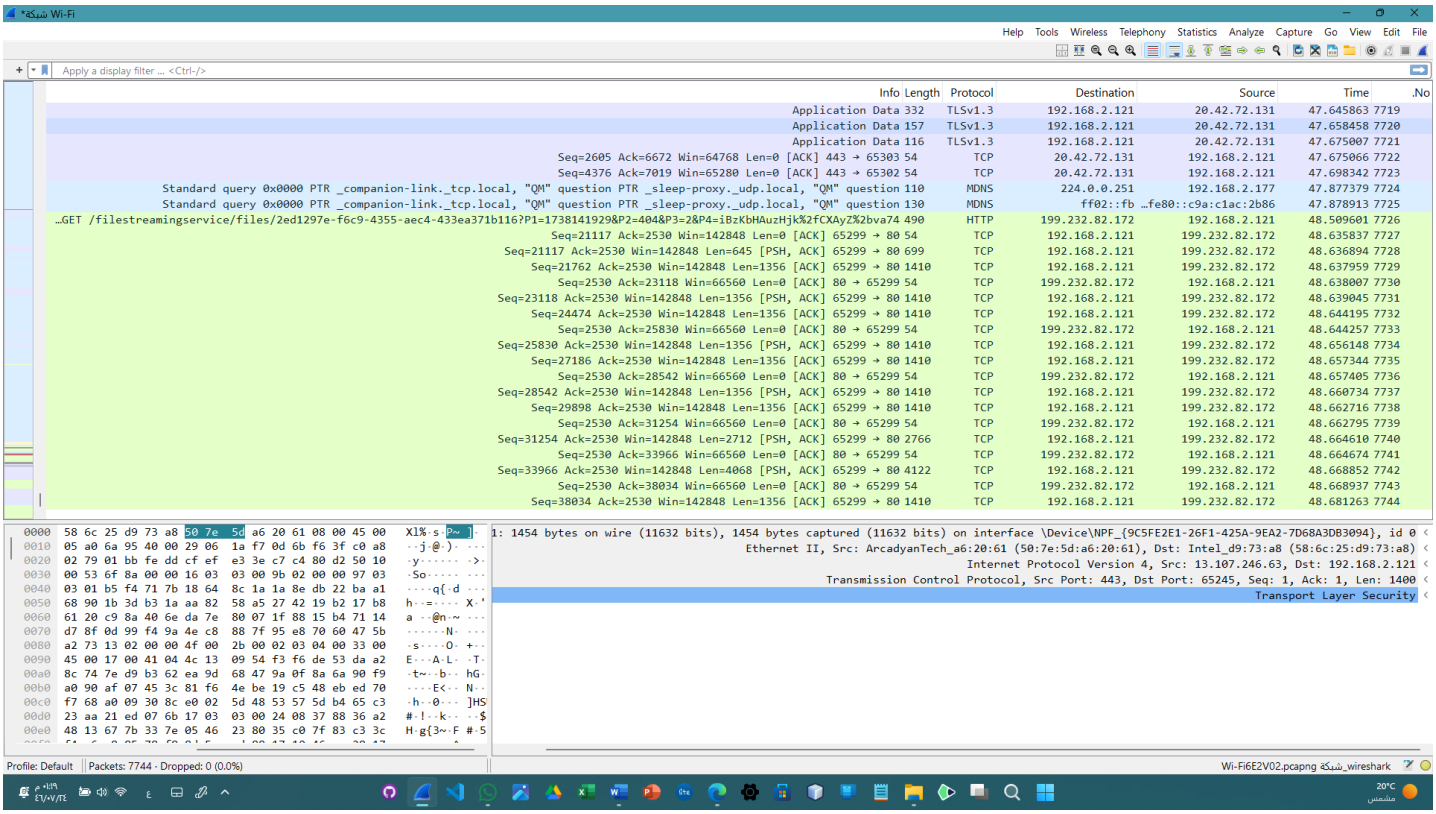
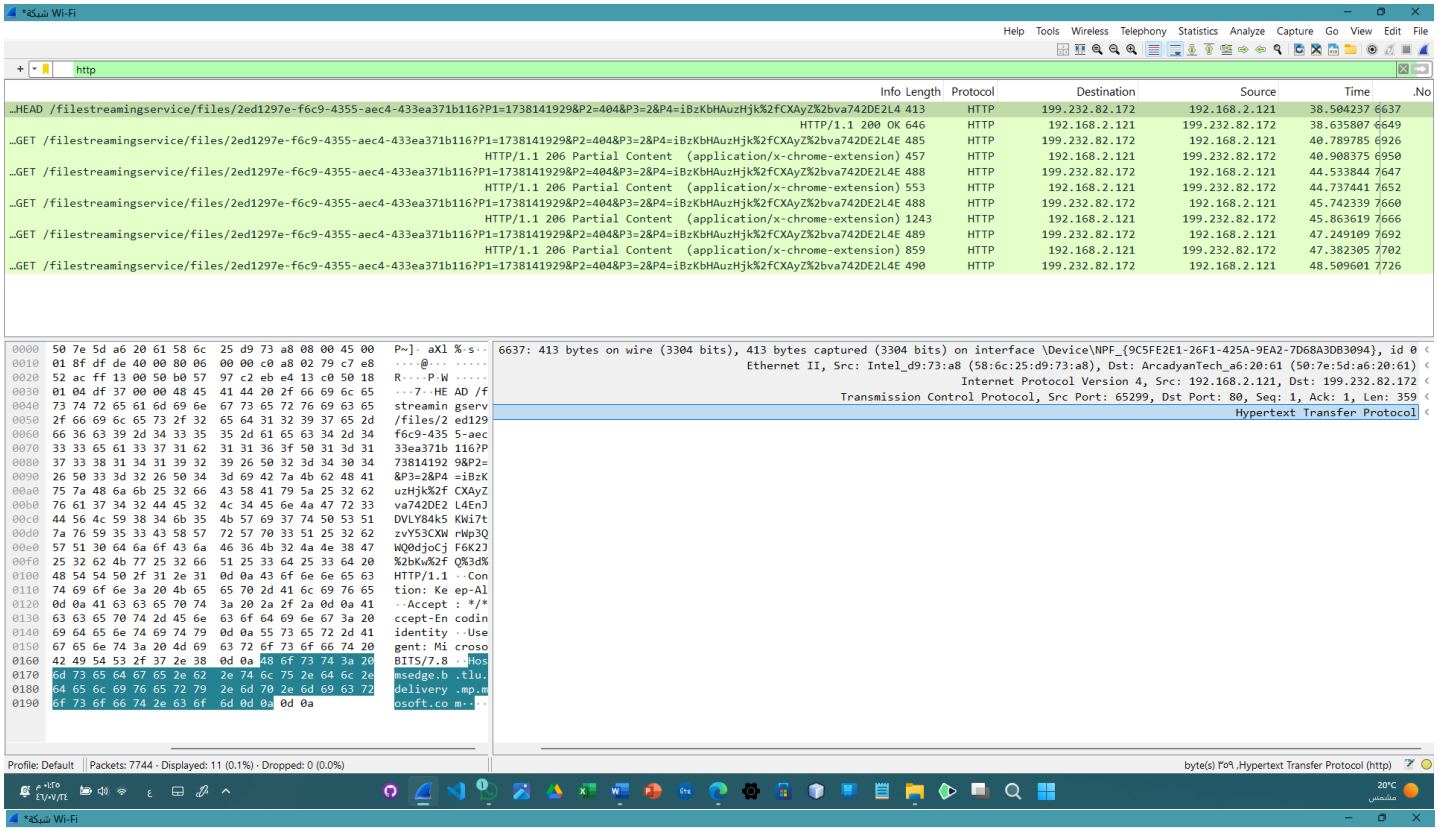
