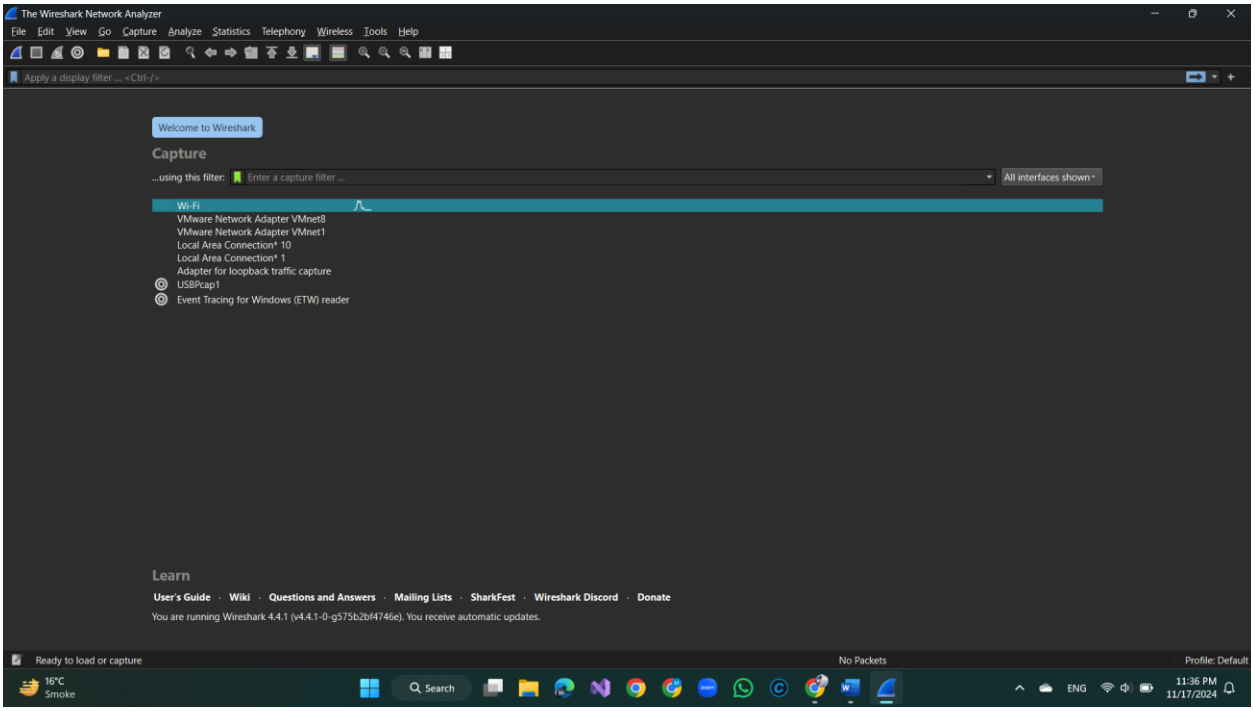
Task 3

Analyzing Network Traffic with Wireshark

In this task, I used **Wireshark** to capture and analyze network traffic, specifically focusing on TCP and UDP packets. Here are the steps I followed:

1: Launch Wireshark:

- ○ Opened the Wireshark application, which displayed available network interfaces such as Wi-Fi and local area connections.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Search
16°C
Smoke
ENG
11:36 PM
11/17/2024

Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 10
Local Area Connection* 1
Adapter for loopback traffic capture
USBPcap1
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.4.1 (v4.4.1-0-g575b2bf4746e). You receive automatic updates.

