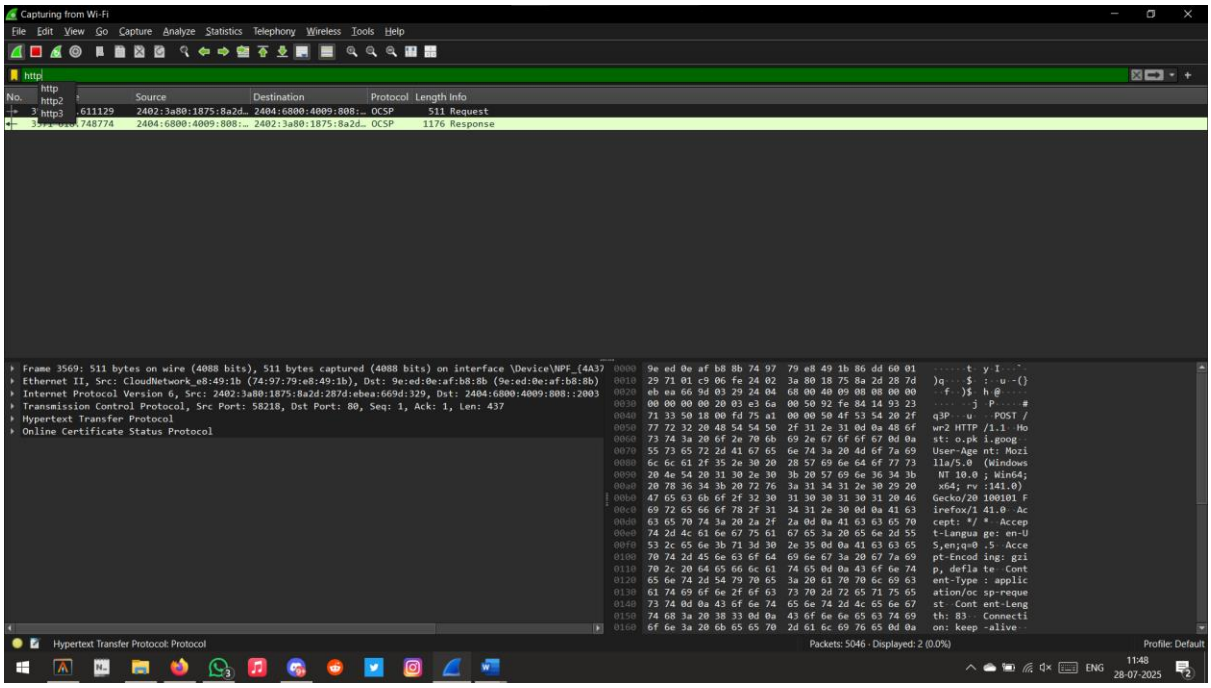
3) udp.port == 80



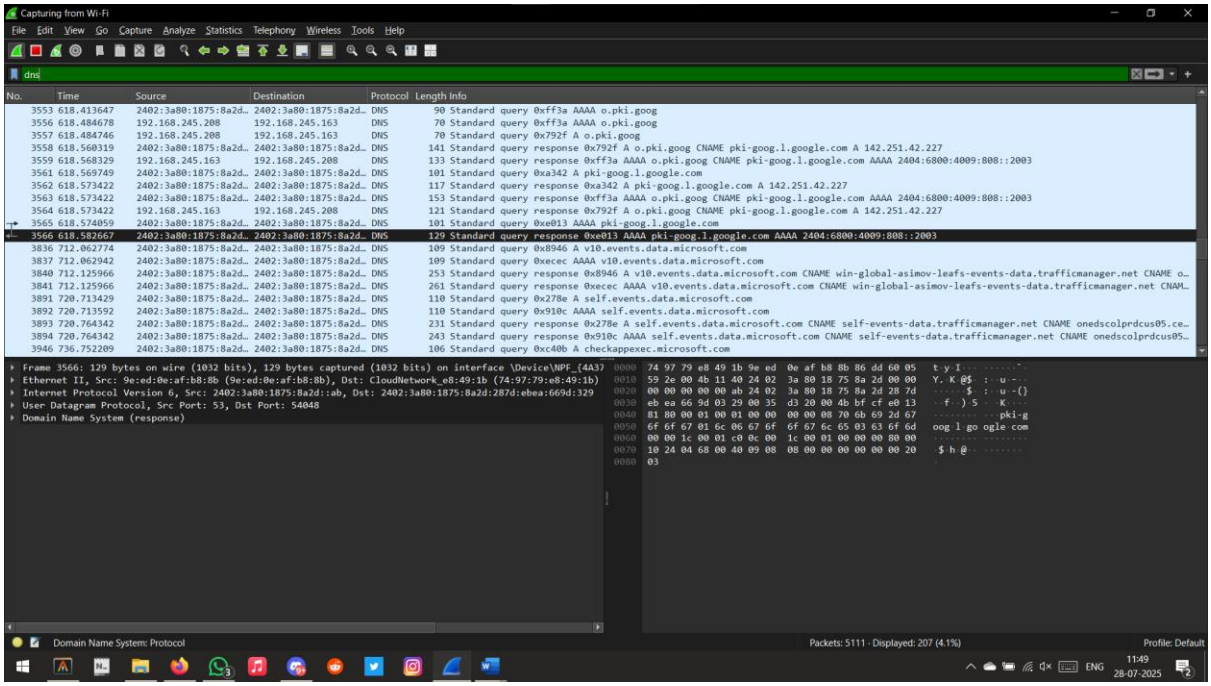
4) icmp


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
Internet Control Message Protocol: Protocol
Packets: 4926 · Displayed: 0 (0.0%)
Profile: Default
ENG
11:47
28-07-2025

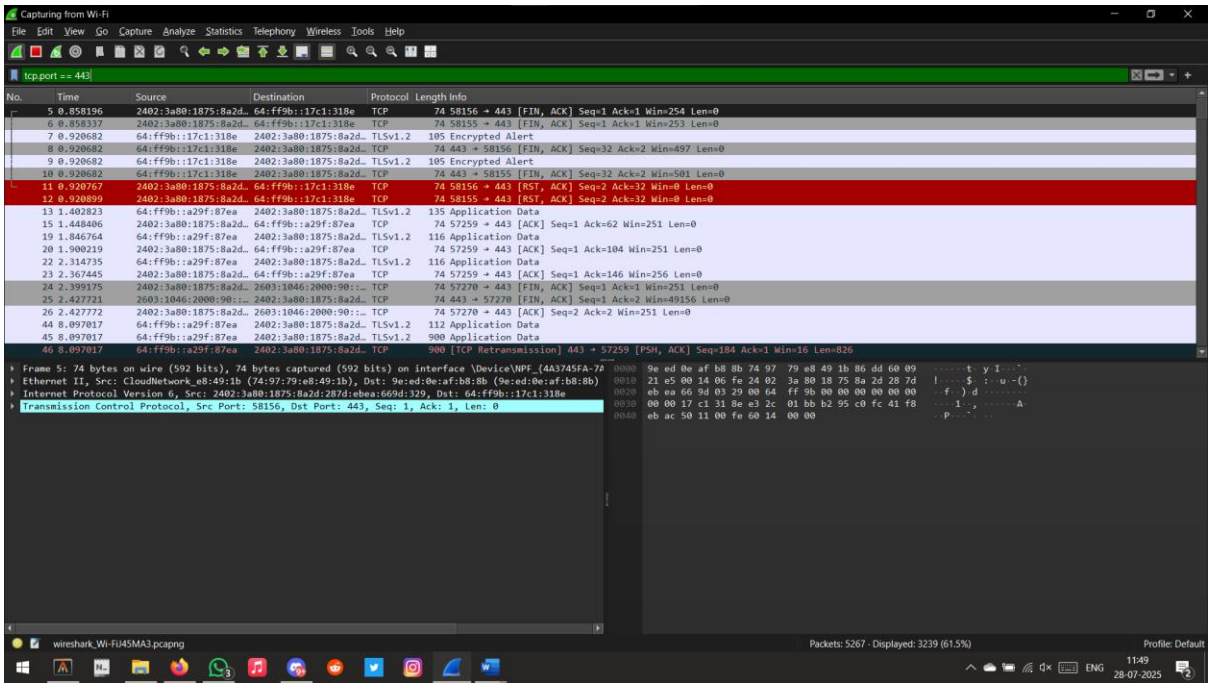
5) https


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3
No. Source Destination Protocol Length Info
3 2402:3a80:1875:8a2d… 2404:6800:4009:808:… OCSP 511 Request
3591 2404:6800:4009:808:… 2402:3a80:1875:8a2d… OCSP 1176 Response
Frame 3569: 511 bytes on wire (4088 bits), 511 bytes captured (4088 bits) on interface \Device\NPF_{4A37
Ethernet II, Src: CloudNetwork_e8:49:1b (74:97:79:e8:49:1b), Dst: 9e:ed:0e:af:b8:8b (9e:ed:0e:af:b8:8b)
Internet Protocol Version 6, Src: 2402:3a80:1875:8a2d:287d:ebea:669d:329, Dst: 2404:6800:4009:808::2003
Transmission Control Protocol, Src Port: 58218, Dst Port: 80, Seq: 1, Ack: 1, Len: 437
Hypertext Transfer Protocol
Online Certificate Status Protocol
Hypertext Transfer Protocol: Protocol
Packets: 5046 · Displayed: 2 (0.0%)
Profile: Default
ENG
11:48
28-07-2025