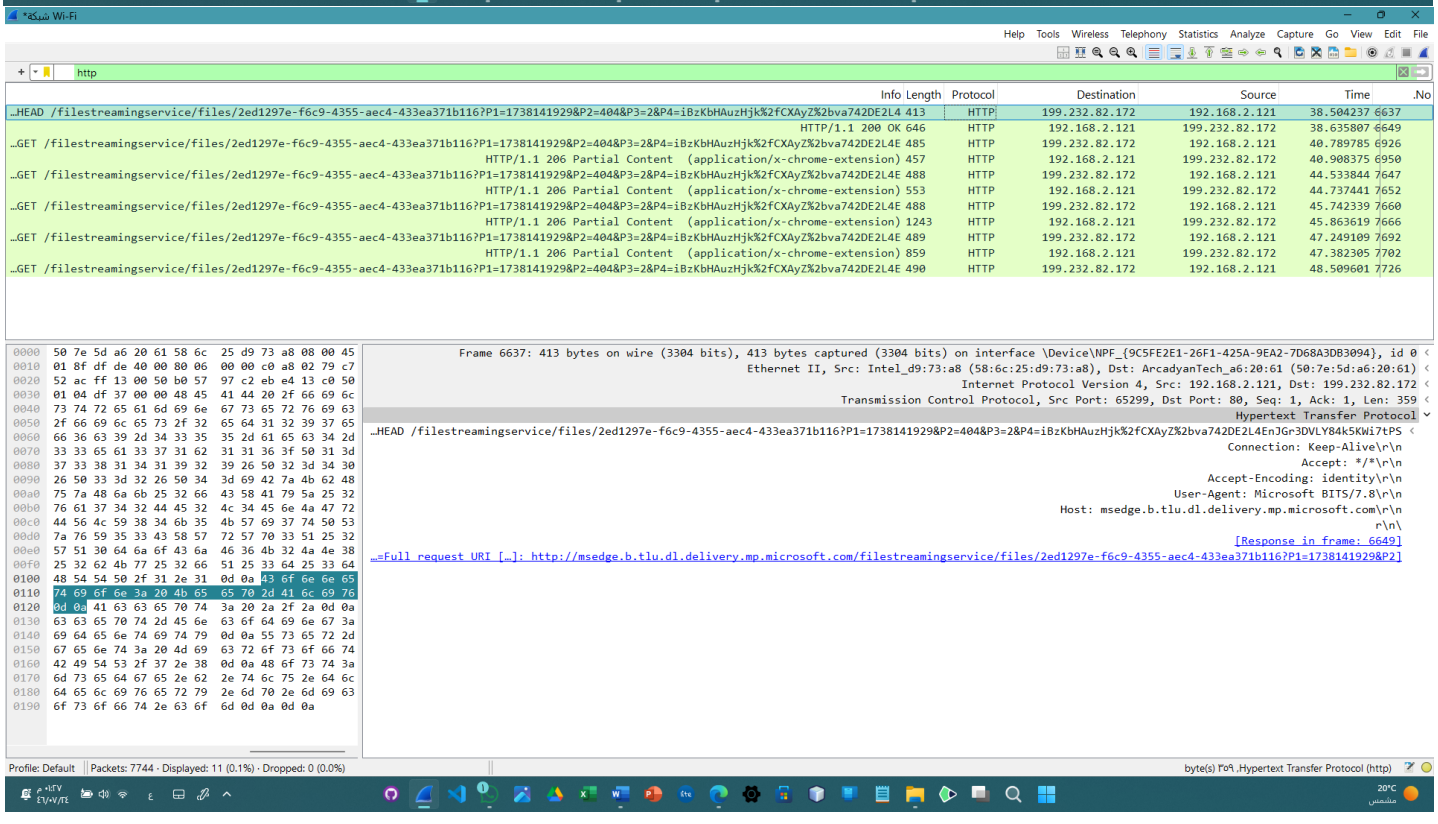
Part 1: Capturing HTTP Traffic.

Task 1: Start Wireshark and capture packets.