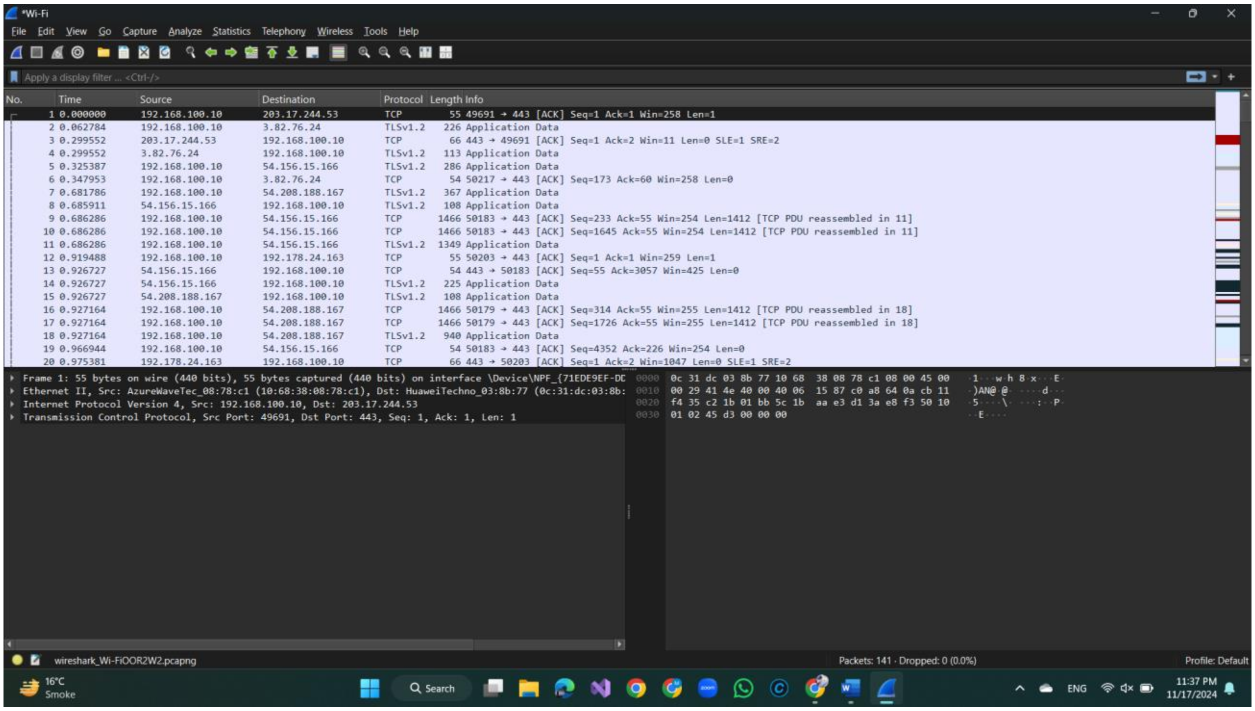
Ready to load or capture

No Packets

Profile: Default

2: Select Network Interface:

- Choose the **Wi-Fi** interface to start monitoring the wireless network traffic.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
16°C
Smoke
Search
ENG
11:37 PM
11/17/2024