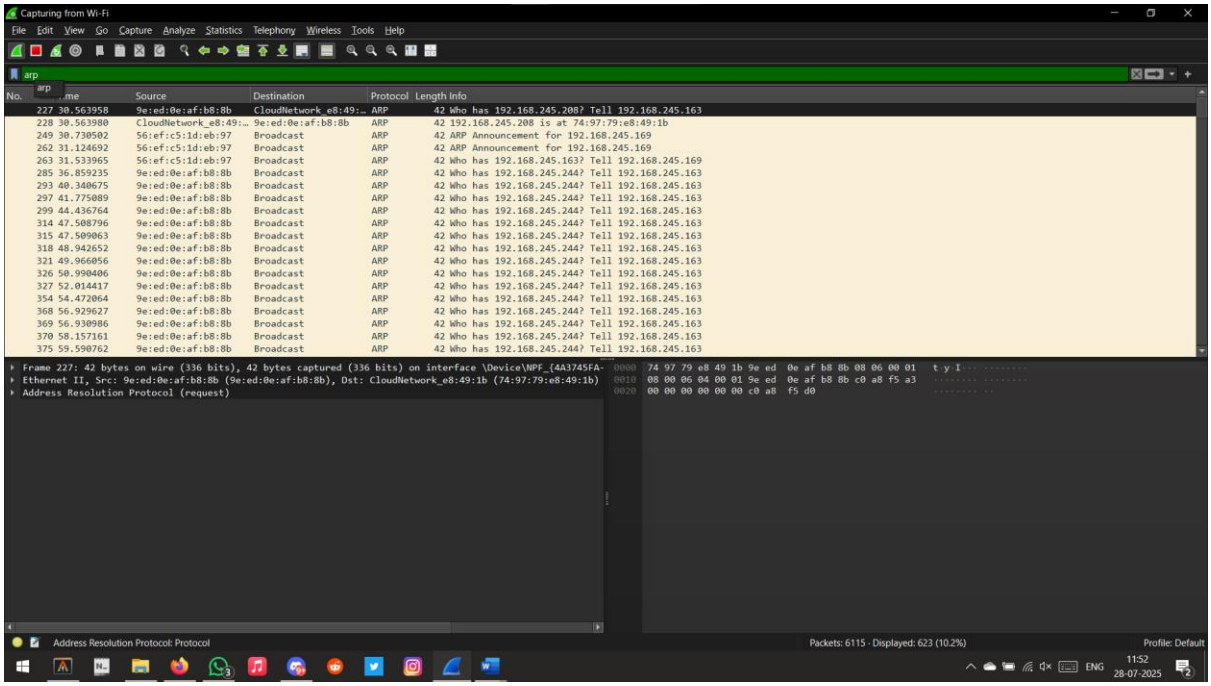
6) dns



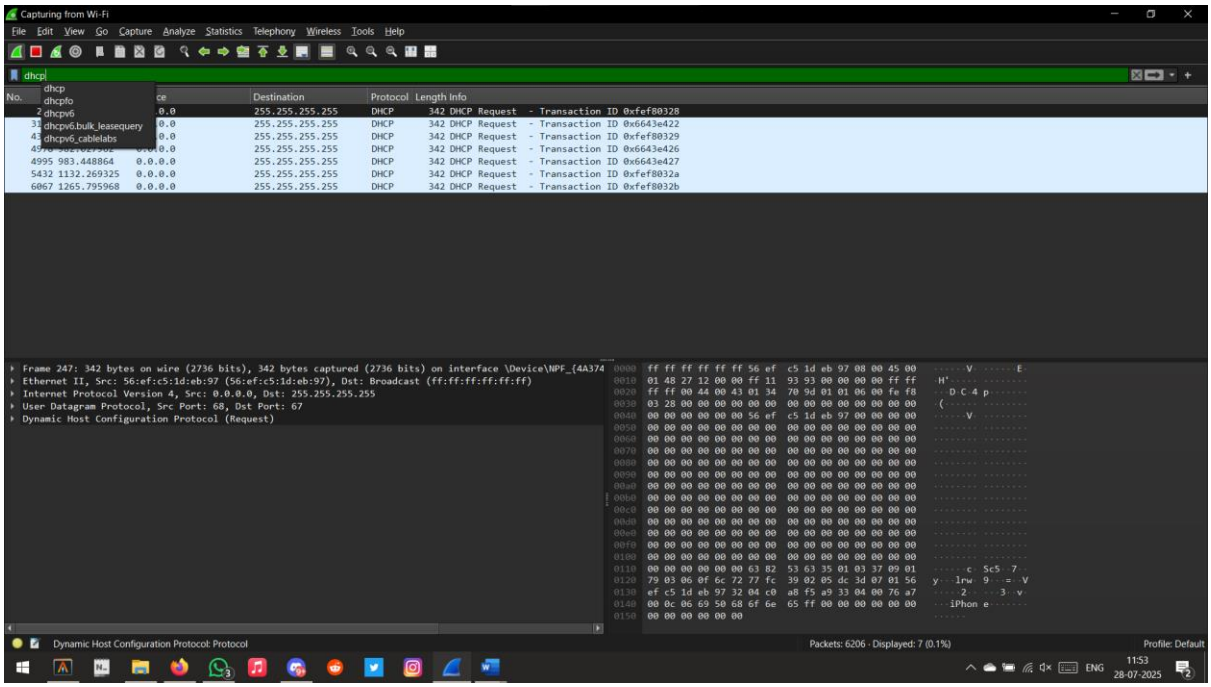
7) tcp.port == 443



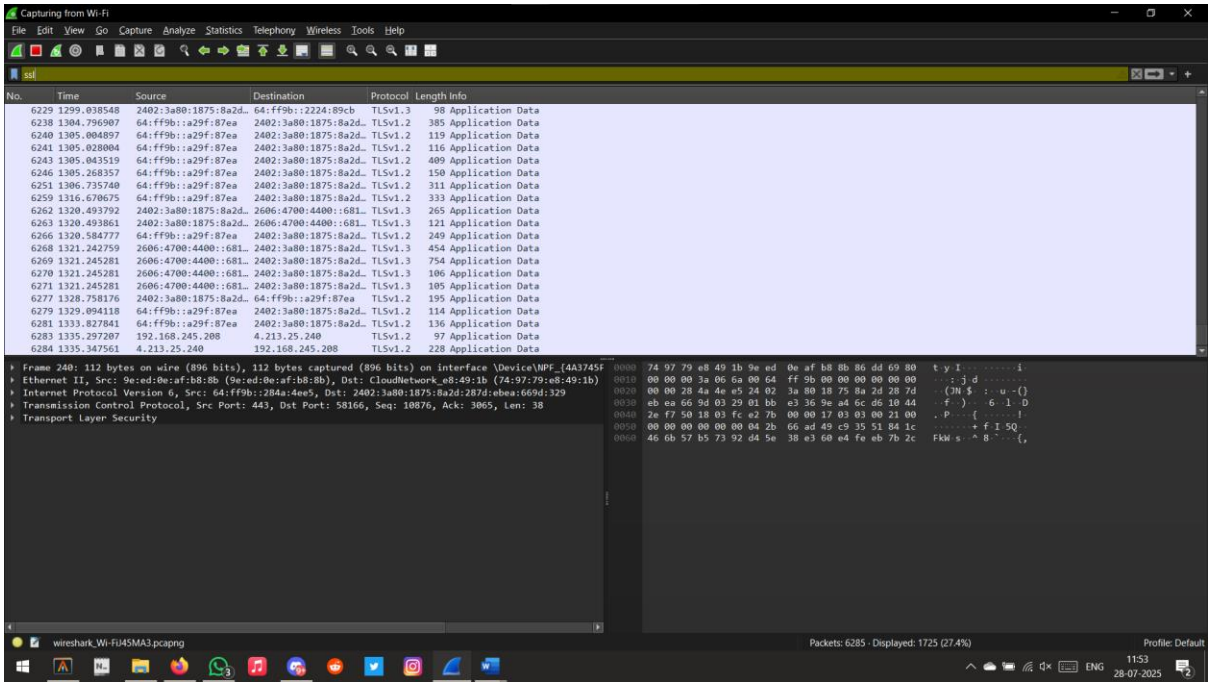
8) arp


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
227 30.563958 9e:ed:0e:af:b8:8b CloudNetwork_e8:49:... ARP 42 Who has 192.168.245.208? Tell 192.168.245.163
228 30.563980 CloudNetwork_e8:49:... 9e:ed:0e:af:b8:8b ARP 42 192.168.245.208 is at 74:97:79:e8:49:1b
249 30.730502 56:ef:c5:1d:eb:97 Broadcast ARP 42 ARP Announcement for 192.168.245.169
262 31.124692 56:ef:c5:1d:eb:97 Broadcast ARP 42 ARP Announcement for 192.168.245.169
263 31.533965 56:ef:c5:1d:eb:97 Broadcast ARP 42 Who has 192.168.245.163? Tell 192.168.245.169
285 36.859235 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
293 40.340675 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
297 41.775089 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
299 44.436764 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
314 47.508796 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
315 47.509063 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
318 48.942652 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
321 49.966056 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
326 50.990406 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
327 52.014417 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
354 54.472064 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
368 56.929627 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
369 56.930986 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
370 58.157161 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
375 59.590762 9e:ed:0e:af:b8:8b Broadcast ARP 42 Who has 192.168.245.244? Tell 192.168.245.163
Frame 227: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{4A3745FA-
Ethernet II, Src: 9e:ed:0e:af:b8:8b (9e:ed:0e:af:b8:8b), Dst: CloudNetwork_e8:49:1b (74:97:79:e8:49:1b)
Address Resolution Protocol (request)
0000 74 97 79 e8 49 1b 9e ed 0e af b8 8b 08 06 00 01 t y I
0010 08 00 06 04 00 01 9e ed 0e af b8 8b c0 a8 f5 a3
0020 00 00 00 00 00 00 c0 a8 f5 d0
Address Resolution Protocol: Protocol
Packets: 6115 · Displayed: 623 (10.2%)
Profile: Default
ENG 11:52 28-07-2025

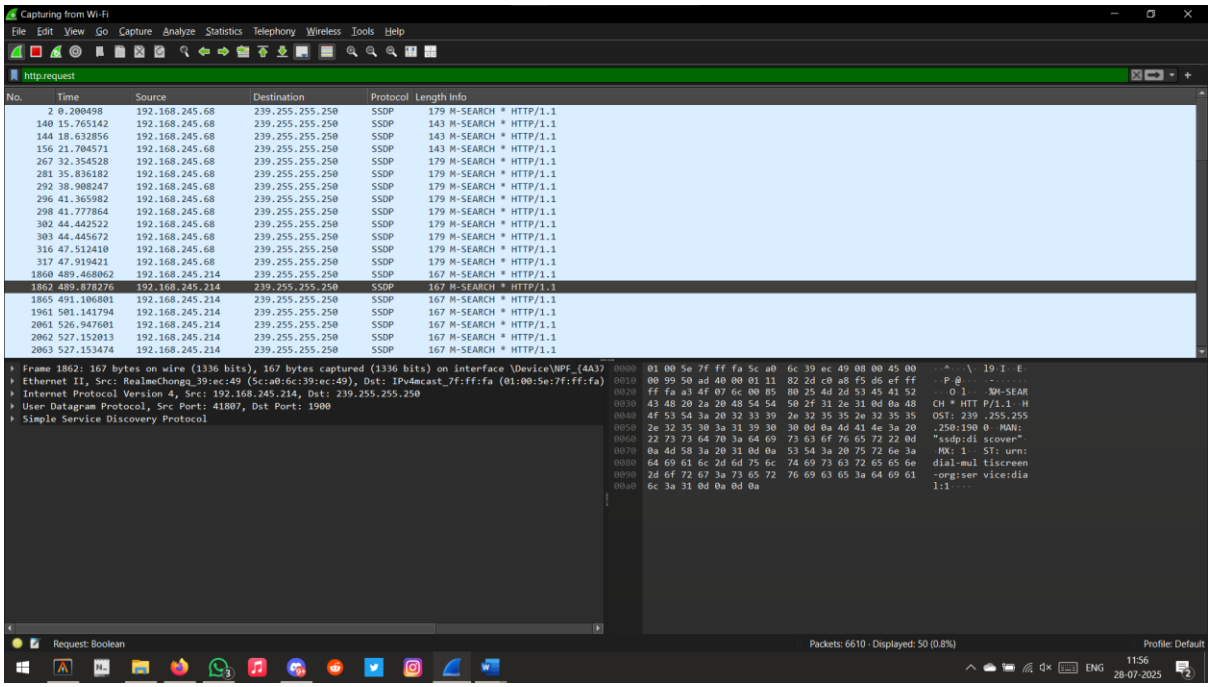
9) dhcp


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
dhcpfo
dhcpv6
dhcpv6.bulk_leasequery
dhcpv6_cablelabs
No. Time Source Destination Protocol Length Info
2 0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0xfef80328
3 0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x6643e422
4 0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0xfef80329
4 0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x6643e426
4995 983.448864 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x6643e427
5432 1132.269325 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0xfef8032a
6067 1265.795968 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0xfef8032b
Frame 247: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{4A374
Ethernet II, Src: 56:ef:c5:1d:eb:97 (56:ef:c5:1d:eb:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
Dynamic Host Configuration Protocol: Protocol
Packets: 6206 · Displayed: 7 (0.1%)
Profile: Default
ENG 11:53 28-07-2025

