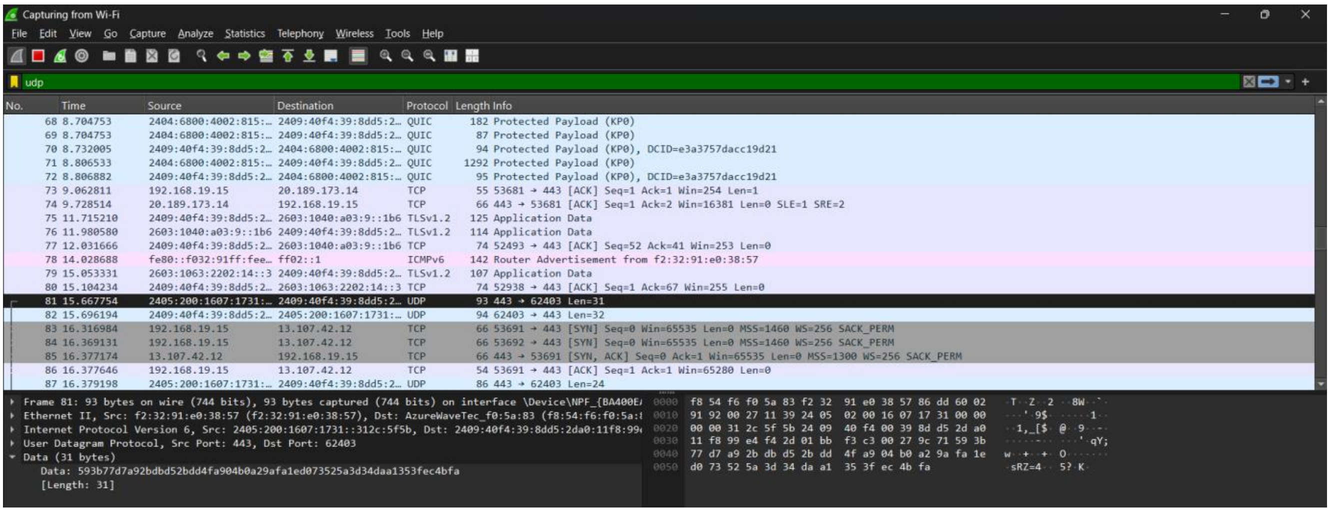
23. Transport layer protocol header analysis using Wire shark- TCP and UDP.

