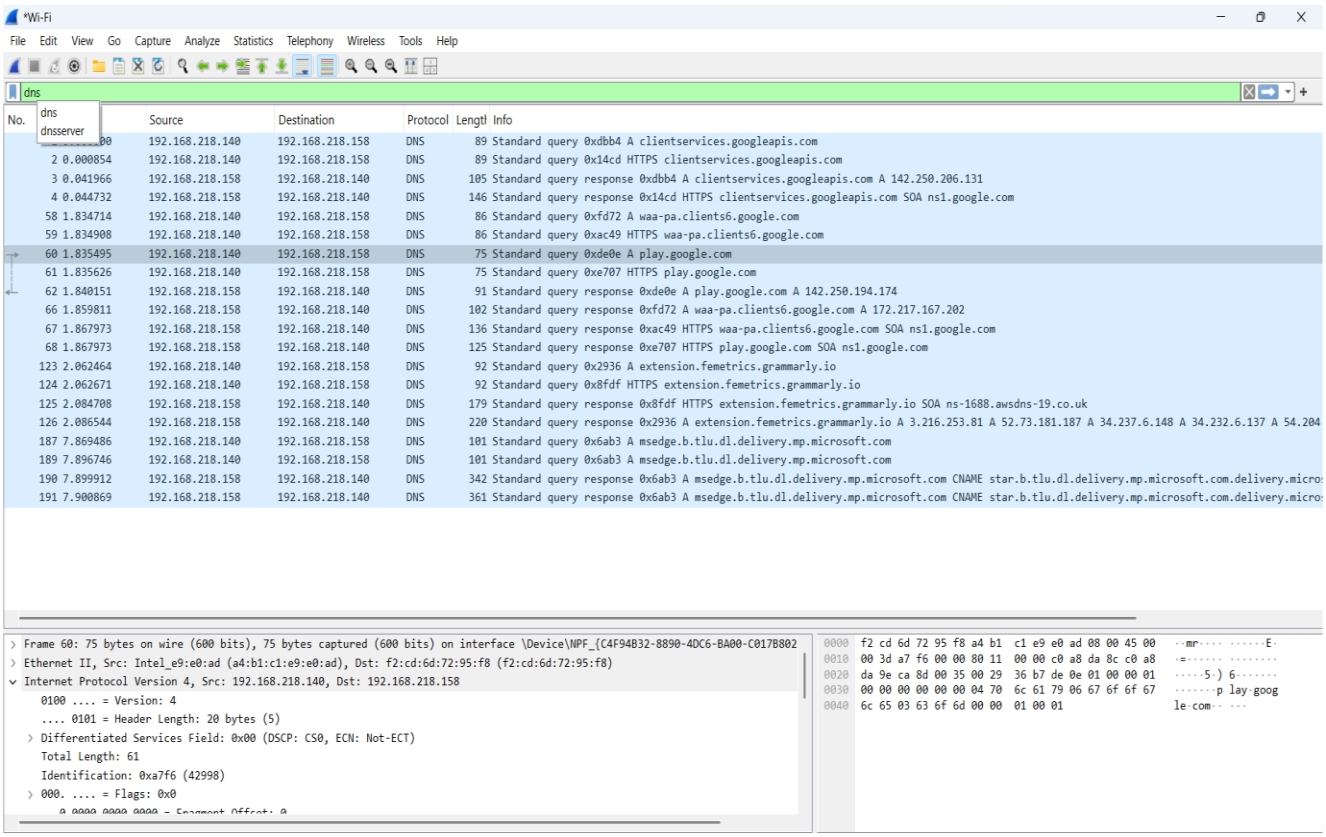
Name: Devansh Srivastava
Registration number: 21BCE0527

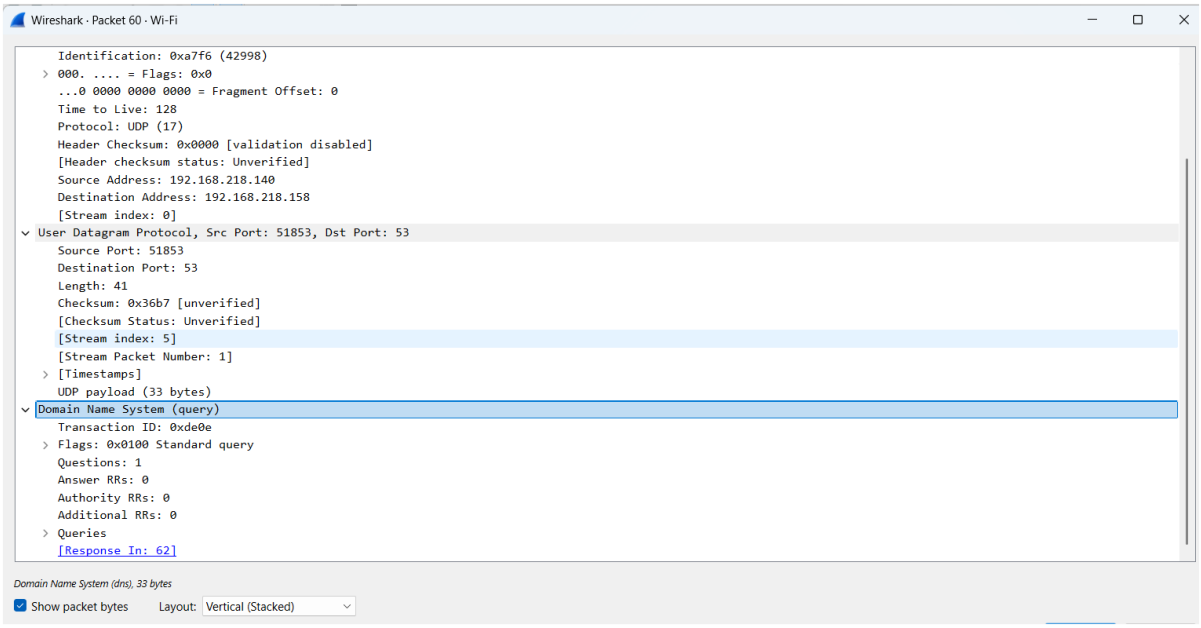
Network Training Programme

Module 7 and 8

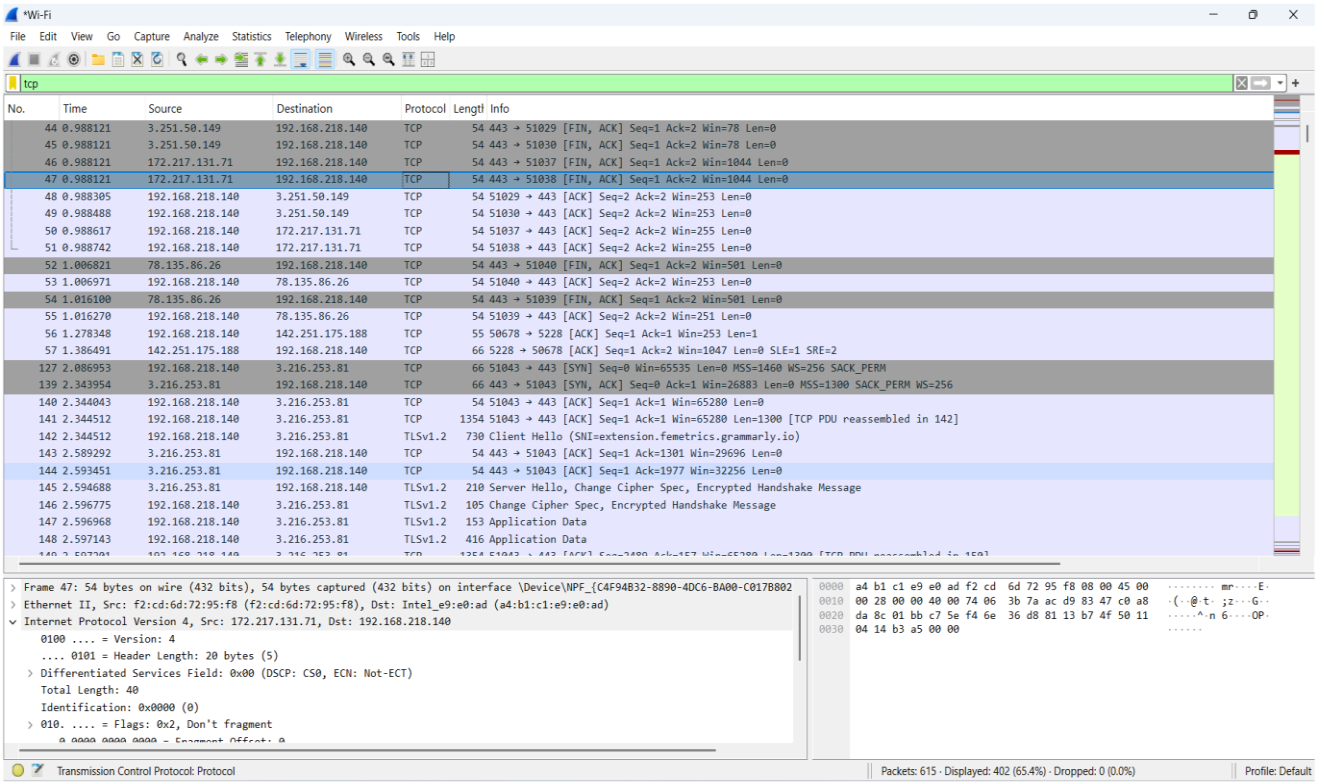
Q2. Use Wireshark to capture and analyze DNS, TCP, UDP traffic and packet header, packet flow, options and flags

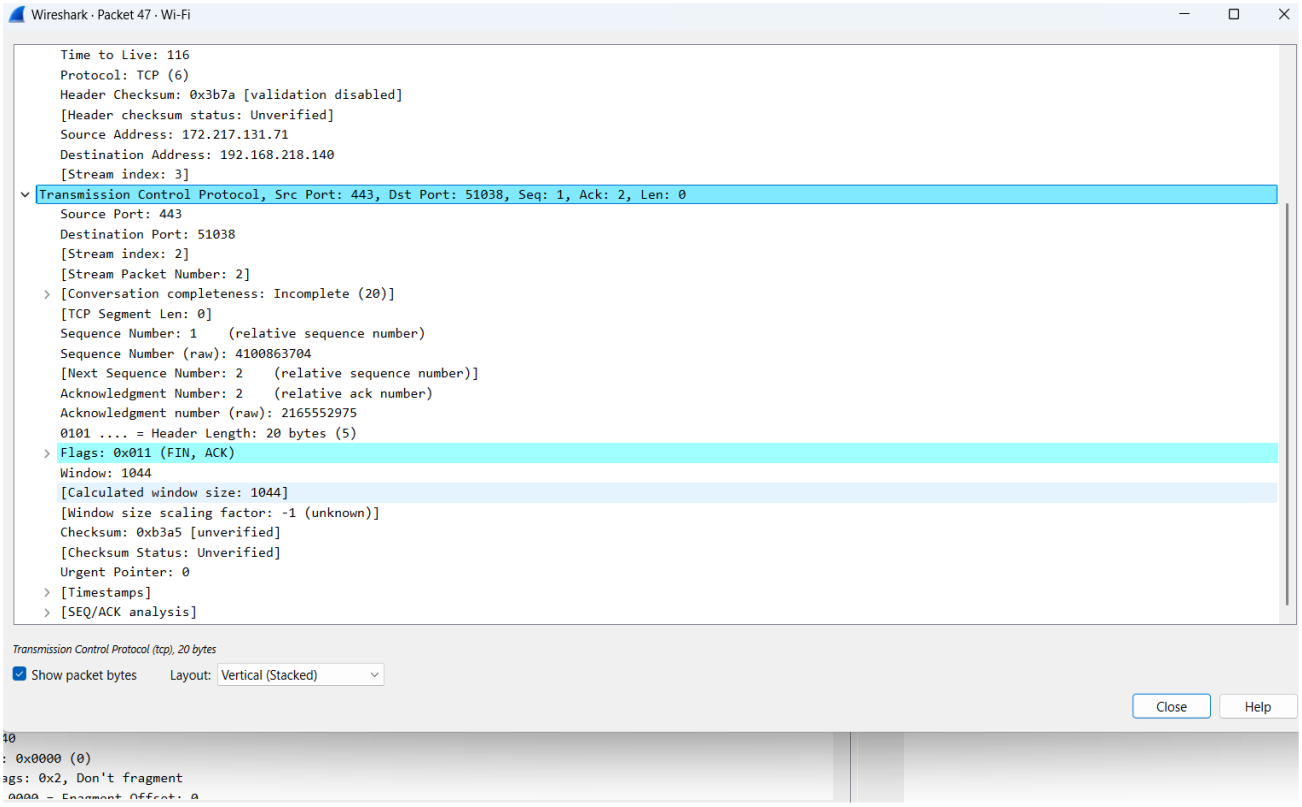
DNS:



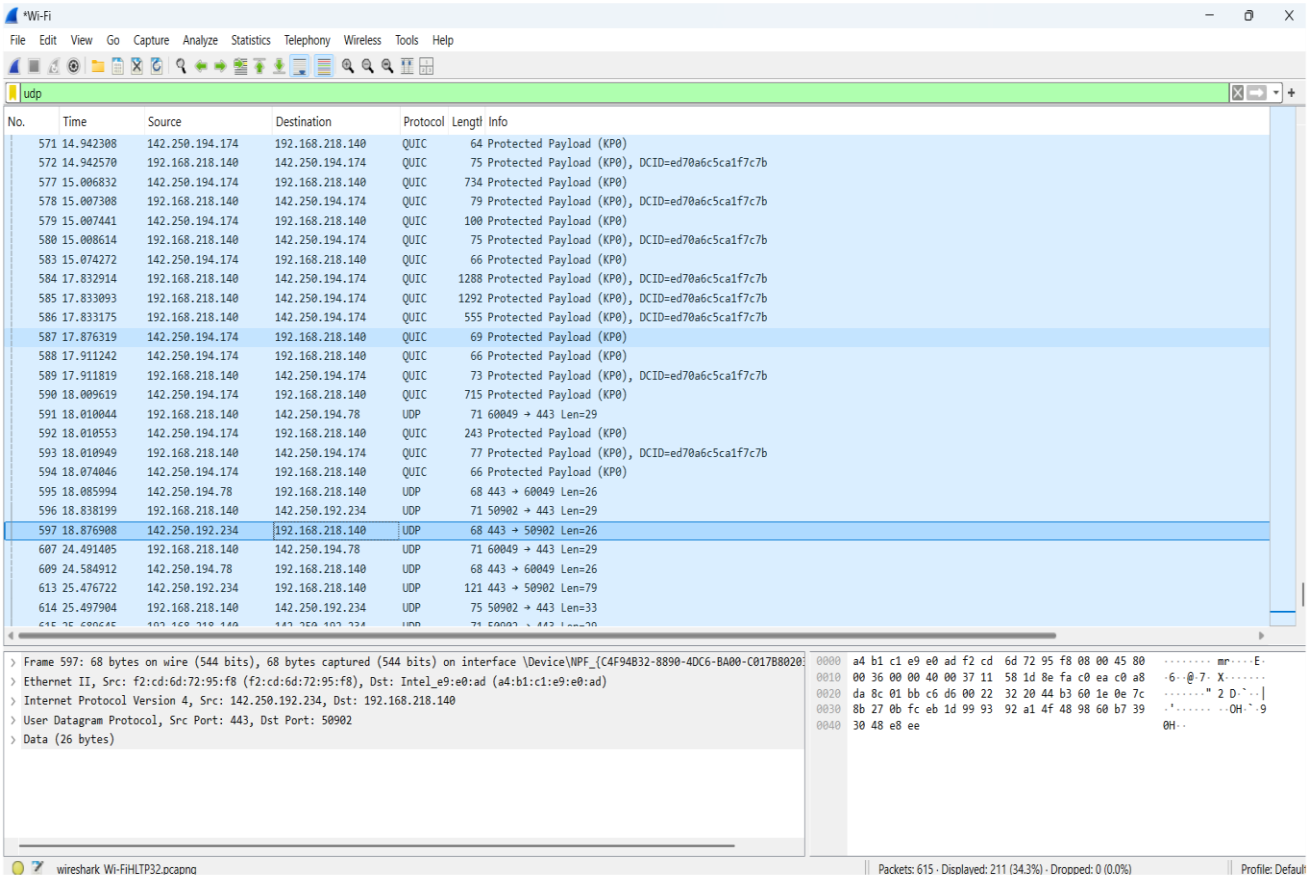

Wireshark · Packet 60 · Wi-Fi
Identification: 0xa7f6 (42998)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.218.140
Destination Address: 192.168.218.158
[Stream index: 0]
User Datagram Protocol, Src Port: 51853, Dst Port: 53
Source Port: 51853
Destination Port: 53