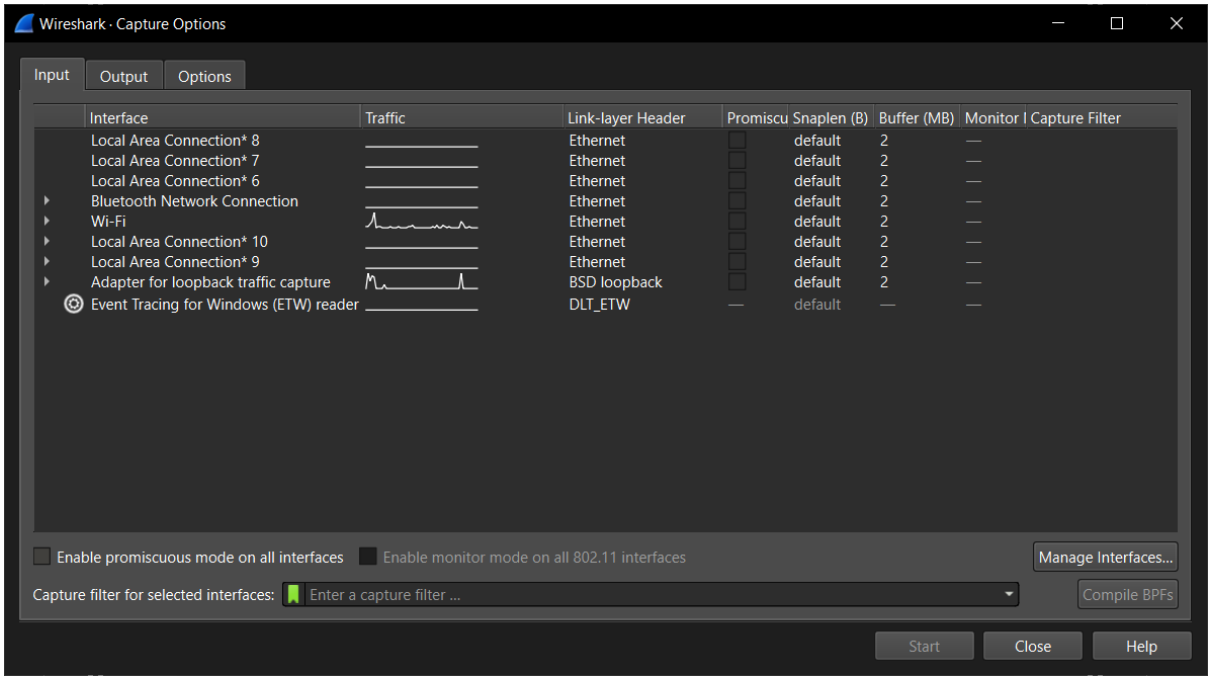
10) ssl

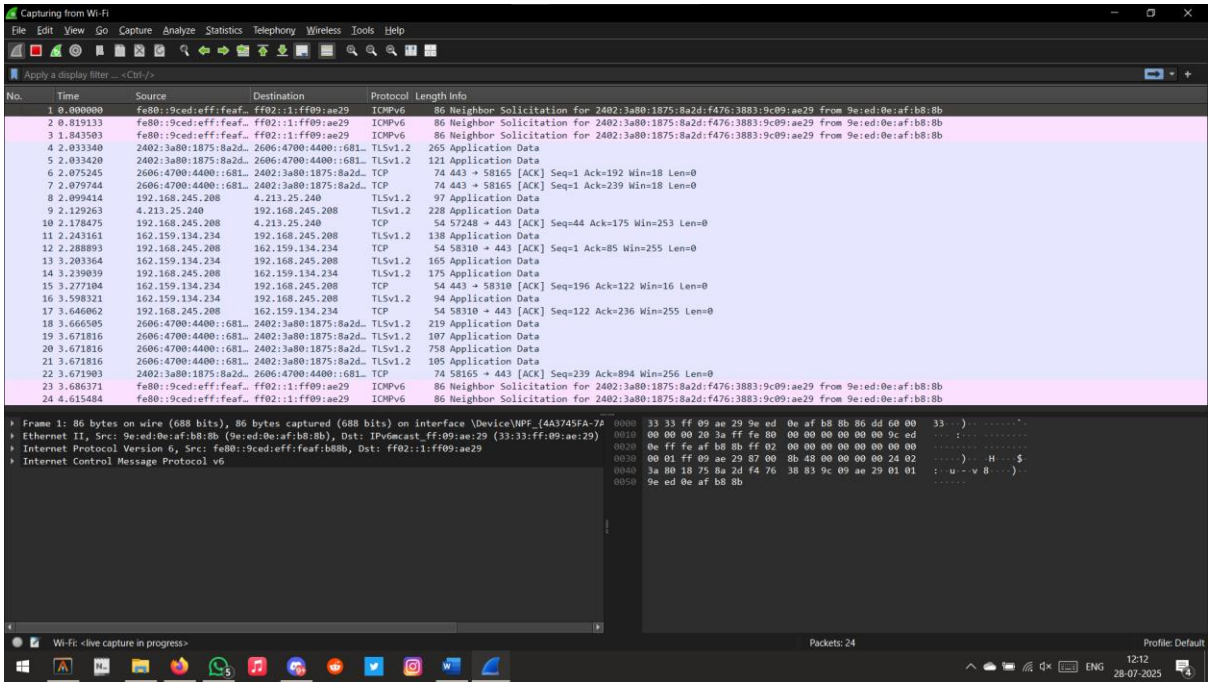


11) http.request

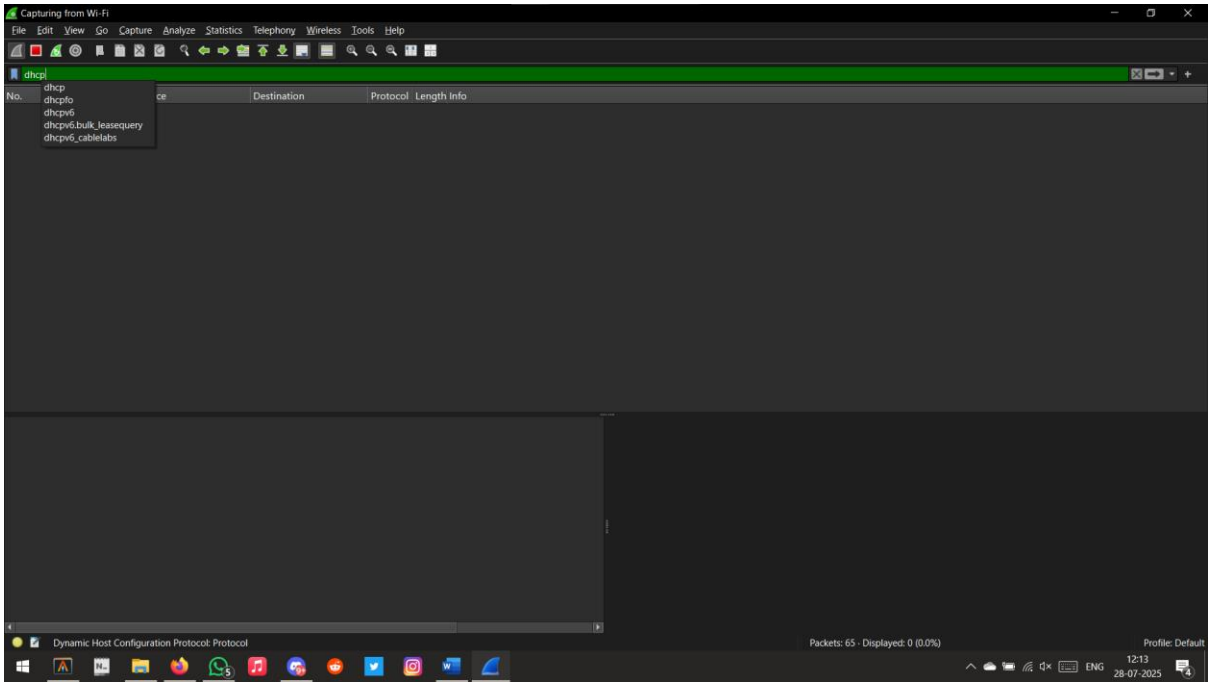


Non-Promiscuos Mode:

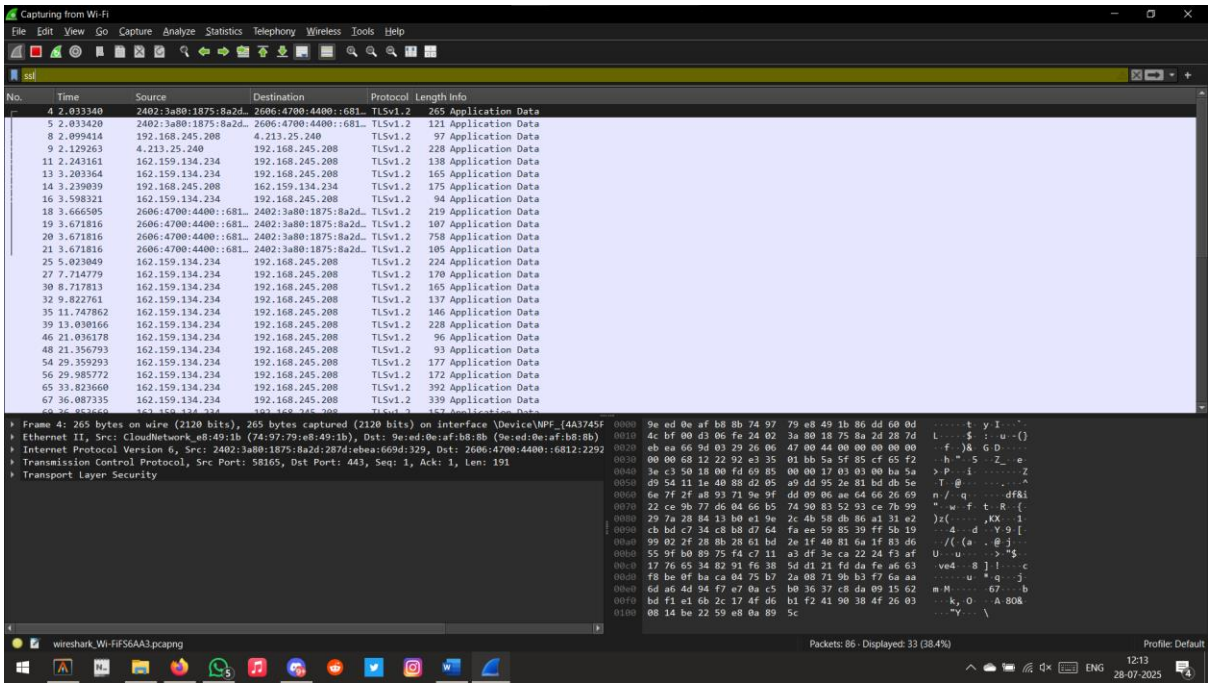




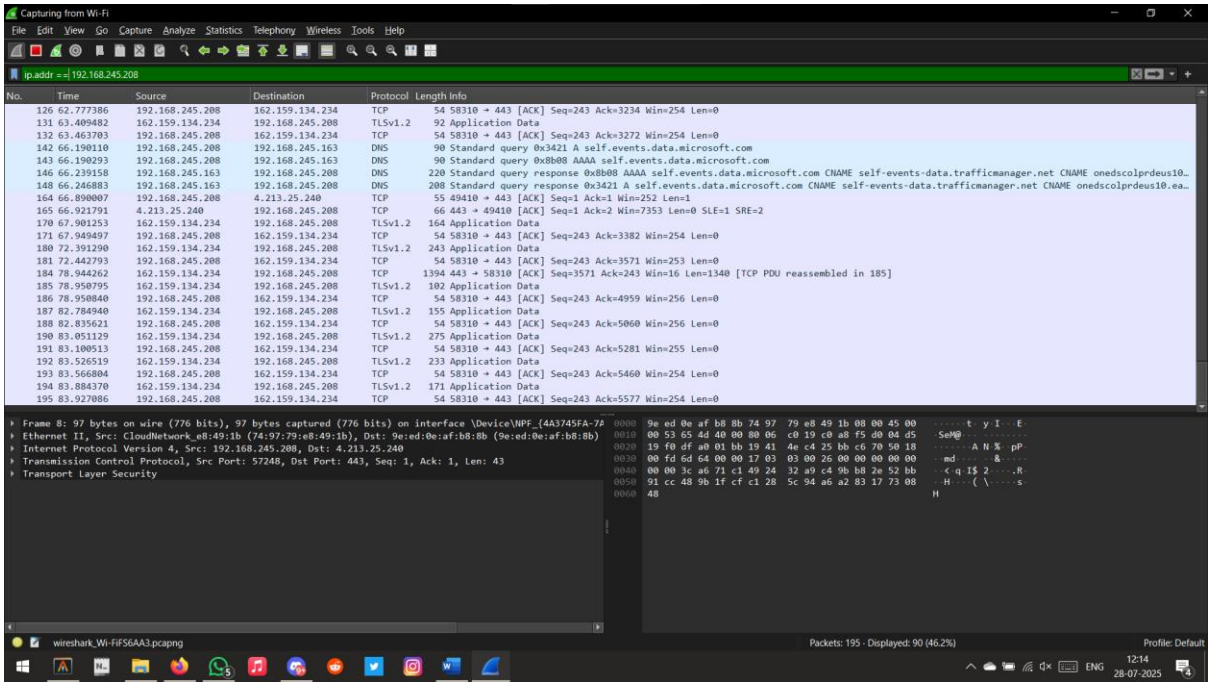
1) Dhcp


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
dhcp
dhcpfo
dhcpv6
dhcpv6.bulk_leasequery
dhcpv6_cablelabs
No. Destination Protocol Length Info
Dynamic Host Configuration Protocol: Protocol
Packets: 65 · Displayed: 0 (0.0%)
Profile: Default
ENG
12:13
28-07-2025

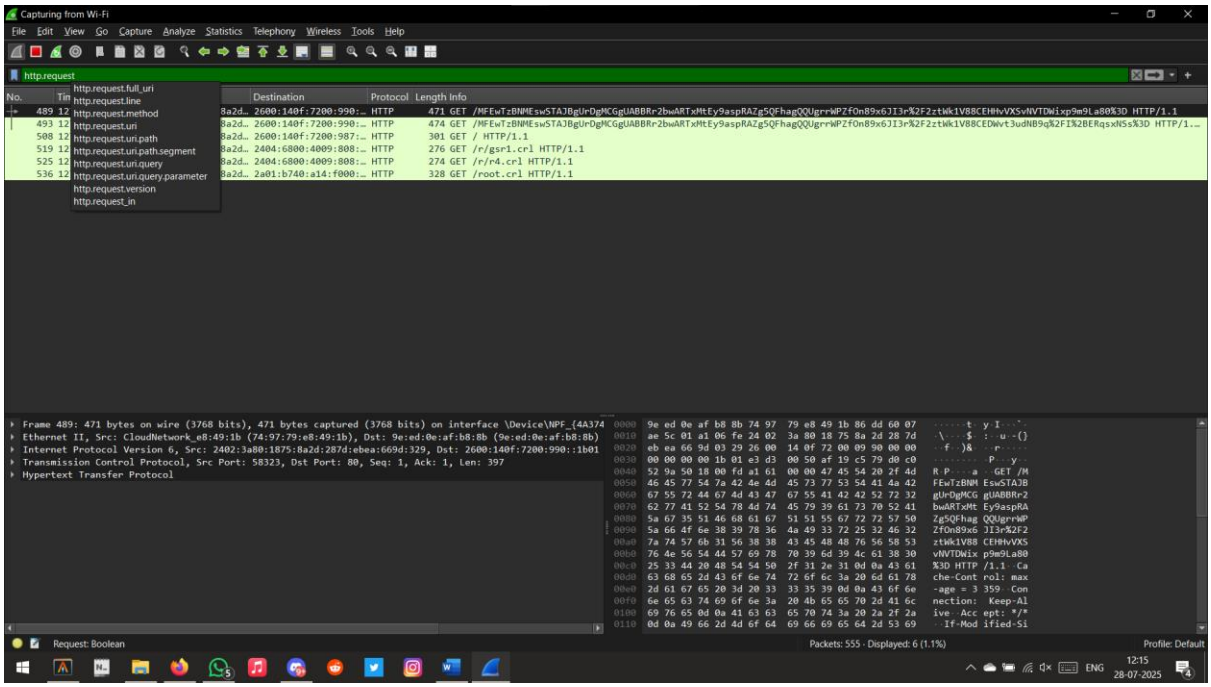
2) Ssl


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
No. Time Source Destination Protocol Length Info
4 2.033340 2402:3a80:1875:8a2d… 2606:4700:4400::681… TLSv1.2 265 Application Data
5 2.033420 2402:3a80:1875:8a2d… 2606:4700:4400::681… TLSv1.2 121 Application Data
8 2.099414 192.168.245.208 4.213.25.240 TLSv1.2 97 Application Data
9 2.129263 4.213.25.240 192.168.245.208 TLSv1.2 228 Application Data
11 2.243161 162.159.134.234 192.168.245.208 TLSv1.2 138 Application Data
13 3.203364 162.159.134.234 192.168.245.208 TLSv1.2 165 Application Data
14 3.239039 192.168.245.208 162.159.134.234 TLSv1.2 175 Application Data
16 3.598321 162.159.134.234 192.168.245.208 TLSv1.2 94 Application Data
18 3.666505 2606:4700:4400::681… 2402:3a80:1875:8a2d… TLSv1.2 219 Application Data
19 3.671816 2606:4700:4400::681… 2402:3a80:1875:8a2d… TLSv1.2 107 Application Data
20 3.671816 2606:4700:4400::681… 2402:3a80:1875:8a2d… TLSv1.2 758 Application Data
21 3.671816 2606:4700:4400::681… 2402:3a80:1875:8a2d… TLSv1.2 105 Application Data
25 5.023049 162.159.134.234 192.168.245.208 TLSv1.2 224 Application Data
27 7.714779 162.159.134.234 192.168.245.208 TLSv1.2 170 Application Data
30 8.717813 162.159.134.234 192.168.245.208 TLSv1.2 165 Application Data
32 9.822761 162.159.134.234 192.168.245.208 TLSv1.2 137 Application Data
35 11.747862 162.159.134.234 192.168.245.208 TLSv1.2 146 Application Data
39 13.030166 162.159.134.234 192.168.245.208 TLSv1.2 228 Application Data
46 21.036178 162.159.134.234 192.168.245.208 TLSv1.2 96 Application Data
48 21.356793 162.159.134.234 192.168.245.208 TLSv1.2 93 Application Data
54 29.359293 162.159.134.234 192.168.245.208 TLSv1.2 177 Application Data
56 29.985772 162.159.134.234 192.168.245.208 TLSv1.2 172 Application Data
65 33.823660 162.159.134.234 192.168.245.208 TLSv1.2 392 Application Data
67 36.087335 162.159.134.234 192.168.245.208 TLSv1.2 339 Application Data
Frame 4: 265 bytes on wire (2120 bits), 265 bytes captured (2120 bits) on interface \Device\NPF_{4A3745F
Ethernet II, Src: CloudNetwork_e8:49:1b (74:97:79:e8:49:1b), Dst: 9e:ed:0e:af:b8:8b (9e:ed:0e:af:b8:8b)
Internet Protocol Version 6, Src: 2402:3a80:1875:8a2d:287d:ebea:669d:329, Dst: 2606:4700:4400::6812:2292
Transmission Control Protocol, Src Port: 58165, Dst Port: 443, Seq: 1, Ack: 1, Len: 191
Transport Layer Security
wireshark_Wi-FiFS6AA3.pcapng
Packets: 86 · Displayed: 33 (38.4%)
Profile: Default
ENG
12:13
28-07-2025

