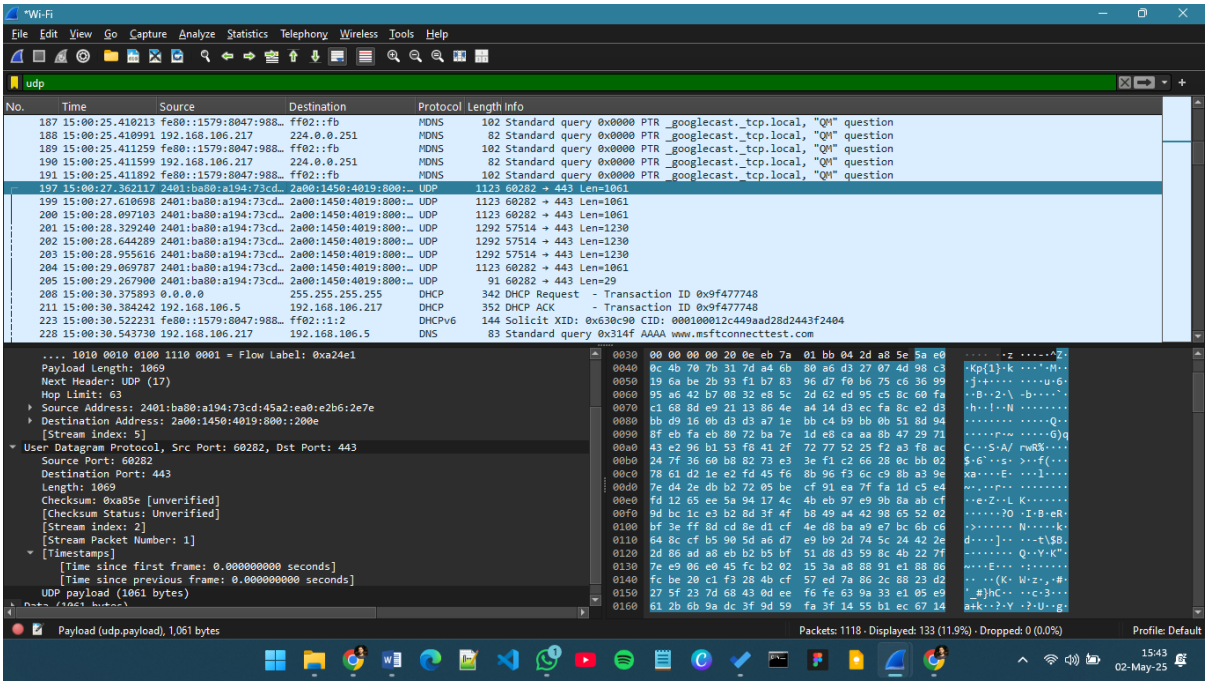
Wireshark: UDP

BSDSF22A001 – Muhammad Rehan

1.