Length: 41
Checksum: 0x36b7 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (33 bytes)
Domain Name System (query)
Transaction ID: 0xde0e
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 62]
Domain Name System (dns), 33 bytes
Show packet bytes
Layout: Vertical (Stacked)

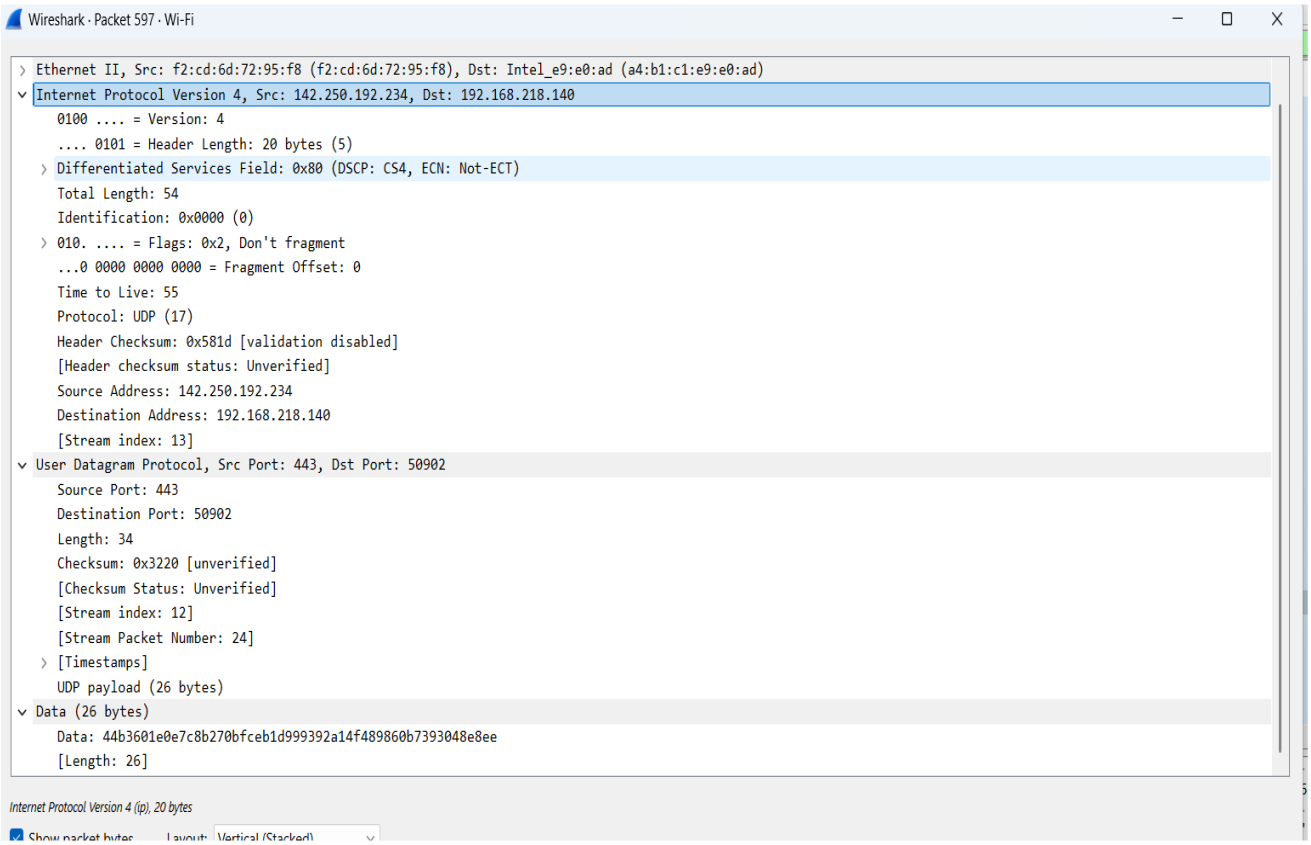
TCP:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
44 0.988121 3.251.50.149 192.168.218.140 TCP 54 443 → 51029 [FIN, ACK] Seq=1 Ack=2 Win=78 Len=0
45 0.988121 3.251.50.149 192.168.218.140 TCP 54 443 → 51030 [FIN, ACK] Seq=1 Ack=2 Win=78 Len=0
46 0.988121 172.217.131.71 192.168.218.140 TCP 54 443 → 51037 [FIN, ACK] Seq=1 Ack=2 Win=1044 Len=0