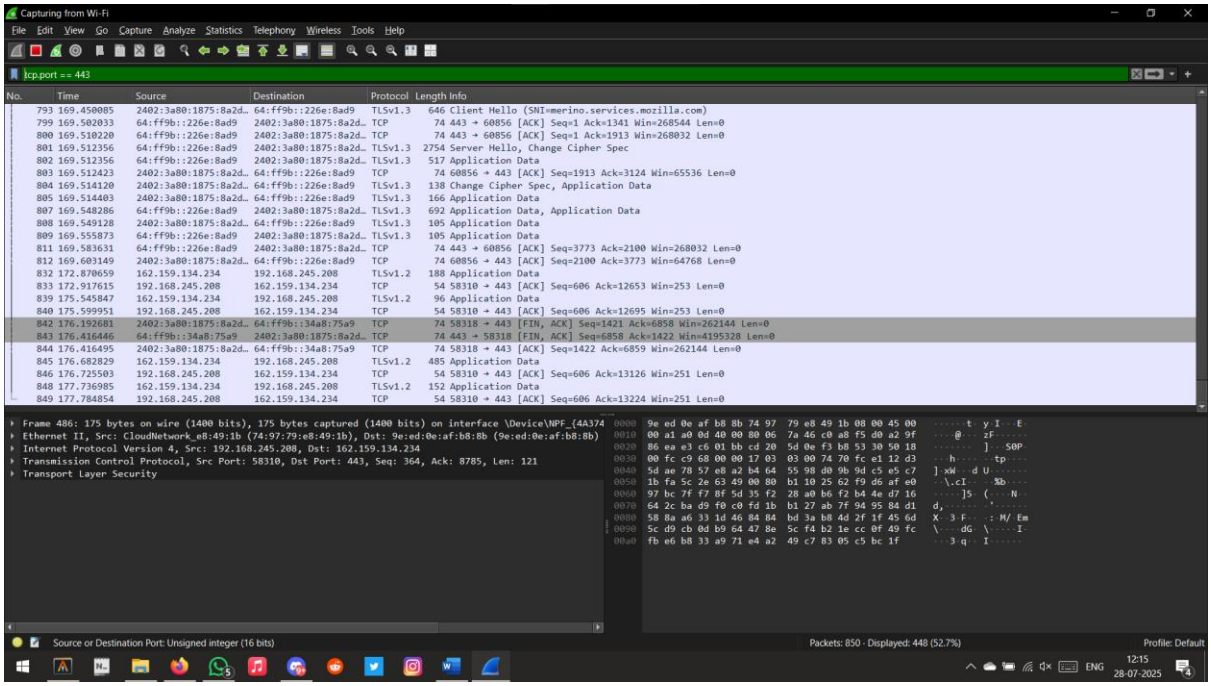
3) Ip and ip.addr == ?