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.100.10  203.17.244.53   TCP        55 49691 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1
   2 0.062784  192.168.100.10  3.82.76.24      TLSv1.2   226 Application Data
   3 0.299552  203.17.244.53   192.168.100.10  TCP        66 443 → 49691 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2
   4 0.299552  3.82.76.24      192.168.100.10  TLSv1.2   113 Application Data
   5 0.325387  192.168.100.10  54.156.15.166   TLSv1.2   286 Application Data
   6 0.347953  192.168.100.10  3.82.76.24      TCP        54 50217 → 443 [ACK] Seq=173 Ack=60 Win=258 Len=0
   7 0.681786  192.168.100.10  54.208.188.167  TLSv1.2   367 Application Data
   8 0.685911  54.156.15.166   192.168.100.10  TLSv1.2   108 Application Data
   9 0.686286  192.168.100.10  54.156.15.166   TCP      1466 50183 → 443 [ACK] Seq=233 Ack=55 Win=254 Len=1412 [TCP PDU reassembled in 11]
  10 0.686286  192.168.100.10  54.156.15.166   TCP      1466 50183 → 443 [ACK] Seq=1645 Ack=55 Win=254 Len=1412 [TCP PDU reassembled in 11]
  11 0.686286  192.168.100.10  54.156.15.166   TLSv1.2  1349 Application Data
  12 0.919488  192.168.100.10  192.178.24.163  TCP        55 50203 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1
  13 0.926727  54.156.15.166   192.168.100.10  TCP        54 443 → 50183 [ACK] Seq=55 Ack=3057 Win=425 Len=0
  14 0.926727  54.156.15.166   192.168.100.10  TLSv1.2   225 Application Data
  15 0.926727  54.208.188.167  192.168.100.10  TLSv1.2   108 Application Data
  16 0.927164  192.168.100.10  54.208.188.167  TCP      1466 50179 → 443 [ACK] Seq=314 Ack=55 Win=255 Len=1412 [TCP PDU reassembled in 18]
  17 0.927164  192.168.100.10  54.208.188.167  TCP      1466 50179 → 443 [ACK] Seq=1726 Ack=55 Win=255 Len=1412 [TCP PDU reassembled in 18]
  18 0.927164  192.168.100.10  54.208.188.167  TLSv1.2   940 Application Data
  19 0.966944  192.168.100.10  54.156.15.166   TCP        54 50183 → 443 [ACK] Seq=4352 Ack=226 Win=254 Len=0
  20 0.975381  192.178.24.163  192.168.100.10  TCP        66 443 → 50203 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
```

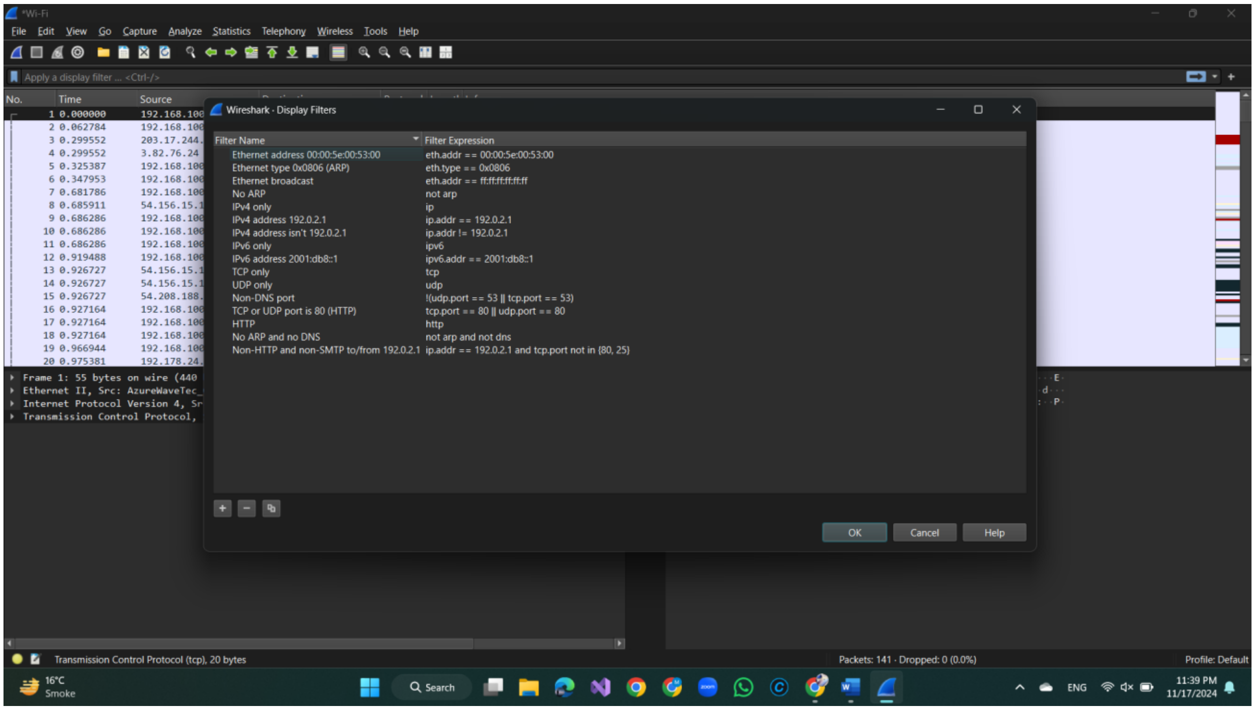
```
▸ Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{71EDE9EF-DC
▸ Ethernet II, Src: AzureWaveTec_08:78:c1 (10:68:38:08:78:c1), Dst: HuaweiTechno_03:8b:77 (0c:31:dc:03:8b:
▸ Internet Protocol Version 4, Src: 192.168.100.10, Dst: 203.17.244.53
▸ Transmission Control Protocol, Src Port: 49691, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

```
0000  0c 31 dc 03 8b 77 10 68  38 08 78 c1 08 00 45 00   ·1···w·h 8·x···E·
0010  00 29 41 4e 40 00 40 06  15 87 c0 a8 64 0a cb 11   ·)AN@·@· ····d···
0020  f4 35 c2 1b 01 bb 5c 1b  aa e3 d1 3a e8 f3 50 10   ·5····\· ···:··P·
0030  01 02 45 d3 00 00 00                               ··E····
```

wireshark_Wi-FiOOR2W2.pcapng   Packets: 141 · Dropped: 0 (0.0%)   Profile: Default

3: Capture Packets:

- Initiated the packet capture, allowing Wireshark to record all network traffic over the selected interface. I collected a total of **141 packets** for analysis.