47 0.988121 172.217.131.71 192.168.218.140 TCP 54 443 → 51038 [FIN, ACK] Seq=1 Ack=2 Win=1044 Len=0
48 0.988305 192.168.218.140 3.251.50.149 TCP 54 51029 → 443 [ACK] Seq=2 Ack=2 Win=253 Len=0
49 0.988488 192.168.218.140 3.251.50.149 TCP 54 51030 → 443 [ACK] Seq=2 Ack=2 Win=253 Len=0
50 0.988617 192.168.218.140 172.217.131.71 TCP 54 51037 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
51 0.988742 192.168.218.140 172.217.131.71 TCP 54 51038 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
52 1.006821 78.135.86.26 192.168.218.140 TCP 54 443 → 51040 [FIN, ACK] Seq=1 Ack=2 Win=501 Len=0
53 1.006971 192.168.218.140 78.135.86.26 TCP 54 51040 → 443 [ACK] Seq=2 Ack=2 Win=253 Len=0
54 1.016100 78.135.86.26 192.168.218.140 TCP 54 443 → 51039 [FIN, ACK] Seq=1 Ack=2 Win=501 Len=0
55 1.016270 192.168.218.140 78.135.86.26 TCP 54 51039 → 443 [ACK] Seq=2 Ack=2 Win=251 Len=0
56 1.278348 192.168.218.140 142.251.175.188 TCP 55 50678 → 5228 [ACK] Seq=1 Ack=1 Win=253 Len=1
57 1.386491 142.251.175.188 192.168.218.140 TCP 66 5228 → 50678 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
127 2.086953 192.168.218.140 3.216.253.81 TCP 66 51043 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
139 2.343954 3.216.253.81 192.168.218.140 TCP 66 443 → 51043 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1300 SACK_PERM WS=256
140 2.344043 192.168.218.140 3.216.253.81 TCP 54 51043 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
