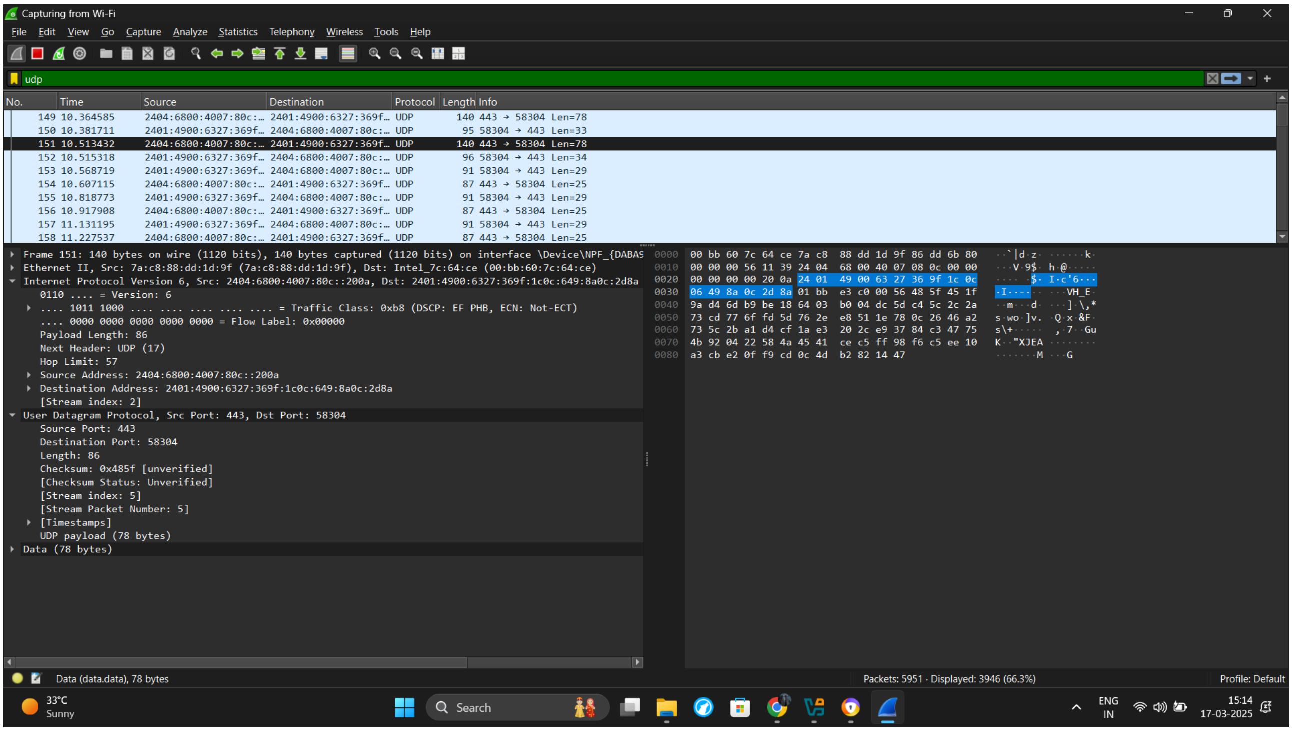
# UDP Traffic


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
33°C
Sunny
Search
ENG
IN
15:14
17-03-2025