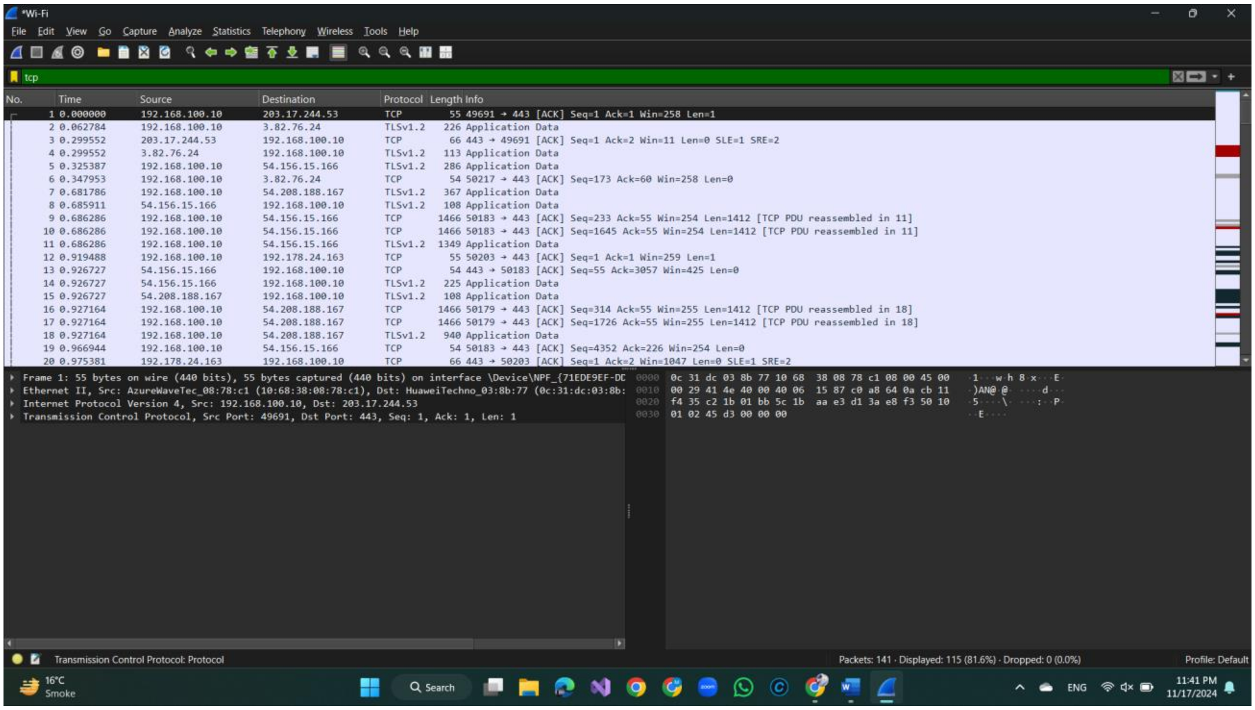

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Display Filters
+
−
OK
Cancel
Help
16°C
Smoke
Search
ENG
11:39 PM
11/17/2024

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1	ip.addr != 192.0.2.1
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS port	!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
HTTP	http
No ARP and no DNS	not arp and not dns
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and tcp.port not in {80, 25}

Transmission Control Protocol (tcp), 20 bytes   Packets: 141 · Dropped: 0 (0.0%)   Profile: Default

4: Apply Display Filters:

- From the **Analyze** option in the top menu, I accessed the **Display Filter** section, which showed various predefined filters.
- In the top search bar labeled "Apply a display filter," I typed **tcp** to filter and display all TCP-related packets.
- Similarly, I applied the **udp** filter, which displayed only UDP packets.