141 2.344512 192.168.218.140 3.216.253.81 TCP 1354 51043 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1300 [TCP PDU reassembled in 142]
142 2.344512 192.168.218.140 3.216.253.81 TLSv1.2 730 Client Hello (SNI=extension.femetrics.grammarly.io)
143 2.589292 3.216.253.81 192.168.218.140 TCP 54 443 → 51043 [ACK] Seq=1 Ack=1301 Win=29696 Len=0
144 2.593451 3.216.253.81 192.168.218.140 TCP 54 443 → 51043 [ACK] Seq=1 Ack=1977 Win=32256 Len=0
145 2.594688 3.216.253.81 192.168.218.140 TLSv1.2 210 Server Hello, Change Cipher Spec, Encrypted Handshake Message
146 2.596775 192.168.218.140 3.216.253.81 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
147 2.596968 192.168.218.140 3.216.253.81 TLSv1.2 153 Application Data
148 2.597143 192.168.218.140 3.216.253.81 TLSv1.2 416 Application Data
Frame 47: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C4F94B32-8890-4DC6-BA00-C017B802
Ethernet II, Src: f2:cd:6d:72:95:f8 (f2:cd:6d:72:95:f8), Dst: Intel_e9:e0:ad (a4:b1:c1:e9:e0:ad)
Internet Protocol Version 4, Src: 172.217.131.71, Dst: 192.168.218.140
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x0000 (0)
010. .... = Flags: 0x2, Don't fragment
0000 a4 b1 c1 e9 e0 ad f2 cd 6d 72 95 f8 08 00 45 00 .... mr....E.
0010 00 28 00 00 40 00 74 06 3b 7a ac d9 83 47 c0 a8 .(..@.t. ;z...G..
0020 da 8c 01 bb c7 5e f4 6e 36 d8 81 13 b7 4f 50 11 .....^.n 6....OP.
0030 04 14 b3 a5 00 00 ......