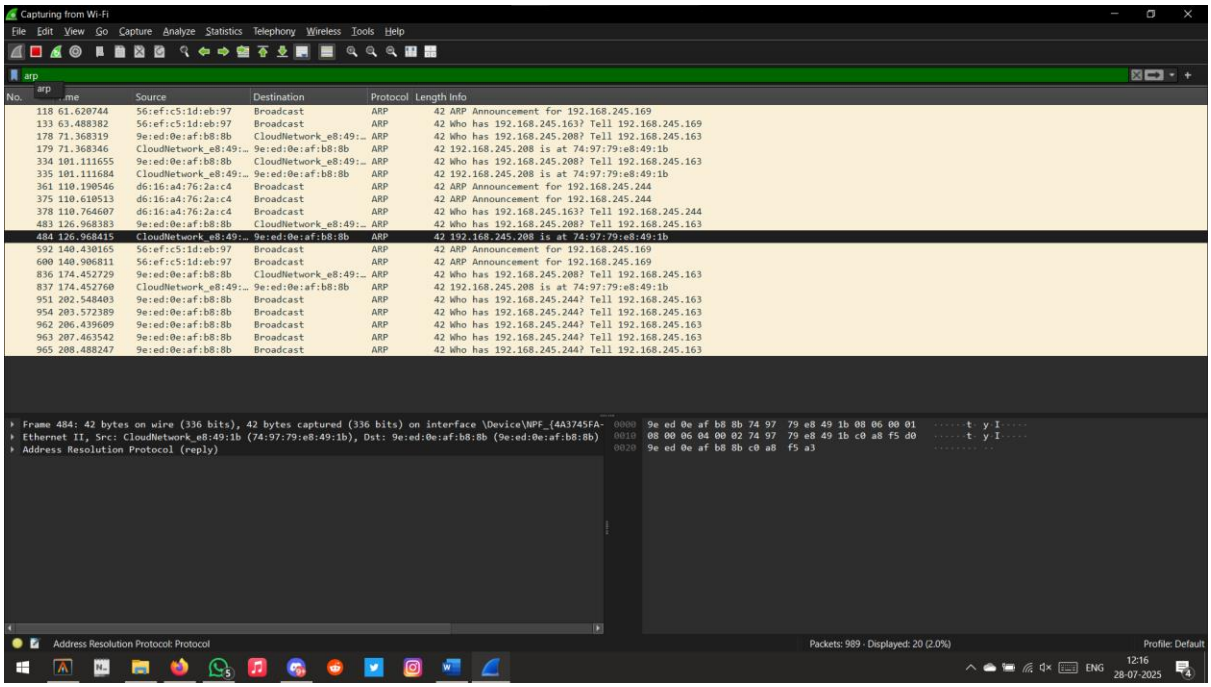
4) http.request



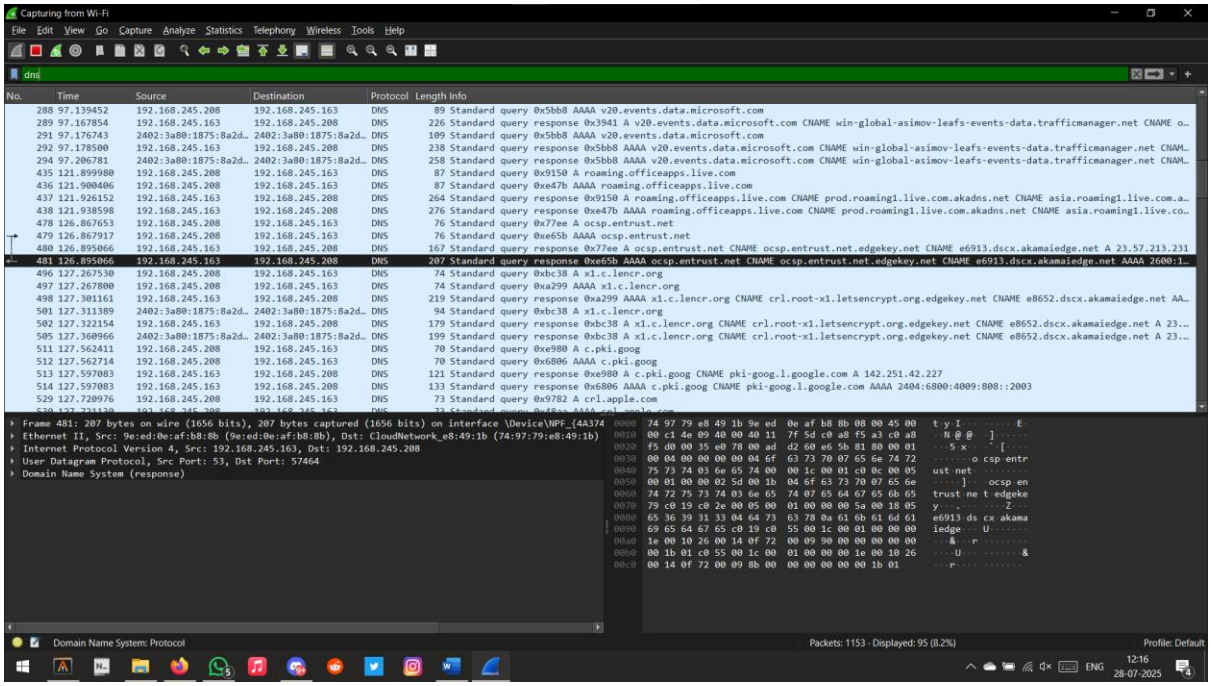
5) tcp.port == 443



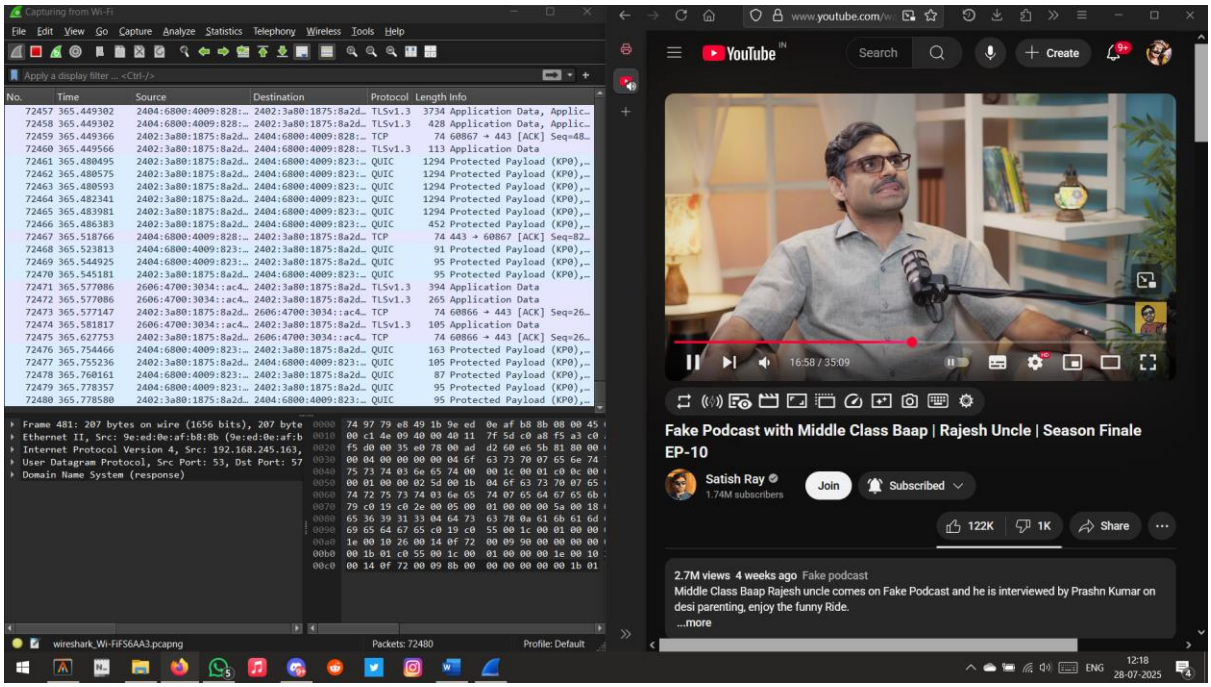
6) arp



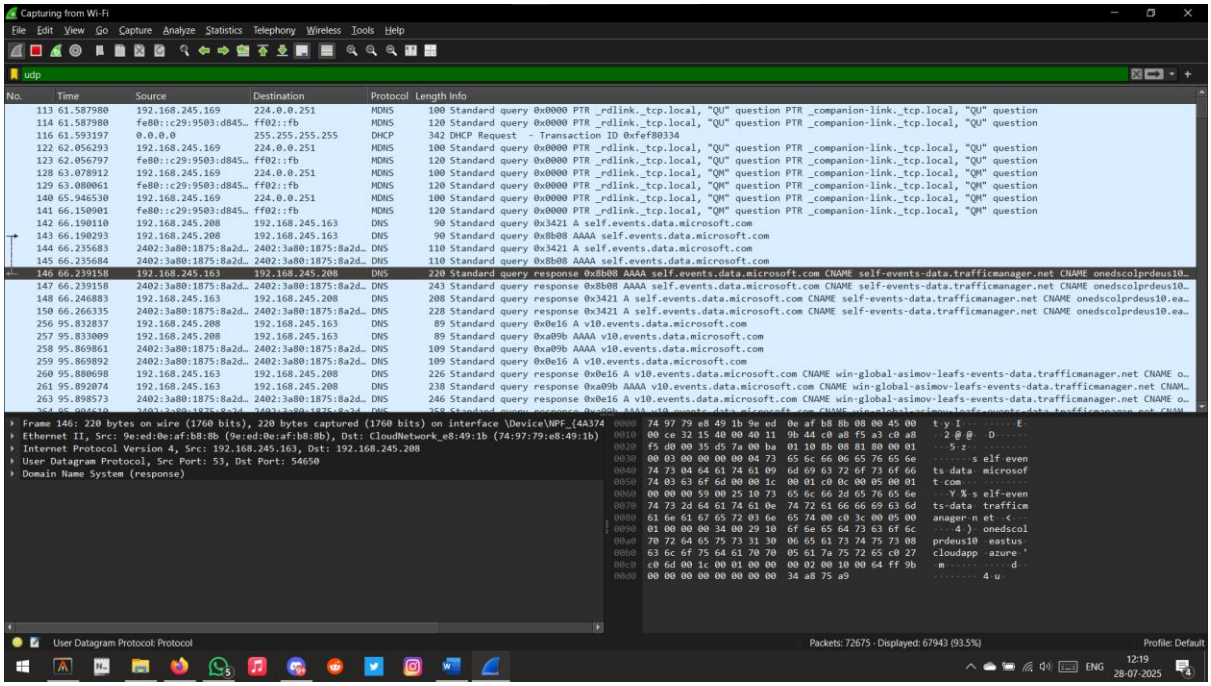
7) dns



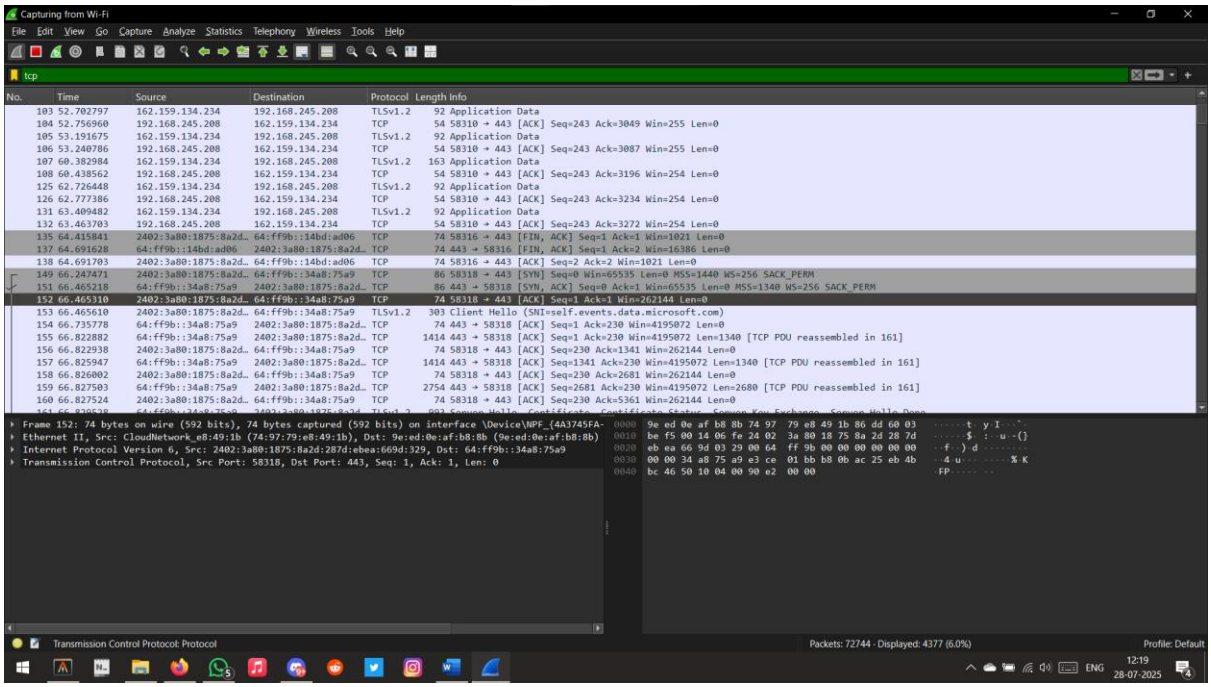
8) while Youtube is playing



9) udp


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
113 61.587980 192.168.245.169 224.0.0.251 MDNS 100 Standard query 0x0000 PTR _rdlink._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question
114 61.587980 fe80::c29:9503:d845… ff02::fb MDNS 120 Standard query 0x0000 PTR _rdlink._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question
116 61.593197 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0xfef80334
122 62.056293 192.168.245.169 224.0.0.251 MDNS 100 Standard query 0x0000 PTR _rdlink._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question
123 62.056797 fe80::c29:9503:d845… ff02::fb MDNS 120 Standard query 0x0000 PTR _rdlink._tcp.local, "QU" question PTR _companion-link._tcp.local, "QU" question
128 63.078912 192.168.245.169 224.0.0.251 MDNS 100 Standard query 0x0000 PTR _rdlink._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question
129 63.080061 fe80::c29:9503:d845… ff02::fb MDNS 120 Standard query 0x0000 PTR _rdlink._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question
140 65.946530 192.168.245.169 224.0.0.251 MDNS 100 Standard query 0x0000 PTR _rdlink._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question
141 66.150901 fe80::c29:9503:d845… ff02::fb MDNS 120 Standard query 0x0000 PTR _rdlink._tcp.local, "QM" question PTR _companion-link._tcp.local, "QM" question
142 66.190110 192.168.245.208 192.168.245.163 DNS 90 Standard query 0x3421 A self.events.data.microsoft.com
143 66.190293 192.168.245.208 192.168.245.163 DNS 90 Standard query 0x8b08 AAAA self.events.data.microsoft.com
144 66.235683 2402:3a80:1875:8a2d… 2402:3a80:1875:8a2d… DNS 110 Standard query 0x3421 A self.events.data.microsoft.com
145 66.235684 2402:3a80:1875:8a2d… 2402:3a80:1875:8a2d… DNS 110 Standard query 0x8b08 AAAA self.events.data.microsoft.com
146 66.239158 192.168.245.163 192.168.245.208 DNS 220 Standard query response 0x8b08 AAAA self.events.data.microsoft.com CNAME self-events-data.trafficmanager.net CNAME onedscolprdeus10…
147 66.239158 2402:3a80:1875:8a2d… 2402:3a80:1875:8a2d… DNS 243 Standard query response 0x8b08 AAAA self.events.data.microsoft.com CNAME self-events-data.trafficmanager.net CNAME onedscolprdeus10…