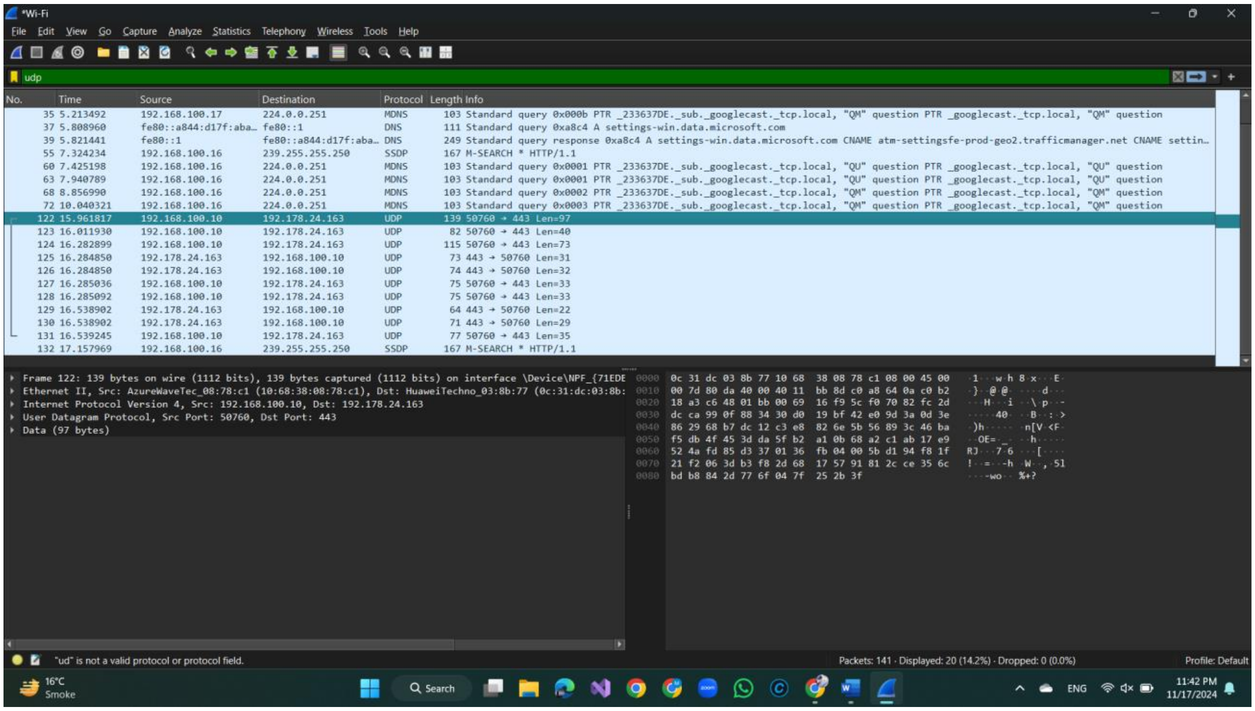

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time      Source           Destination      Protocol Length Info
    1 0.000000  192.168.100.10   203.17.244.53    TCP        55 49691 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1
    2 0.062784  192.168.100.10   3.82.76.24       TLSv1.2   226 Application Data
    3 0.299552  203.17.244.53    192.168.100.10   TCP        66 443 → 49691 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2
    4 0.299552  3.82.76.24       192.168.100.10   TLSv1.2   113 Application Data
    5 0.325387  192.168.100.10   54.156.15.166    TLSv1.2   286 Application Data
    6 0.347953  192.168.100.10   3.82.76.24       TCP        54 50217 → 443 [ACK] Seq=173 Ack=60 Win=258 Len=0
    7 0.681786  192.168.100.10   54.208.188.167   TLSv1.2   367 Application Data
    8 0.685911  54.156.15.166    192.168.100.10   TLSv1.2   108 Application Data
    9 0.686286  192.168.100.10   54.156.15.166    TCP      1466 50183 → 443 [ACK] Seq=233 Ack=55 Win=254 Len=1412 [TCP PDU reassembled in 11]
   10 0.686286  192.168.100.10   54.156.15.166    TCP      1466 50183 → 443 [ACK] Seq=1645 Ack=55 Win=254 Len=1412 [TCP PDU reassembled in 11]
   11 0.686286  192.168.100.10   54.156.15.166    TLSv1.2  1349 Application Data
   12 0.919488  192.168.100.10   192.178.24.163   TCP        55 50203 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1
   13 0.926727  54.156.15.166    192.168.100.10   TCP        54 443 → 50183 [ACK] Seq=55 Ack=3057 Win=425 Len=0
   14 0.926727  54.156.15.166    192.168.100.10   TLSv1.2   225 Application Data
   15 0.926727  54.208.188.167   192.168.100.10   TLSv1.2   108 Application Data
   16 0.927164  192.168.100.10   54.208.188.167   TCP      1466 50179 → 443 [ACK] Seq=314 Ack=55 Win=255 Len=1412 [TCP PDU reassembled in 18]
   17 0.927164  192.168.100.10   54.208.188.167   TCP      1466 50179 → 443 [ACK] Seq=1726 Ack=55 Win=255 Len=1412 [TCP PDU reassembled in 18]
   18 0.927164  192.168.100.10   54.208.188.167   TLSv1.2   940 Application Data
   19 0.966944  192.168.100.10   54.156.15.166    TCP        54 50183 → 443 [ACK] Seq=4352 Ack=226 Win=254 Len=0
   20 0.975381  192.178.24.163   192.168.100.10   TCP        66 443 → 50203 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
```