udp

```
No.   Time       Source                  Destination             Protocol Length Info
  149 10.364585  2404:6800:4007:80c:…  2401:4900:6327:369f…  UDP      140 443 → 58304 Len=78
  150 10.381711  2401:4900:6327:369f…  2404:6800:4007:80c:…  UDP       95 58304 → 443 Len=33
  151 10.513432  2404:6800:4007:80c:…  2401:4900:6327:369f…  UDP      140 443 → 58304 Len=78
  152 10.515318  2401:4900:6327:369f…  2404:6800:4007:80c:…  UDP       96 58304 → 443 Len=34
  153 10.568719  2401:4900:6327:369f…  2404:6800:4007:80c:…  UDP       91 58304 → 443 Len=29
  154 10.607115  2404:6800:4007:80c:…  2401:4900:6327:369f…  UDP       87 443 → 58304 Len=25
  155 10.818773  2401:4900:6327:369f…  2404:6800:4007:80c:…  UDP       91 58304 → 443 Len=29
  156 10.917908  2404:6800:4007:80c:…  2401:4900:6327:369f…  UDP       87 443 → 58304 Len=25
  157 11.131195  2401:4900:6327:369f…  2404:6800:4007:80c:…  UDP       91 58304 → 443 Len=29
  158 11.227537  2404:6800:4007:80c:…  2401:4900:6327:369f…  UDP       87 443 → 58304 Len=25
```

```
Frame 151: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface \Device\NPF_{DABA9
Ethernet II, Src: 7a:c8:88:dd:1d:9f (7a:c8:88:dd:1d:9f), Dst: Intel_7c:64:ce (00:bb:60:7c:64:ce)
Internet Protocol Version 6, Src: 2404:6800:4007:80c::200a, Dst: 2401:4900:6327:369f:1c0c:649:8a0c:2d8a
    0110 .... = Version: 6
    .... 1011 1000 .... .... .... .... .... = Traffic Class: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 86
    Next Header: UDP (17)
    Hop Limit: 57
    Source Address: 2404:6800:4007:80c::200a
    Destination Address: 2401:4900:6327:369f:1c0c:649:8a0c:2d8a
    [Stream index: 2]
User Datagram Protocol, Src Port: 443, Dst Port: 58304
    Source Port: 443
    Destination Port: 58304
    Length: 86
    Checksum: 0x485f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
    [Stream Packet Number: 5]
    [Timestamps]
    UDP payload (78 bytes)
Data (78 bytes)
```