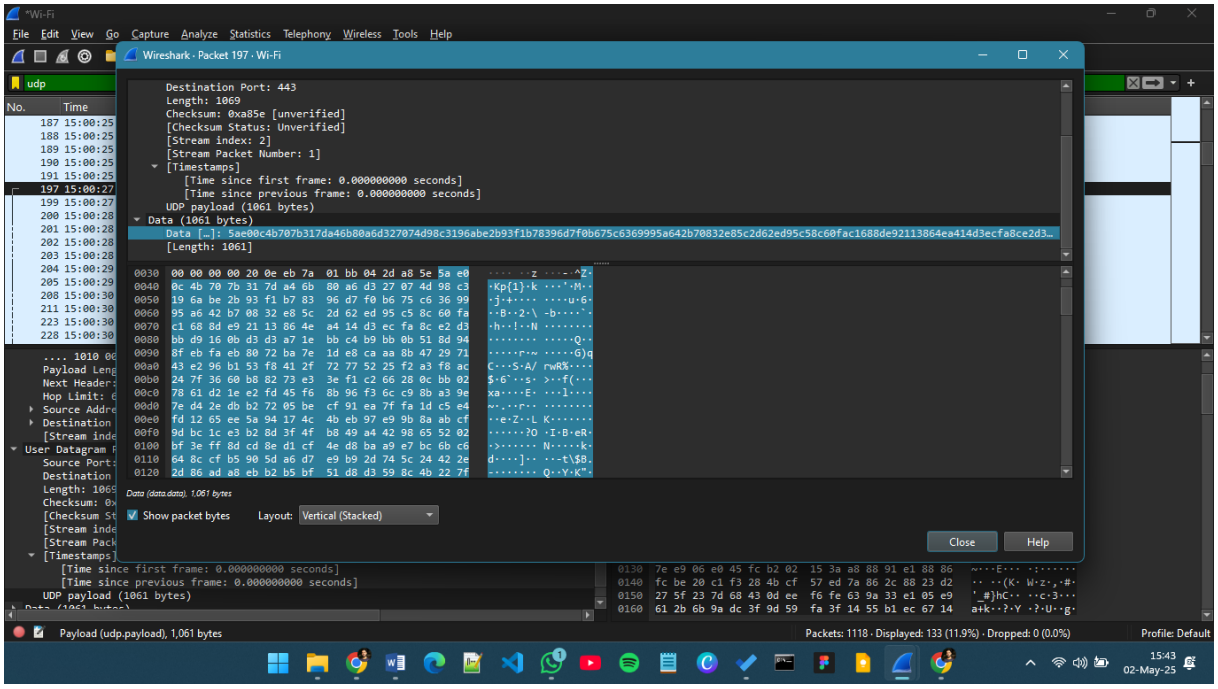
a. **Packet Number:** 197



b. **Protocol Message:**

5ae00c4b707b317da46b80a6d327074d98c3196abe2b93f1b78396d7f0b675c6369995a6
42b70832e85c2d62ed95c58c60fac1688de92113864ea414d3ecfa8ce2d3bbd9160bd3d3
a71ebbc4b9bb0b518d948febfaeb8072ba7e1de8caaa8b47297143e296b153f8412f7277
5225f2a3f8ac247f3660b88273e33ef1c266280cbb027861d21ee2fd45f68b96f36cc98ba3
9e7ed42edbb27205becf91ea7ffa1dc5e4fd1265ee5a94174c4beb97e99b8aabcf9dbc1ce3
b28d3f4fb849a44298655202bf3eff8dcd8ed1cf4ed8baa9e7bc6bc6648ccfb5905da6d7e9
b92d745c24422e2d86ada8ebb2b5bf51d8d3598c4b227f7ee906e045fcb202153aa88891
e18886fcbe20c1f3284bcf57ed7a862c8823d2275f237d68430deef6fe639a33e105e9612b
6b9adc3f9d59fa3f1455b1ec67148d8ffb018cc64188423b9c70732c38553a8d11a87bac2c
91d3ad5e1aeacea728789cfd47c8a9f8888b12f10e0133cd0f186019bf18611baabe86e39
3c72774b2cff2990d9bdac66033c695651b0e4745dae3c7c0361ba5001c003bdceb09038c
213072ba25d2a6ad258242f89ef7869a20a179d658efabca05ed124d668044156ad5184b
7abbb86739979154df40ce2ead0f0f69ffad3484d0f1b72e793734f8ad55d7a0e922ba3b9
d21b84e470c0bcbd4a5bba5fa7517788aa475e834133846a086b685f1aacf3795b642777
e49456296bf200d6bf5daf3dc039c245234ce505eef3eaf8e66d92a79f0b1b46ea1d39ffc6
6dad071525bb5b3c5288bd10566a7c18754e47f24fcc61c407c989080cae9544e1d8f91a6
cf21a4a9e2fd057cfc3e2d2d8f856fc8662cb4a3530dd4dd373835324a705800cb8dda6e3f
c41e9cd9e3643b6314fae98b3e714affe0aff4dd0398731e9f820789fb80e54ce1678de941