```
› Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{71EDE9EF-DC
› Ethernet II, Src: AzureWaveTec_08:78:c1 (10:68:38:08:78:c1), Dst: HuaweiTechno_03:8b:77 (0c:31:dc:03:8b:
› Internet Protocol Version 4, Src: 192.168.100.10, Dst: 203.17.244.53
› Transmission Control Protocol, Src Port: 49691, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

```
0000  0c 31 dc 03 8b 77 10 68  38 08 78 c1 08 00 45 00   ·1···w·h 8·x···E·
0010  00 29 41 4e 40 00 40 06  15 87 c0 a8 64 0a cb 11   ·)AN@·@· ····d···
0020  f4 35 c2 1b 01 bb 5c 1b  aa e3 d1 3a e8 f3 50 10   ·5····\· ···:··P·
0030  01 02 45 d3 00 00 00                               ··E····
```

Transmission Control Protocol: Protocol
Packets: 141 · Displayed: 115 (81.6%) · Dropped: 0 (0.0%)
Profile: Default
16°C
Smoke
Search
ENG
11:41 PM
11/17/2024


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

```
No.   Time       Source                 Destination            Protocol Length Info
   35 5.213492   192.168.100.17         224.0.0.251            MDNS     103 Standard query 0x000b PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
   37 5.808960   fe80::a844:d17f:aba…   fe80::1                DNS      111 Standard query 0xa8c4 A settings-win.data.microsoft.com
   39 5.821441   fe80::1                fe80::a844:d17f:aba…   DNS      249 Standard query response 0xa8c4 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settin…
   55 7.324234   192.168.100.16         239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
   60 7.425198   192.168.100.16         224.0.0.251            MDNS     103 Standard query 0x0001 PTR _233637DE._sub._googlecast._tcp.local, "QU" question PTR _googlecast._tcp.local, "QU" question
   63 7.940789   192.168.100.16         224.0.0.251            MDNS     103 Standard query 0x0001 PTR _233637DE._sub._googlecast._tcp.local, "QU" question PTR _googlecast._tcp.local, "QU" question
   68 8.856990   192.168.100.16         224.0.0.251            MDNS     103 Standard query 0x0002 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
   72 10.040321  192.168.100.16         224.0.0.251            MDNS     103 Standard query 0x0003 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  122 15.961817  192.168.100.10         192.178.24.163         UDP      139 50760 → 443 Len=97
  123 16.011930  192.168.100.10         192.178.24.163         UDP       82 50760 → 443 Len=40
  124 16.282899  192.168.100.10         192.178.24.163         UDP      115 50760 → 443 Len=73
  125 16.284850  192.178.24.163         192.168.100.10         UDP       73 443 → 50760 Len=31
  126 16.284850  192.178.24.163         192.168.100.10         UDP       74 443 → 50760 Len=32
  127 16.285036  192.168.100.10         192.178.24.163         UDP       75 50760 → 443 Len=33
  128 16.285092  192.168.100.10         192.178.24.163         UDP       75 50760 → 443 Len=33
  129 16.538902  192.178.24.163         192.168.100.10         UDP       64 443 → 50760 Len=22
  130 16.538902  192.178.24.163         192.168.100.10         UDP       71 443 → 50760 Len=29
  131 16.539245  192.168.100.10         192.178.24.163         UDP       77 50760 → 443 Len=35
  132 17.157969  192.168.100.16         239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
```

```
▸ Frame 122: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface \Device\NPF_{71EDE
▸ Ethernet II, Src: AzureWaveTec_08:78:c1 (10:68:38:08:78:c1), Dst: HuaweiTechno_03:8b:77 (0c:31:dc:03:8b:
▸ Internet Protocol Version 4, Src: 192.168.100.10, Dst: 192.178.24.163
▸ User Datagram Protocol, Src Port: 50760, Dst Port: 443
▸ Data (97 bytes)
```

```
0000  0c 31 dc 03 8b 77 10 68  38 08 78 c1 08 00 45 00   ·1···w·h 8·x···E·
0010  00 7d 80 da 40 00 40 11  bb 8d c0 a8 64 0a c0 b2   ·}··@·@· ····d···
0020  18 a3 c6 48 01 bb 00 69  16 f9 5c f0 70 82 fc 2d   ···H···i ··\·p··-
0030  dc ca 99 0f 88 34 30 d0  19 bf 42 e0 9d 3a 0d 3e   ·····40· ··B··:·>
0040  86 29 68 b7 dc 12 c3 e8  82 6e 5b 56 89 3c 46 ba   ·)h····· ·n[V·<F·
0050  f5 db 4f 45 3d da 5f b2  a1 0b 68 a2 c1 ab 17 e9   ··OE=·_· ··h·····
0060  52 4a fd 85 d3 37 01 36  fb 04 00 5b d1 94 f8 1f   RJ···7·6 ···[····
0070  21 f2 06 3d b3 f8 2d 68  17 57 91 81 2c ce 35 6c   !··=··-h ·W··,·5l
0080  bd b8 84 2d 77 6f 04 7f  25 2b 3f                  ···-wo·· %+?
```