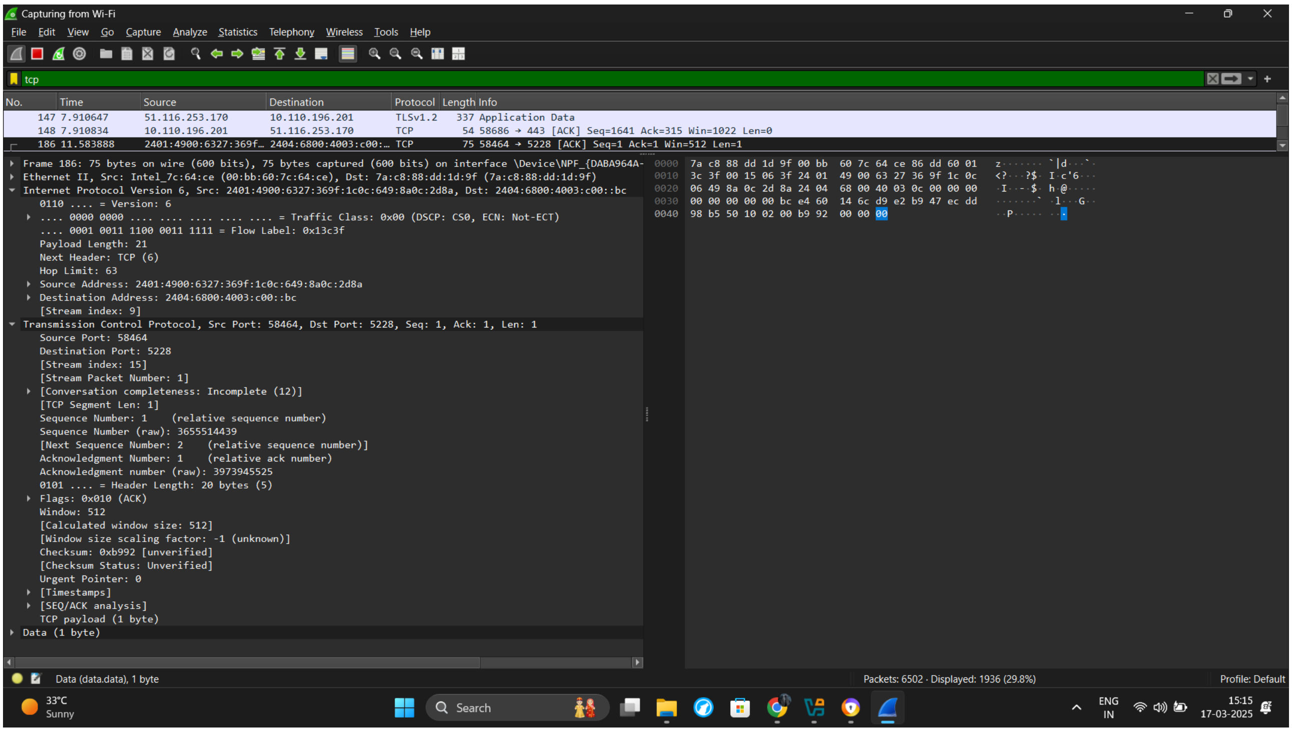
```
0000  00 bb 60 7c 64 ce 7a c8  88 dd 1d 9f 86 dd 6b 80   ··`|d·z· ······k·
0010  00 00 00 56 11 39 24 04  68 00 40 07 08 0c 00 00   ···V·9$· h·@·····
0020  00 00 00 00 20 0a 24 01  49 00 63 27 36 9f 1c 0c   ···· ·$· I·c'6···
0030  06 49 8a 0c 2d 8a 01 bb  e3 c0 00 56 48 5f 45 1f   ·I··-··· ···VH_E·
0040  9a d4 6d b9 be 18 64 03  b0 04 dc 5d c4 5c 2c 2a   ··m···d· ···]·\,*
0050  73 cd 77 6f fd 5d 76 2e  e8 51 1e 78 0c 26 46 a2   s·wo·]v. ·Q·x·&F·
0060  73 5c 2b a1 d4 cf 1a e3  20 2c e9 37 84 c3 47 75   s\+····· ,·7··Gu
0070  4b 92 04 22 58 4a 45 41  ce c5 ff 98 f6 c5 ee 10   K··"XJEA ········
0080  a3 cb e2 0f f9 cd 0c 4d  b2 82 14 47               ·······M ···G
```

Data (data.data), 78 bytes

Packets: 5951 · Displayed: 3946 (66.3%)

Profile: Default

# TCP Traffic


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
33°C
Sunny
Search
ENG
IN
15:15
17-03-2025

tcp

```
No.   Time       Source                  Destination             Protocol Length Info
  147 7.910647   51.116.253.170          10.110.196.201          TLSv1.2  337 Application Data
  148 7.910834   10.110.196.201          51.116.253.170          TCP       54 58686 → 443 [ACK] Seq=1641 Ack=315 Win=1022 Len=0
  186 11.583888  2401:4900:6327:369f…  2404:6800:4003:c00:…  TCP       75 58464 → 5228 [ACK] Seq=1 Ack=1 Win=512 Len=1
```

```
Frame 186: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{DABA964A-
Ethernet II, Src: Intel_7c:64:ce (00:bb:60:7c:64:ce), Dst: 7a:c8:88:dd:1d:9f (7a:c8:88:dd:1d:9f)
Internet Protocol Version 6, Src: 2401:4900:6327:369f:1c0c:649:8a0c:2d8a, Dst: 2404:6800:4003:c00::bc
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0001 0011 1100 0011 1111 = Flow Label: 0x13c3f
    Payload Length: 21
    Next Header: TCP (6)
    Hop Limit: 63
    Source Address: 2401:4900:6327:369f:1c0c:649:8a0c:2d8a
    Destination Address: 2404:6800:4003:c00::bc
    [Stream index: 9]
Transmission Control Protocol, Src Port: 58464, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
    Source Port: 58464
    Destination Port: 5228
    [Stream index: 15]
    [Stream Packet Number: 1]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 1]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3655514439
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3973945525
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 512
    [Calculated window size: 512]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xb992 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (1 byte)
Data (1 byte)
```