UDP


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

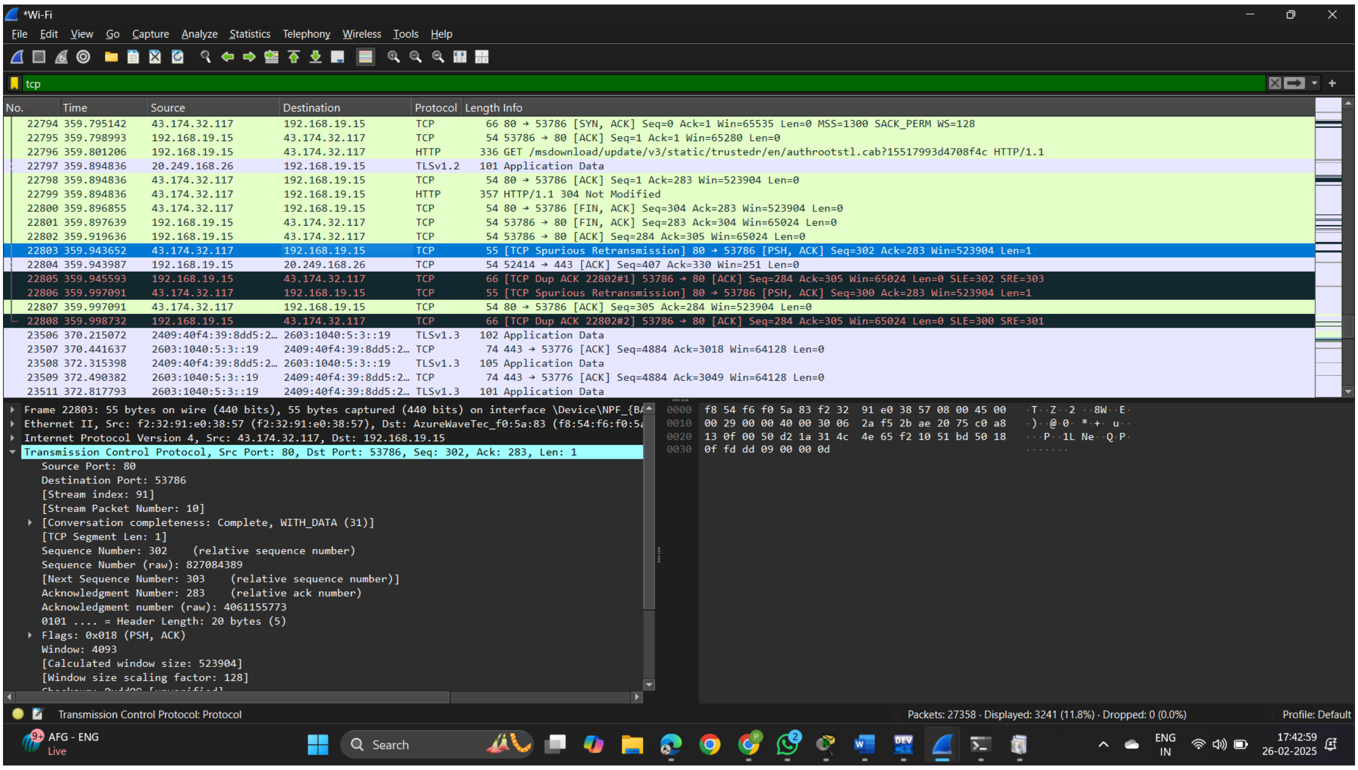
```
udp

No.   Time       Source                 Destination            Protocol Length Info
   68 8.704753   2404:6800:4002:815:…   2409:40f4:39:8dd5:2…   QUIC      182 Protected Payload (KP0)
   69 8.704753   2404:6800:4002:815:…   2409:40f4:39:8dd5:2…   QUIC       87 Protected Payload (KP0)
   70 8.732005   2409:40f4:39:8dd5:2…   2404:6800:4002:815:…   QUIC       94 Protected Payload (KP0), DCID=e3a3757dacc19d21
   71 8.806533   2404:6800:4002:815:…   2409:40f4:39:8dd5:2…   QUIC     1292 Protected Payload (KP0)
   72 8.806882   2409:40f4:39:8dd5:2…   2404:6800:4002:815:…   QUIC       95 Protected Payload (KP0), DCID=e3a3757dacc19d21
   73 9.062811   192.168.19.15          20.189.173.14          TCP        55 53681 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
   74 9.728514   20.189.173.14          192.168.19.15          TCP        66 443 → 53681 [ACK] Seq=1 Ack=2 Win=16381 Len=0 SLE=1 SRE=2
   75 11.715210  2409:40f4:39:8dd5:2…   2603:1040:a03:9::1b6   TLSv1.2   125 Application Data
   76 11.980580  2603:1040:a03:9::1b6   2409:40f4:39:8dd5:2…   TLSv1.2   114 Application Data
   77 12.031666  2409:40f4:39:8dd5:2…   2603:1040:a03:9::1b6   TCP        74 52493 → 443 [ACK] Seq=52 Ack=41 Win=253 Len=0
   78 14.028688  fe80::f032:91ff:fee…   ff02::1                ICMPv6    142 Router Advertisement from f2:32:91:e0:38:57
   79 15.053331  2603:1063:2202:14::3   2409:40f4:39:8dd5:2…   TLSv1.2   107 Application Data
   80 15.104234  2409:40f4:39:8dd5:2…   2603:1063:2202:14::3   TCP        74 52938 → 443 [ACK] Seq=1 Ack=67 Win=255 Len=0
   81 15.667754  2405:200:1607:1731:…   2409:40f4:39:8dd5:2…   UDP        93 443 → 62403 Len=31
   82 15.696194  2409:40f4:39:8dd5:2…   2405:200:1607:1731:…   UDP        94 62403 → 443 Len=32
   83 16.316984  192.168.19.15          13.107.42.12           TCP        66 53691 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   84 16.369131  192.168.19.15          13.107.42.12           TCP        66 53692 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   85 16.377174  13.107.42.12           192.168.19.15          TCP        66 443 → 53691 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=256 SACK_PERM
   86 16.377646  192.168.19.15          13.107.42.12           TCP        54 53691 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
   87 16.379198  2405:200:1607:1731:…   2409:40f4:39:8dd5:2…   UDP        86 443 → 62403 Len=24
```

```
> Frame 81: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{BA400E/
> Ethernet II, Src: f2:32:91:e0:38:57 (f2:32:91:e0:38:57), Dst: AzureWaveTec_f0:5a:83 (f8:54:f6:f0:5a:8
> Internet Protocol Version 6, Src: 2405:200:1607:1731::312c:5f5b, Dst: 2409:40f4:39:8dd5:2da0:11f8:99
> User Datagram Protocol, Src Port: 443, Dst Port: 62403
v Data (31 bytes)
    Data: 593b77d7a92bdbd52bdd4fa904b0a29afa1ed073525a3d34daa1353fec4bfa
    [Length: 31]
```

```
0000  f8 54 f6 f0 5a 83 f2 32  91 e0 38 57 86 dd 60 02   ·T··Z··2 ··8W··`·
0010  91 92 00 27 11 39 24 05  02 00 16 07 17 31 00 00   ···'·9$· ·····1··
0020  00 00 31 2c 5f 5b 24 09  40 f4 00 39 8d d5 2d a0   ··1,_[$· @··9··-·
0030  11 f8 99 e4 f4 2d 01 bb  f3 c3 00 27 9c 71 59 3b   ·····-·· ···'·qY;
0040  77 d7 a9 2b db d5 2b dd  4f a9 04 b0 a2 9a fa 1e   w··+··+· O·······
0050  d0 73 52 5a 3d 34 da a1  35 3f ec 4b fa            ·sRZ=4·· 5?·K·
```