2c772a1a2299217e576945d116dae37cd1d63552c858830f22e76a3fbc77d9394ceb237c256123439d6ff8b7e086ae3bd2275ffd6e9d3cddcc1dce0a385d0a49a5319dace0fe5b7a0950c1c0e4e2be35376b6bf48c4f1982b3594c999a5db0ef91131c13f1387bb3ac6178035ea9b8c100754b2d69c0d26d5f0a5379126e0425d565eac08ba1de88e1370a5510d5dd38fc37065e012273e5fd0b926c86e18e6b14af474b4d953d43b3704d437a6dee615da75c51f60e693fb8fbdef2fe40d6c147100392ba8dca8637dbff7e55b3b6e2a7cbc8184f35ded11a0a54a7582dfb514886665879fa721596a69071cecd4eecfece310935d30a6da00a44a2f6ac4475638449dcb205be0a3df233b476f3169d40334a36e0499eeab4ad36334ff1ec3c651dce5e197d0f50b973d1b06fb9e2f5162ac1453ec4c373cb276d03ce877b59bf4ac8d6c0f89143e3e947abd1d0644ecc910d8bb6fd888e1db33898113d24a3bfaf41546952e2074dec0bc8e216ac44c2d3755c48c79e2439e89e67df32fd494b5f45ee1f55cad4a896b2997dd7300efac1c0



c. **No. of header fields:** 4

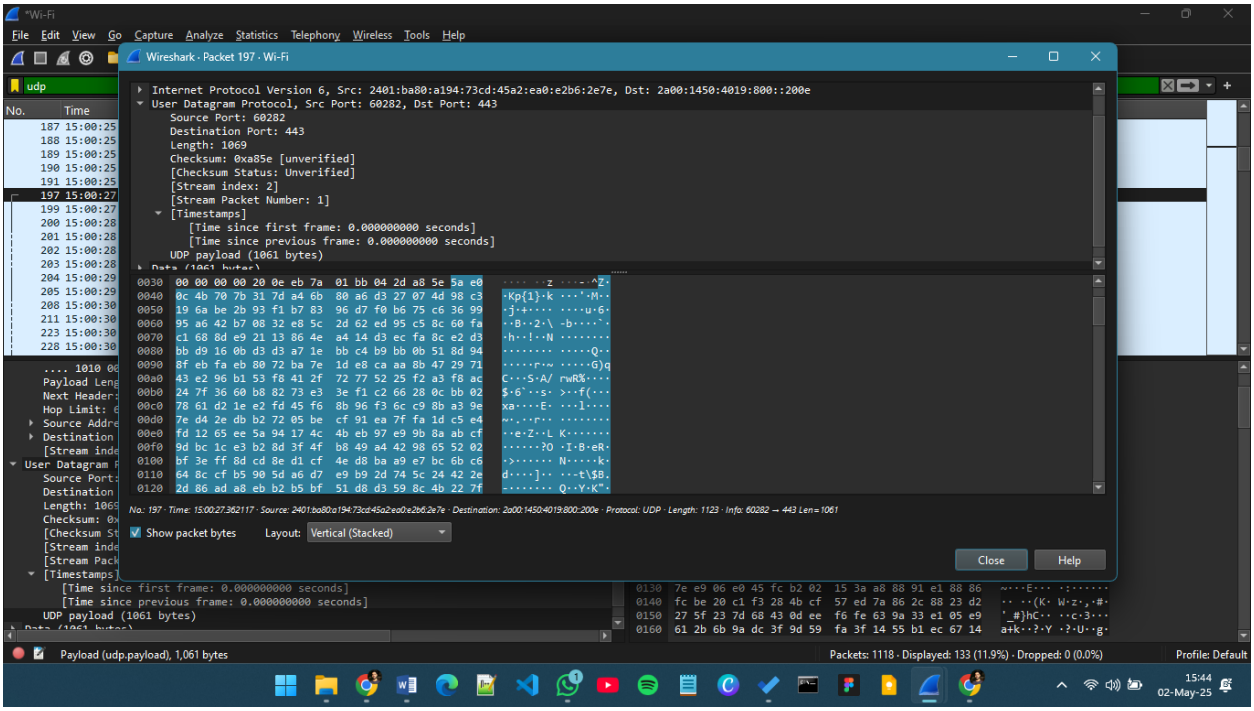
d. Names of fields:

i. **Source Port** (udp.srcport)