148 66.246883 192.168.245.163 192.168.245.208 DNS 208 Standard query response 0x3421 A self.events.data.microsoft.com CNAME self-events-data.trafficmanager.net CNAME onedscolprdeus10.ea…
150 66.266335 2402:3a80:1875:8a2d… 2402:3a80:1875:8a2d… DNS 228 Standard query response 0x3421 A self.events.data.microsoft.com CNAME self-events-data.trafficmanager.net CNAME onedscolprdeus10.ea…
256 95.832837 192.168.245.208 192.168.245.163 DNS 89 Standard query 0x0e16 A v10.events.data.microsoft.com
257 95.833009 192.168.245.208 192.168.245.163 DNS 89 Standard query 0xa09b AAAA v10.events.data.microsoft.com
258 95.869861 2402:3a80:1875:8a2d… 2402:3a80:1875:8a2d… DNS 109 Standard query 0xa09b AAAA v10.events.data.microsoft.com
259 95.869892 2402:3a80:1875:8a2d… 2402:3a80:1875:8a2d… DNS 109 Standard query 0x0e16 A v10.events.data.microsoft.com
260 95.880698 192.168.245.163 192.168.245.208 DNS 226 Standard query response 0x0e16 A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net CNAME o…
261 95.892074 192.168.245.163 192.168.245.208 DNS 238 Standard query response 0xa09b AAAA v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net CNAM…
263 95.898573 2402:3a80:1875:8a2d… 2402:3a80:1875:8a2d… DNS 246 Standard query response 0x0e16 A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net CNAME o…
Frame 146: 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface \Device\NPF_{4A374
Ethernet II, Src: 9e:ed:0e:af:b8:8b (9e:ed:0e:af:b8:8b), Dst: CloudNetwork_e8:49:1b (74:97:79:e8:49:1b)
Internet Protocol Version 4, Src: 192.168.245.163, Dst: 192.168.245.208
User Datagram Protocol, Src Port: 53, Dst Port: 54650
Domain Name System (response)
User Datagram Protocol: Protocol
Packets: 72675 · Displayed: 67943 (93.5%)
Profile: Default
ENG
12:19
28-07-2025

10) tcp


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
103 52.702797 162.159.134.234 192.168.245.208 TLSv1.2 92 Application Data
104 52.756960 192.168.245.208 162.159.134.234 TCP 54 58310 → 443 [ACK] Seq=243 Ack=3049 Win=255 Len=0
105 53.191675 162.159.134.234 192.168.245.208 TLSv1.2 92 Application Data
106 53.240786 192.168.245.208 162.159.134.234 TCP 54 58310 → 443 [ACK] Seq=243 Ack=3087 Win=255 Len=0
107 60.382984 162.159.134.234 192.168.245.208 TLSv1.2 163 Application Data
108 60.438562 192.168.245.208 162.159.134.234 TCP 54 58310 → 443 [ACK] Seq=243 Ack=3196 Win=254 Len=0
125 62.726448 162.159.134.234 192.168.245.208 TLSv1.2 92 Application Data
126 62.777386 192.168.245.208 162.159.134.234 TCP 54 58310 → 443 [ACK] Seq=243 Ack=3234 Win=254 Len=0