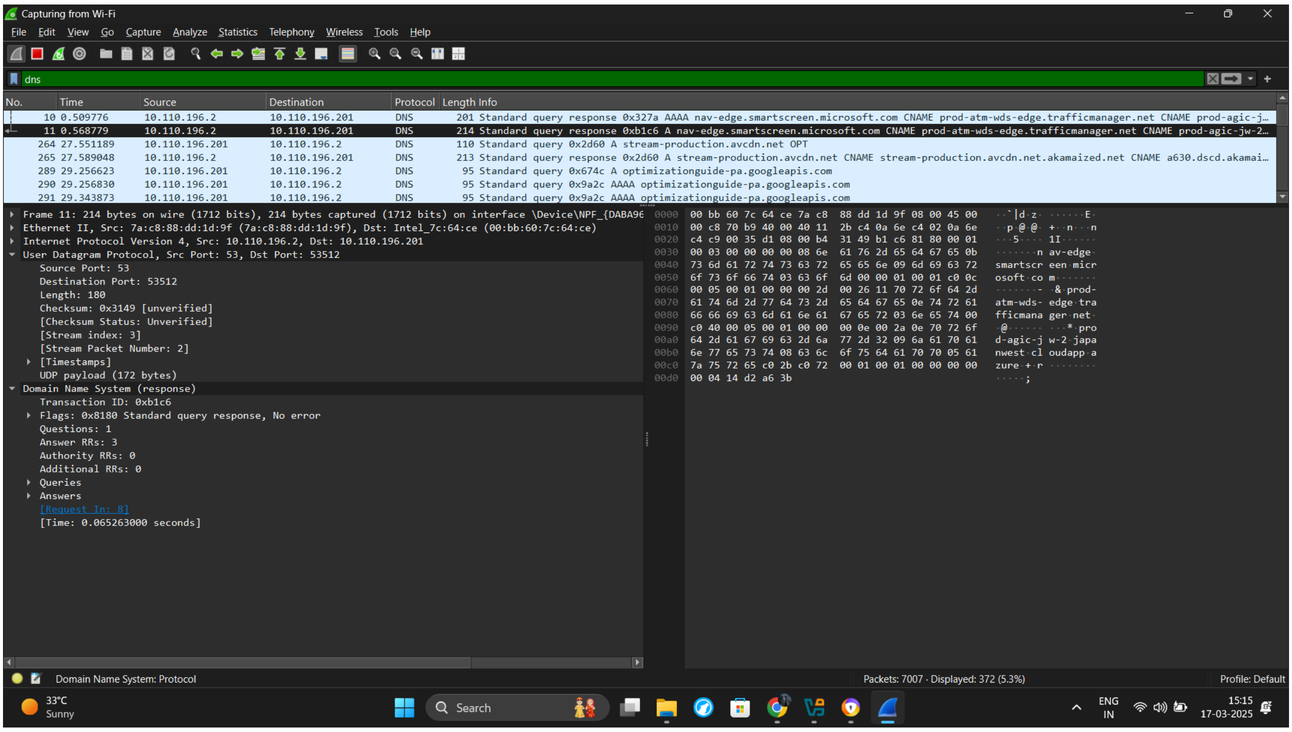
```
0000  7a c8 88 dd 1d 9f 00 bb  60 7c 64 ce 86 dd 60 01   z······· `|d···`·
0010  3c 3f 00 15 06 3f 24 01  49 00 63 27 36 9f 1c 0c   <?···?$· I·c'6···
0020  06 49 8a 0c 2d 8a 24 04  68 00 40 03 0c 00 00 00   ·I··-·$· h·@·····
0030  00 00 00 00 00 bc e4 60  14 6c d9 e2 b9 47 ec dd   ·······` ·l···G··
0040  98 b5 50 10 02 00 b9 92  00 00 00                  ··P····· ···
```

Data (data.data), 1 byte

Packets: 6502 · Displayed: 1936 (29.8%)