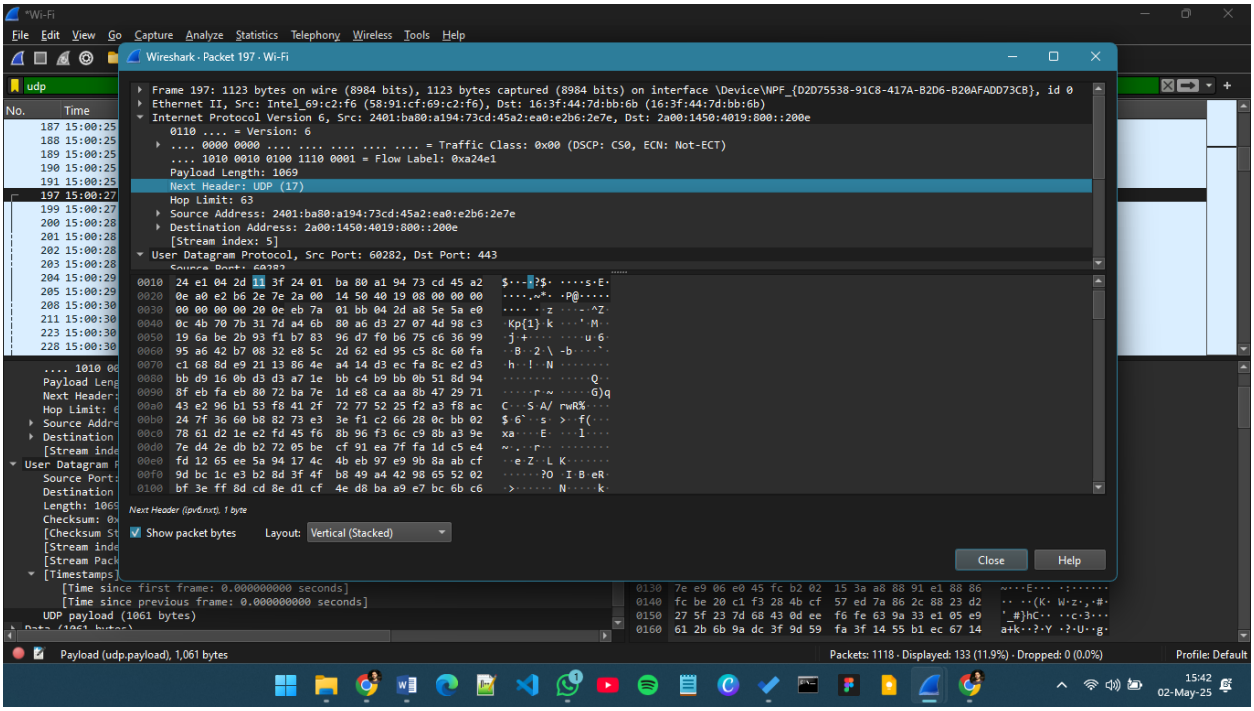
ii. **Destination** (udp.dstport)

iii. **Length** (udp.length)