131 63.409482 162.159.134.234 192.168.245.208 TLSv1.2 92 Application Data
132 63.463703 192.168.245.208 162.159.134.234 TCP 54 58310 → 443 [ACK] Seq=243 Ack=3272 Win=254 Len=0
135 64.415841 2402:3a80:1875:8a2d… 64:ff9b::14bd:ad06 TCP 74 58316 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
137 64.691628 64:ff9b::14bd:ad06 2402:3a80:1875:8a2d… TCP 74 443 → 58316 [FIN, ACK] Seq=1 Ack=2 Win=16386 Len=0
138 64.691703 2402:3a80:1875:8a2d… 64:ff9b::14bd:ad06 TCP 74 58316 → 443 [ACK] Seq=2 Ack=2 Win=1021 Len=0
149 66.247471 2402:3a80:1875:8a2d… 64:ff9b::34a8:75a9 TCP 86 58318 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
151 66.465218 64:ff9b::34a8:75a9 2402:3a80:1875:8a2d… TCP 86 443 → 58318 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM
152 66.465310 2402:3a80:1875:8a2d… 64:ff9b::34a8:75a9 TCP 74 58318 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
153 66.465610 2402:3a80:1875:8a2d… 64:ff9b::34a8:75a9 TLSv1.2 303 Client Hello (SNI=self.events.data.microsoft.com)
154 66.735778 64:ff9b::34a8:75a9 2402:3a80:1875:8a2d… TCP 74 443 → 58318 [ACK] Seq=1 Ack=230 Win=4195072 Len=0
155 66.822882 64:ff9b::34a8:75a9 2402:3a80:1875:8a2d… TCP 1414 443 → 58318 [ACK] Seq=1 Ack=230 Win=4195072 Len=1340 [TCP PDU reassembled in 161]
156 66.822938 2402:3a80:1875:8a2d… 64:ff9b::34a8:75a9 TCP 74 58318 → 443 [ACK] Seq=230 Ack=1341 Win=262144 Len=0
157 66.825947 64:ff9b::34a8:75a9 2402:3a80:1875:8a2d… TCP 1414 443 → 58318 [ACK] Seq=1341 Ack=230 Win=4195072 Len=1340 [TCP PDU reassembled in 161]
158 66.826002 2402:3a80:1875:8a2d… 64:ff9b::34a8:75a9 TCP 74 58318 → 443 [ACK] Seq=230 Ack=2681 Win=262144 Len=0
159 66.827503 64:ff9b::34a8:75a9 2402:3a80:1875:8a2d… TCP 2754 443 → 58318 [ACK] Seq=2681 Ack=230 Win=4195072 Len=2680 [TCP PDU reassembled in 161]
160 66.827524 2402:3a80:1875:8a2d… 64:ff9b::34a8:75a9 TCP 74 58318 → 443 [ACK] Seq=230 Ack=5361 Win=262144 Len=0
Frame 152: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4A3745FA-
Ethernet II, Src: CloudNetwork_e8:49:1b (74:97:79:e8:49:1b), Dst: 9e:ed:0e:af:b8:8b (9e:ed:0e:af:b8:8b)
Internet Protocol Version 6, Src: 2402:3a80:1875:8a2d:287d:ebea:669d:329, Dst: 64:ff9b::34a8:75a9
Transmission Control Protocol, Src Port: 58318, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
Transmission Control Protocol: Protocol
Packets: 72744 · Displayed: 4377 (6.0%)
Profile: Default
ENG
12:19
28-07-2025

Performance (7M)	Journal (3M)	Lab Ethics (2M)	Attendance (3M)	Total (15M)	Faculty Signature