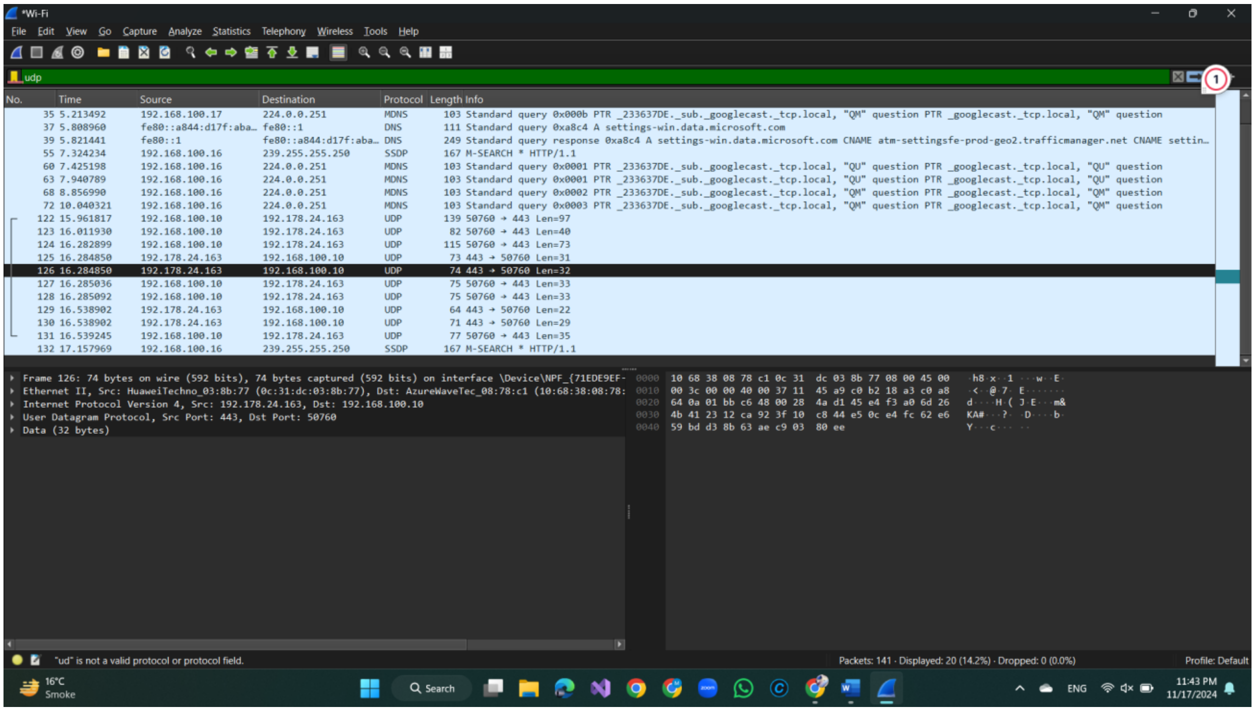
"ud" is not a valid protocol or protocol field.