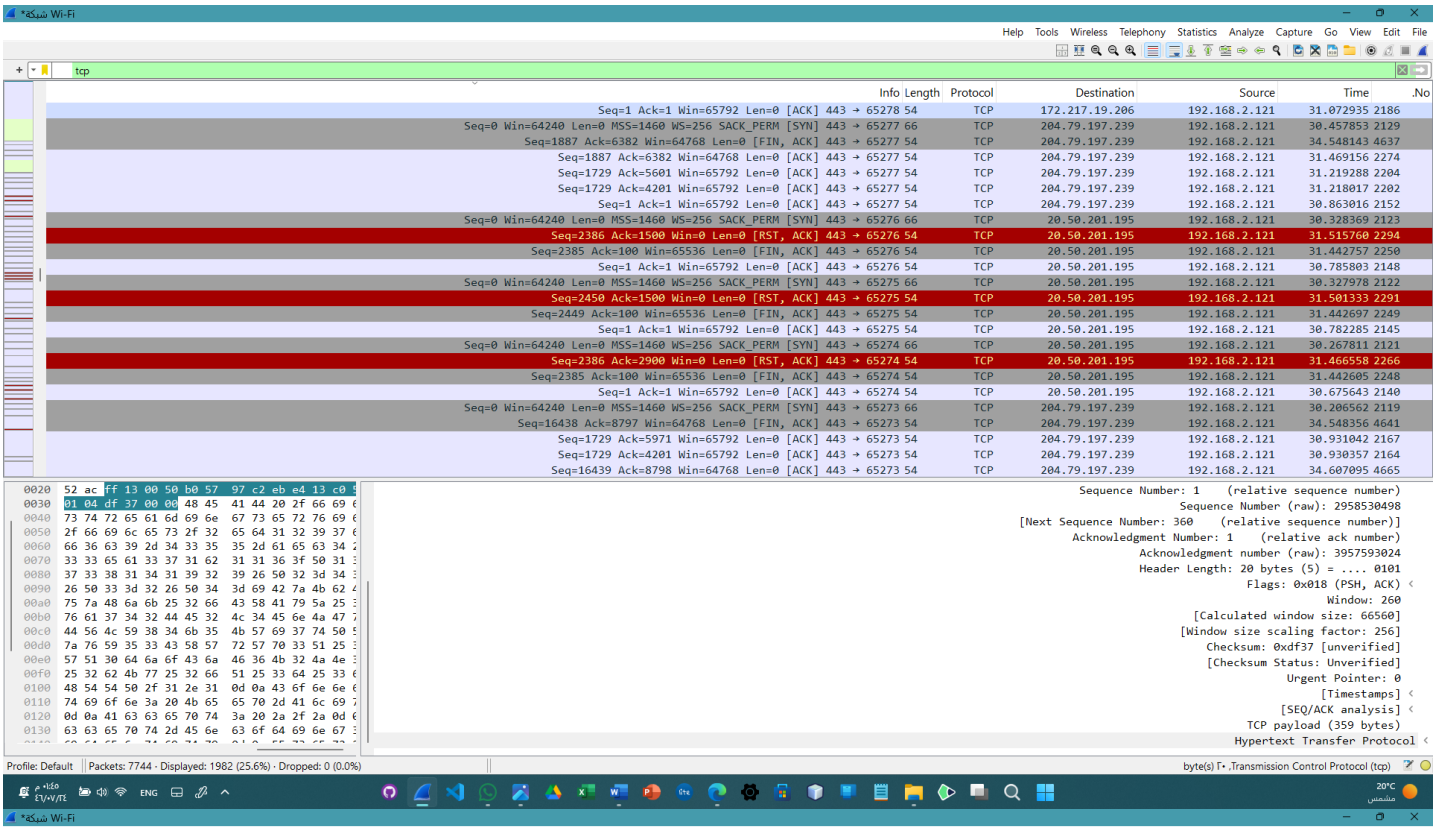
Task 2: Filter HTTP packets and analyze them.