TCP


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp

No.    Time        Source                 Destination            Protocol Length Info
 22794 359.795142  43.174.32.117          192.168.19.15          TCP        66 80 → 53786 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM WS=128
 22795 359.798993  192.168.19.15          43.174.32.117          TCP        54 53786 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 22796 359.801206  192.168.19.15          43.174.32.117          HTTP      336 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?15517993d4708f4c HTTP/1.1
 22797 359.894836  20.249.168.26          192.168.19.15          TLSv1.2   101 Application Data
 22798 359.894836  43.174.32.117          192.168.19.15          TCP        54 80 → 53786 [ACK] Seq=1 Ack=283 Win=523904 Len=0
 22799 359.894836  43.174.32.117          192.168.19.15          HTTP      357 HTTP/1.1 304 Not Modified
 22800 359.896855  43.174.32.117          192.168.19.15          TCP        54 80 → 53786 [FIN, ACK] Seq=304 Ack=283 Win=523904 Len=0
 22801 359.897639  192.168.19.15          43.174.32.117          TCP        54 53786 → 80 [FIN, ACK] Seq=283 Ack=304 Win=65024 Len=0
 22802 359.919636  192.168.19.15          43.174.32.117          TCP        54 53786 → 80 [ACK] Seq=284 Ack=305 Win=65024 Len=0
 22803 359.943652  43.174.32.117          192.168.19.15          TCP        55 [TCP Spurious Retransmission] 80 → 53786 [PSH, ACK] Seq=302 Ack=283 Win=523904 Len=1
 22804 359.943987  192.168.19.15          20.249.168.26          TCP        54 52414 → 443 [ACK] Seq=407 Ack=330 Win=251 Len=0
 22805 359.945593  192.168.19.15          43.174.32.117          TCP        66 [TCP Dup ACK 22802#1] 53786 → 80 [ACK] Seq=284 Ack=305 Win=65024 Len=0 SLE=302 SRE=303
 22806 359.997091  43.174.32.117          192.168.19.15          TCP        55 [TCP Spurious Retransmission] 80 → 53786 [PSH, ACK] Seq=300 Ack=283 Win=523904 Len=1
 22807 359.997091  43.174.32.117          192.168.19.15          TCP        54 80 → 53786 [ACK] Seq=305 Ack=284 Win=523904 Len=0
 22808 359.998732  192.168.19.15          43.174.32.117          TCP        66 [TCP Dup ACK 22802#2] 53786 → 80 [ACK] Seq=284 Ack=305 Win=65024 Len=0 SLE=300 SRE=301
 23506 370.215072  2409:40f4:39:8dd5:2…   2603:1040:5:3::19      TLSv1.3   102 Application Data
 23507 370.441637  2603:1040:5:3::19      2409:40f4:39:8dd5:2…   TCP        74 443 → 53776 [ACK] Seq=4884 Ack=3018 Win=64128 Len=0
 23508 372.315398  2409:40f4:39:8dd5:2…   2603:1040:5:3::19      TLSv1.3   105 Application Data
 23509 372.490382  2603:1040:5:3::19      2409:40f4:39:8dd5:2…   TCP        74 443 → 53776 [ACK] Seq=4884 Ack=3049 Win=64128 Len=0
 23511 372.817793  2603:1040:5:3::19      2409:40f4:39:8dd5:2…   TLSv1.3   101 Application Data
```

```
> Frame 22803: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{BA
> Ethernet II, Src: f2:32:91:e0:38:57 (f2:32:91:e0:38:57), Dst: AzureWaveTec_f0:5a:83 (f8:54:f6:f0:5a
> Internet Protocol Version 4, Src: 43.174.32.117, Dst: 192.168.19.15
v Transmission Control Protocol, Src Port: 80, Dst Port: 53786, Seq: 302, Ack: 283, Len: 1
    Source Port: 80
    Destination Port: 53786
    [Stream index: 91]
    [Stream Packet Number: 10]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1]
    Sequence Number: 302    (relative sequence number)
    Sequence Number (raw): 827084389
    [Next Sequence Number: 303    (relative sequence number)]
    Acknowledgment Number: 283    (relative ack number)
    Acknowledgment number (raw): 4061155773
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 4093
    [Calculated window size: 523904]
    [Window size scaling factor: 128]
```

```
0000  f8 54 f6 f0 5a 83 f2 32  91 e0 38 57 08 00 45 00   ·T··Z··2 ··8W··E·
0010  00 29 00 00 40 00 30 06  2a f5 2b ae 20 75 c0 a8   ·)··@·0· *·+· u··
0020  13 0f 00 50 d2 1a 31 4c  4e 65 f2 10 51 bd 50 18   ···P··1L Ne··Q·P·
0030  0f fd dd 09 00 00 0d                               ·······
```

Transmission Control Protocol: Protocol

Packets: 27358 · Displayed: 3241 (11.8%) · Dropped: 0 (0.0%)

Profile: Default