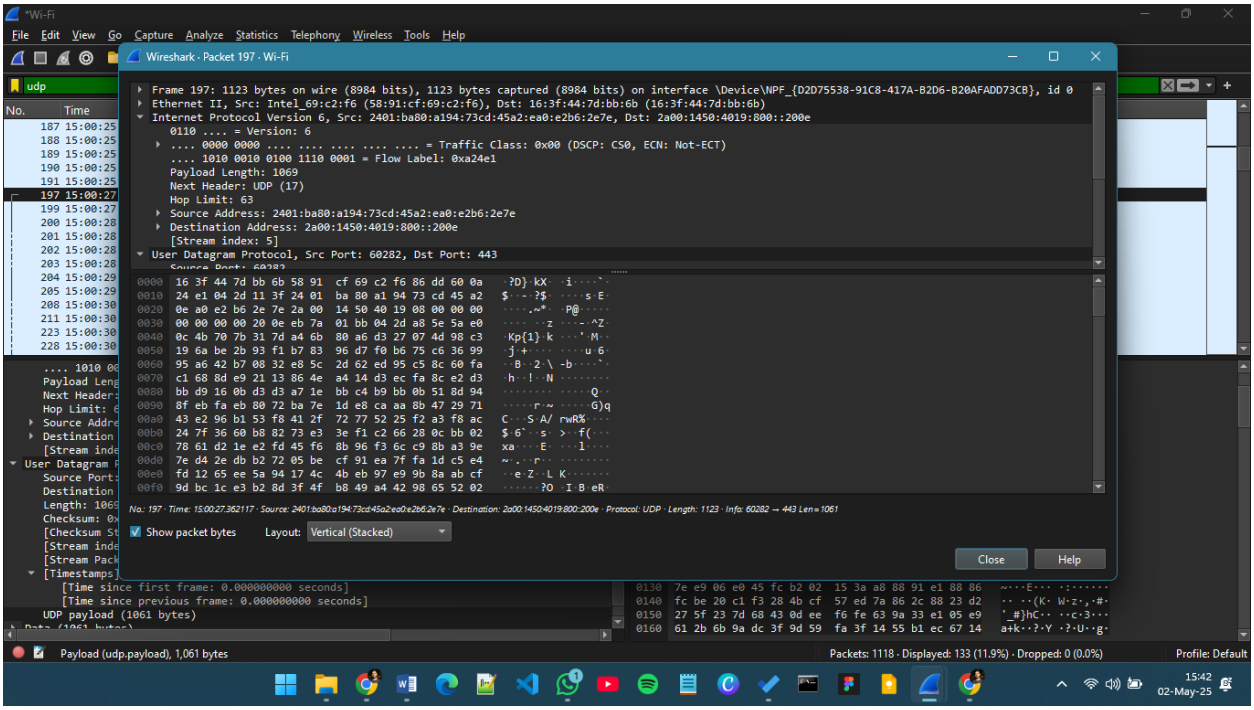
iv. **Checksum** (udp.checksum)