Profile: Default

# DNS Traffic


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

```
No.  Time        Source            Destination       Protocol Length Info
  10 0.509776    10.110.196.2      10.110.196.201    DNS      201 Standard query response 0x327a AAAA nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME prod-agic-j…
  11 0.568779    10.110.196.2      10.110.196.201    DNS      214 Standard query response 0xb1c6 A nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME prod-agic-jw-2…
 264 27.551189   10.110.196.201    10.110.196.2      DNS      110 Standard query 0x2d60 A stream-production.avcdn.net OPT
 265 27.589048   10.110.196.2      10.110.196.201    DNS      213 Standard query response 0x2d60 A stream-production.avcdn.net CNAME stream-production.avcdn.net.akamaized.net CNAME a630.dscd.akamai…
 289 29.256623   10.110.196.201    10.110.196.2      DNS       95 Standard query 0x674c A optimizationguide-pa.googleapis.com
 290 29.256830   10.110.196.201    10.110.196.2      DNS       95 Standard query 0x9a2c AAAA optimizationguide-pa.googleapis.com
 291 29.343873   10.110.196.201    10.110.196.2      DNS       95 Standard query 0x9a2c AAAA optimizationguide-pa.googleapis.com
```

```
> Frame 11: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface \Device\NPF_{DABA96
> Ethernet II, Src: 7a:c8:88:dd:1d:9f (7a:c8:88:dd:1d:9f), Dst: Intel_7c:64:ce (00:bb:60:7c:64:ce)
> Internet Protocol Version 4, Src: 10.110.196.2, Dst: 10.110.196.201
v User Datagram Protocol, Src Port: 53, Dst Port: 53512
      Source Port: 53
      Destination Port: 53512
      Length: 180
      Checksum: 0x3149 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 3]
      [Stream Packet Number: 2]
    > [Timestamps]
      UDP payload (172 bytes)
v Domain Name System (response)
      Transaction ID: 0xb1c6
    > Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 3
      Authority RRs: 0
      Additional RRs: 0
    > Queries
    > Answers
      [Request In: 8]
      [Time: 0.065263000 seconds]
```

```
0000  00 bb 60 7c 64 ce 7a c8  88 dd 1d 9f 08 00 45 00   ··`|d·z· ······E·
0010  00 c8 70 b9 40 00 40 11  2b c4 0a 6e c4 02 0a 6e   ··p·@·@· +··n···n
0020  c4 c9 00 35 d1 08 00 b4  31 49 b1 c6 81 80 00 01   ···5···· 1I······
0030  00 03 00 00 00 00 08 6e  61 76 2d 65 64 67 65 0b   ·······n av-edge·
0040  73 6d 61 72 74 73 63 72  65 65 6e 09 6d 69 63 72   smartscr een·micr
0050  6f 73 6f 66 74 03 63 6f  6d 00 00 01 00 01 c0 0c   osoft·co m·······
0060  00 05 00 01 00 00 00 2d  00 26 11 70 72 6f 64 2d   ·······- ·&·prod-
0070  61 74 6d 2d 77 64 73 2d  65 64 67 65 0e 74 72 61   atm-wds- edge·tra
0080  66 66 69 63 6d 61 6e 61  67 65 72 03 6e 65 74 00   fficmana ger·net·
0090  c0 40 00 05 00 01 00 00  00 0e 00 2a 0e 70 72 6f   ·@······ ···*·pro
00a0  64 2d 61 67 69 63 2d 6a  77 2d 32 09 6a 61 70 61   d-agic-j w-2·japa
00b0  6e 77 65 73 74 08 63 6c  6f 75 64 61 70 70 05 61   nwest·cl oudapp·a
00c0  7a 75 72 65 c0 2b c0 72  00 01 00 01 00 00 00 00   zure·+·r ········
00d0  00 04 14 d2 a6 3b                                  ·····;
```

Domain Name System: Protocol
Packets: 7007 · Displayed: 372 (5.3%)
Profile: Default
33°C
Sunny
Search
ENG
IN
15:15
17-03-2025