Packets: 141 · Displayed: 20 (14.2%) · Dropped: 0 (0.0%)

Profile: Default

5: View I/O Graphs:

- Click on **Statistics** in the top menu and select **I/O Graphs** to view a graphical representation of network traffic. The graph displayed TCP traffic errors, allowing for further analysis.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
1

```
No.   Time       Source                 Destination            Protocol Length Info
   35 5.213492   192.168.100.17         224.0.0.251            MDNS     103 Standard query 0x000b PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
   37 5.808960   fe80::a844:d17f:aba…   fe80::1                DNS      111 Standard query 0xa8c4 A settings-win.data.microsoft.com
   39 5.821441   fe80::1                fe80::a844:d17f:aba…   DNS      249 Standard query response 0xa8c4 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settin…
   55 7.324234   192.168.100.16         239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
   60 7.425198   192.168.100.16         224.0.0.251            MDNS     103 Standard query 0x0001 PTR _233637DE._sub._googlecast._tcp.local, "QU" question PTR _googlecast._tcp.local, "QU" question
   63 7.940789   192.168.100.16         224.0.0.251            MDNS     103 Standard query 0x0001 PTR _233637DE._sub._googlecast._tcp.local, "QU" question PTR _googlecast._tcp.local, "QU" question
   68 8.856990   192.168.100.16         224.0.0.251            MDNS     103 Standard query 0x0002 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
   72 10.040321  192.168.100.16         224.0.0.251            MDNS     103 Standard query 0x0003 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  122 15.961817  192.168.100.10         192.178.24.163         UDP      139 50760 → 443 Len=97
  123 16.011930  192.168.100.10         192.178.24.163         UDP       82 50760 → 443 Len=40
  124 16.282899  192.168.100.10         192.178.24.163         UDP      115 50760 → 443 Len=73
  125 16.284850  192.178.24.163         192.168.100.10         UDP       73 443 → 50760 Len=31
  126 16.284850  192.178.24.163         192.168.100.10         UDP       74 443 → 50760 Len=32
  127 16.285036  192.168.100.10         192.178.24.163         UDP       75 50760 → 443 Len=33
  128 16.285092  192.168.100.10         192.178.24.163         UDP       75 50760 → 443 Len=33
  129 16.538902  192.178.24.163         192.168.100.10         UDP       64 443 → 50760 Len=22
  130 16.538902  192.178.24.163         192.168.100.10         UDP       71 443 → 50760 Len=29
  131 16.539245  192.168.100.10         192.178.24.163         UDP       77 50760 → 443 Len=35
  132 17.157969  192.168.100.16         239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
```

```
▸ Frame 126: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{71EDE9EF-
▸ Ethernet II, Src: HuaweiTechno_03:8b:77 (0c:31:dc:03:8b:77), Dst: AzureWaveTec_08:78:c1 (10:68:38:08:78:
▸ Internet Protocol Version 4, Src: 192.178.24.163, Dst: 192.168.100.10
▸ User Datagram Protocol, Src Port: 443, Dst Port: 50760
▸ Data (32 bytes)
```

```
0000  10 68 38 08 78 c1 0c 31  dc 03 8b 77 08 00 45 00   ·h8·x··1 ···w··E·
0010  00 3c 00 00 40 00 37 11  45 a9 c0 b2 18 a3 c0 a8   ·<··@·7· E·······
0020  64 0a 01 bb c6 48 00 28  4a d1 45 e4 f3 a0 6d 26   d····H·( J·E···m&
0030  4b 41 23 12 ca 92 3f 10  c8 44 e5 0c e4 fc 62 e6   KA#···?· ·D····b·
0040  59 bd d3 8b 63 ae c9 03  80 ee                     Y···c··· ··
```

"ud" is not a valid protocol or protocol field.

Packets: 141 · Displayed: 20 (14.2%) · Dropped: 0 (0.0%)

Profile: Default

6: Analysis of Packets:

i. **Initial Handshake (TCP, TLS, QUIC)**:

- Packets 1-3 show the **TCP three-way handshake** between the local machine and an external server, indicating the start of a communication session.

ii. **Encrypted Traffic**:

- Many packets (such as 10, 12, 14) involve **encrypted TLS data**.

iii. **QUIC Protocol**:

- Packets like 50-90 involve QUIC, a relatively new protocol running over UDP for faster and more secure web communications (used by platforms like Google).

iv. **Connection Resets and Alerts**:

- Packets like 21 and 22 show **RST, and ACK flags**, indicating connection resets. Reset flags can suggest issues with connections or intentional termination.

v. **DNS Queries**:

- Packets 43 and 44 show **DNS queries** from your local machine to the router, specifically querying the domain google.com.