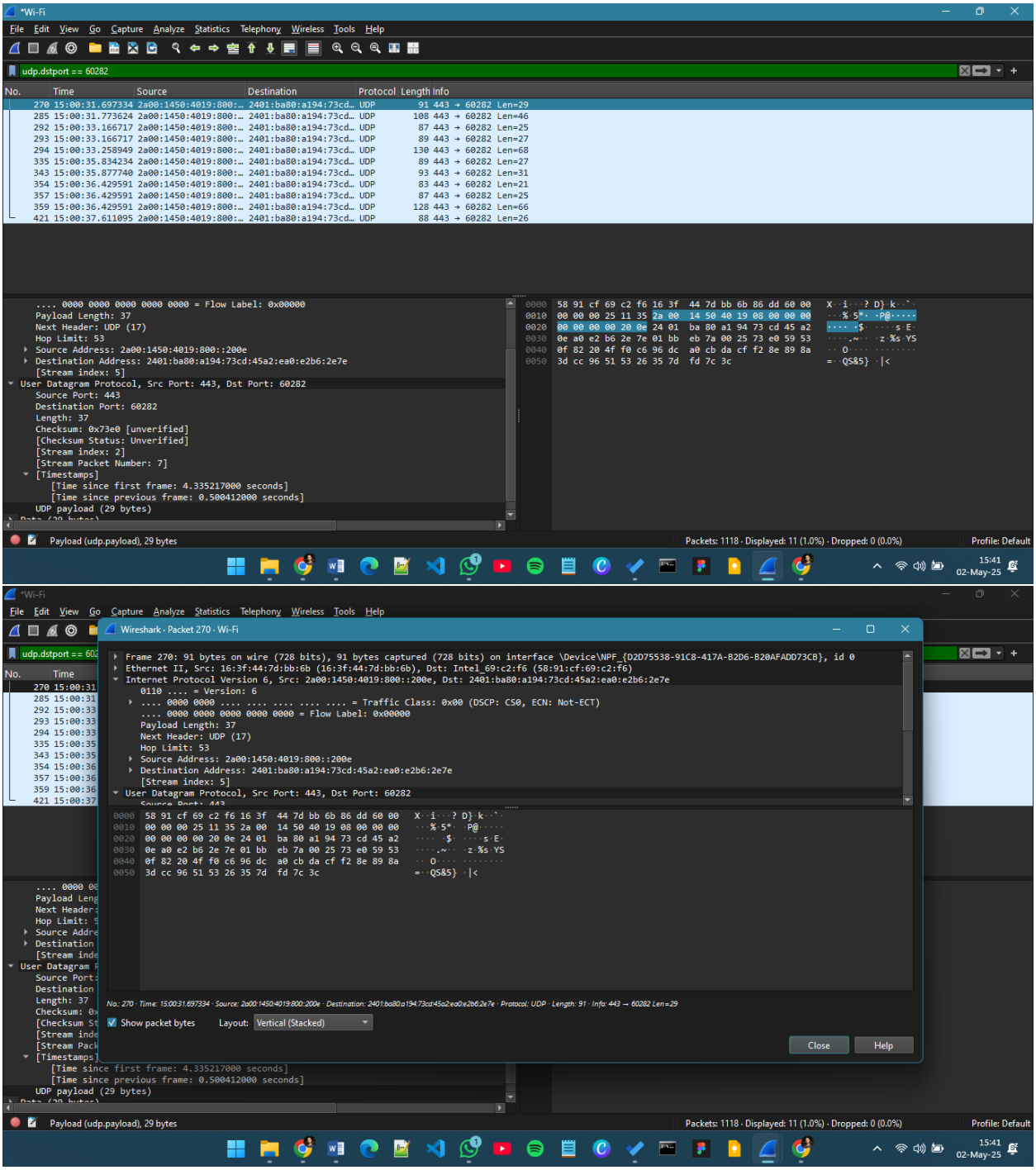


2. Each UDP header field is **2 bytes (16 bits)** long. With 4 fields—Source Port, Destination Port, Length, and Checksum—the total UDP header size is **8 bytes**.
3. The Length field indicates the total size of the UDP segment (header + payload). In my captured packet, the Length is **1069 bytes**, and the UDP header is **8 bytes**, so the UDP payload is **1069 – 8 = 1061 bytes**, which matches the payload shown in Wireshark.
4. The maximum size of a UDP segment is **65,535 bytes**. Subtracting the 8-byte header, the maximum UDP payload is **65,527 bytes**.
5. The Source Port field is 16 bits, so the largest possible source port number is **65,535**.
6. The **protocol number for UDP** is **17** in decimal notation.



7. In my trace file, the **first UDP packet** is **Packet Number 197**, and the **second UDP packet** is **Packet Number 270**. The **source port (60282)** of the first packet is the **destination port** of the second packet, and the **destination port (443)** of the first packet is the **source port** of the second packet, which shows the reply relationship between the two packets.