Transmission Control Protocol: Protocol
Packets: 615 · Displayed: 402 (65.4%) · Dropped: 0 (0.0%)
Profile: Default


Wireshark · Packet 47 · Wi-Fi
Time to Live: 116
Protocol: TCP (6)
Header Checksum: 0x3b7a [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.217.131.71
Destination Address: 192.168.218.140
[Stream index: 3]
Transmission Control Protocol, Src Port: 443, Dst Port: 51038, Seq: 1, Ack: 2, Len: 0
Source Port: 443
Destination Port: 51038
[Stream index: 2]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 4100863704
[Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 2165552975
0101 .... = Header Length: 20 bytes (5)
Flags: 0x011 (FIN, ACK)
Window: 1044
[Calculated window size: 1044]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xb3a5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
Transmission Control Protocol (tcp), 20 bytes
Show packet bytes
Layout: Vertical (Stacked)
Close
Help

UDP:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
571 14.942308 142.250.194.174 192.168.218.140 QUIC 64 Protected Payload (KP0)
572 14.942570 192.168.218.140 142.250.194.174 QUIC 75 Protected Payload (KP0), DCID=ed70a6c5ca1f7c7b
577 15.006832 142.250.194.174 192.168.218.140 QUIC 734 Protected Payload (KP0)
578 15.007308 192.168.218.140 142.250.194.174 QUIC 79 Protected Payload (KP0), DCID=ed70a6c5ca1f7c7b
579 15.007441 142.250.194.174 192.168.218.140 QUIC 100 Protected Payload (KP0)
580 15.008614 192.168.218.140 142.250.194.174 QUIC 75 Protected Payload (KP0), DCID=ed70a6c5ca1f7c7b
583 15.074272 142.250.194.174 192.168.218.140 QUIC 66 Protected Payload (KP0)
584 17.832914 192.168.218.140 142.250.194.174 QUIC 1288 Protected Payload (KP0), DCID=ed70a6c5ca1f7c7b
585 17.833093 192.168.218.140 142.250.194.174 QUIC 1292 Protected Payload (KP0), DCID=ed70a6c5ca1f7c7b
586 17.833175 192.168.218.140 142.250.194.174 QUIC 555 Protected Payload (KP0), DCID=ed70a6c5ca1f7c7b
587 17.876319 142.250.194.174 192.168.218.140 QUIC 69 Protected Payload (KP0)
588 17.911242 142.250.194.174 192.168.218.140 QUIC 66 Protected Payload (KP0)
589 17.911819 192.168.218.140 142.250.194.174 QUIC 73 Protected Payload (KP0), DCID=ed70a6c5ca1f7c7b
590 18.009619 142.250.194.174 192.168.218.140 QUIC 715 Protected Payload (KP0)
591 18.010044 192.168.218.140 142.250.194.78 UDP 71 60049 → 443 Len=29
592 18.010553 142.250.194.174 192.168.218.140 QUIC 243 Protected Payload (KP0)
593 18.010949 192.168.218.140 142.250.194.174 QUIC 77 Protected Payload (KP0), DCID=ed70a6c5ca1f7c7b
594 18.074046 142.250.194.174 192.168.218.140 QUIC 66 Protected Payload (KP0)
595 18.085994 142.250.194.78 192.168.218.140 UDP 68 443 → 60049 Len=26
596 18.838199 192.168.218.140 142.250.192.234 UDP 71 50902 → 443 Len=29
597 18.876908 142.250.192.234 192.168.218.140 UDP 68 443 → 50902 Len=26
607 24.491405 192.168.218.140 142.250.194.78 UDP 71 60049 → 443 Len=29
609 24.584912 142.250.194.78 192.168.218.140 UDP 68 443 → 60049 Len=26
613 25.476722 142.250.192.234 192.168.218.140 UDP 121 443 → 50902 Len=79
614 25.497904 192.168.218.140 142.250.192.234 UDP 75 50902 → 443 Len=33
Frame 597: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{C4F94B32-8890-4DC6-BA00-C017B8020
Ethernet II, Src: f2:cd:6d:72:95:f8 (f2:cd:6d:72:95:f8), Dst: Intel_e9:e0:ad (a4:b1:c1:e9:e0:ad)
Internet Protocol Version 4, Src: 142.250.192.234, Dst: 192.168.218.140
User Datagram Protocol, Src Port: 443, Dst Port: 50902
Data (26 bytes)
0000 a4 b1 c1 e9 e0 ad f2 cd 6d 72 95 f8 08 00 45 80
0010 00 36 00 00 40 00 37 11 58 1d 8e fa c0 ea c0 a8
0020 da 8c 01 bb c6 d6 00 22 32 20 44 b3 60 1e 0e 7c
0030 8b 27 0b fc eb 1d 99 93 92 a1 4f 48 98 60 b7 39
0040 30 48 e8 ee
wireshark Wi-FiHLTP32.pcapng
Packets: 615 · Displayed: 211 (34.3%) · Dropped: 0 (0.0%)
Profile: Default



Key Learning:

1. Wireshark helps us in visualising network communication.
2. TCP has connection-oriented flags (SYN, ACK, FIN, etc.).
3. UDP is connectionless and used for faster communication.