*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.dstport == 60282
No. Time Source Destination Protocol Length Info
270 15:00:31.697334 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 91 443 → 60282 Len=29
285 15:00:31.773624 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 108 443 → 60282 Len=46
292 15:00:33.166717 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 87 443 → 60282 Len=25
293 15:00:33.166717 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 89 443 → 60282 Len=27
294 15:00:33.258949 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 130 443 → 60282 Len=68
335 15:00:35.834234 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 89 443 → 60282 Len=27
343 15:00:35.877740 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 93 443 → 60282 Len=31
354 15:00:36.429591 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 83 443 → 60282 Len=21
357 15:00:36.429591 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 87 443 → 60282 Len=25
359 15:00:36.429591 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 128 443 → 60282 Len=66
421 15:00:37.611095 2a00:1450:4019:800:… 2401:ba80:a194:73cd… UDP 88 443 → 60282 Len=26
.... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
Payload Length: 37
Next Header: UDP (17)
Hop Limit: 53
Source Address: 2a00:1450:4019:800::200e
Destination Address: 2401:ba80:a194:73cd:45a2:ea0:e2b6:2e7e
[Stream index: 5]
User Datagram Protocol, Src Port: 443, Dst Port: 60282
Source Port: 443
Destination Port: 60282
Length: 37
Checksum: 0x73e0 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
[Stream Packet Number: 7]
[Timestamps]
[Time since first frame: 4.335217000 seconds]
[Time since previous frame: 0.500412000 seconds]
UDP payload (29 bytes)
0000 58 91 cf 69 c2 f6 16 3f 44 7d bb 6b 86 dd 60 00
0010 00 00 00 25 11 35 2a 00 14 50 40 19 08 00 00 00
0020 00 00 00 00 20 0e 24 01 ba 80 a1 94 73 cd 45 a2
0030 0e a0 e2 b6 2e 7e 01 bb eb 7a 00 25 73 e0 59 53
0040 0f 82 20 4f f0 c6 96 dc a0 cb da cf f2 8e 89 8a
0050 3d cc 96 51 53 26 35 7d fd 7c 3c
Payload (udp.payload), 29 bytes
Packets: 1118 · Displayed: 11 (1.0%) · Dropped: 0 (0.0%)
Profile: Default
15:41
02-May-25

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 270 · Wi-Fi
Frame 270: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{D2D75538-91C8-417A-B2D6-B20AFADD73CB}, id 0
Ethernet II, Src: 16:3f:44:7d:bb:6b (16:3f:44:7d:bb:6b), Dst: Intel_69:c2:f6 (58:91:cf:69:c2:f6)
Internet Protocol Version 6, Src: 2a00:1450:4019:800::200e, Dst: 2401:ba80:a194:73cd:45a2:ea0:e2b6:2e7e
0110 .... = Version: 6
.... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
Payload Length: 37
Next Header: UDP (17)
Hop Limit: 53
Source Address: 2a00:1450:4019:800::200e
Destination Address: 2401:ba80:a194:73cd:45a2:ea0:e2b6:2e7e
[Stream index: 5]
User Datagram Protocol, Src Port: 443, Dst Port: 60282
0000 58 91 cf 69 c2 f6 16 3f 44 7d bb 6b 86 dd 60 00
0010 00 00 00 25 11 35 2a 00 14 50 40 19 08 00 00 00
0020 00 00 00 00 20 0e 24 01 ba 80 a1 94 73 cd 45 a2
0030 0e a0 e2 b6 2e 7e 01 bb eb 7a 00 25 73 e0 59 53
0040 0f 82 20 4f f0 c6 96 dc a0 cb da cf f2 8e 89 8a
0050 3d cc 96 51 53 26 35 7d fd 7c 3c
No.: 270 · Time: 15:00:31.697334 · Source: 2a00:1450:4019:800::200e · Destination: 2401:ba80:a194:73cd:45a2:ea0:e2b6:2e7e · Protocol: UDP · Length: 91 · Info: 443 → 60282 Len=29
Show packet bytes
Layout: Vertical (Stacked)
Close
Help
Payload (udp.payload), 29 bytes
Packets: 1118 · Displayed: 11 (1.0%) · Dropped: 0 (0.0%)
Profile: Default
15:41
02-May-25