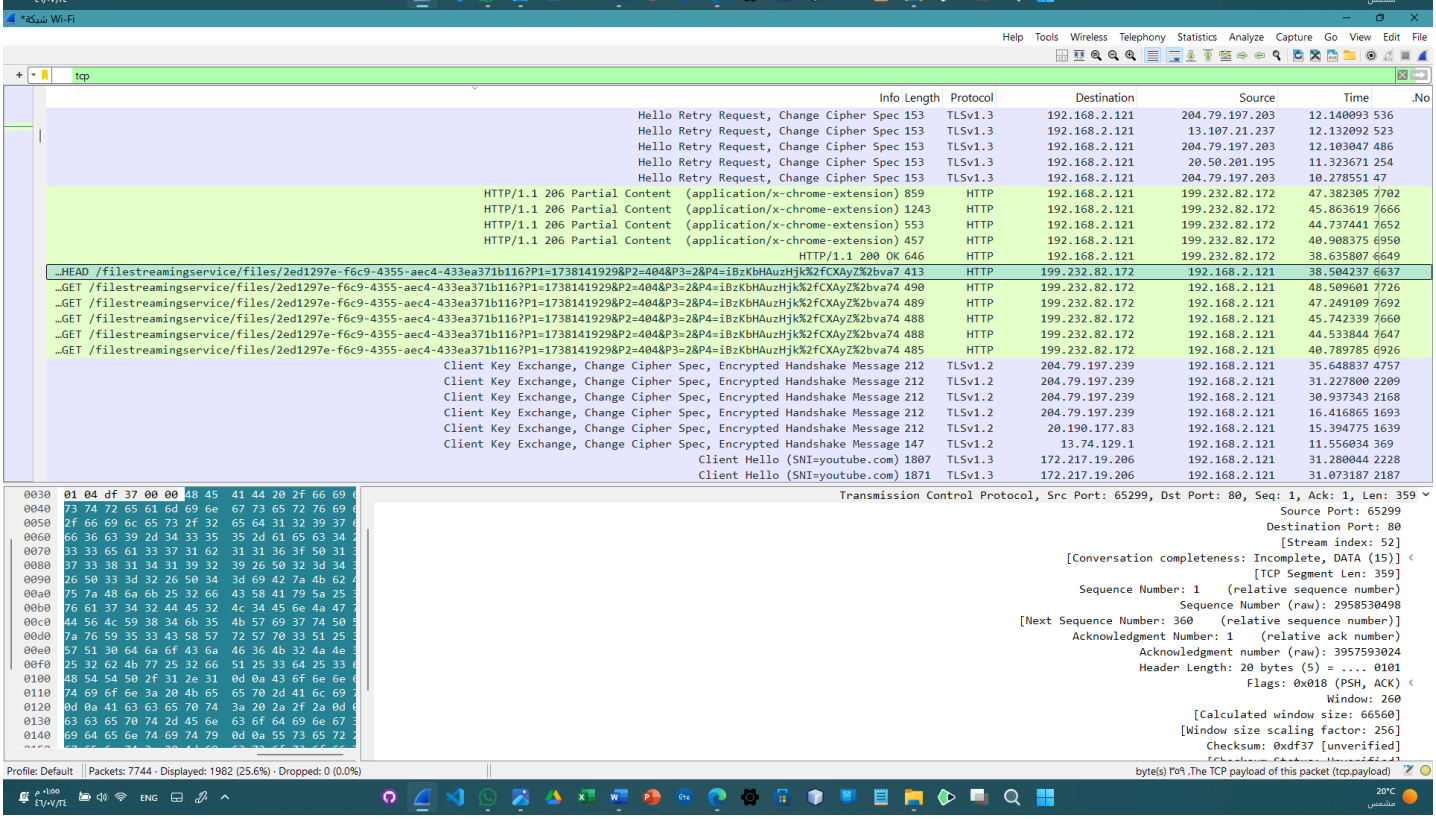


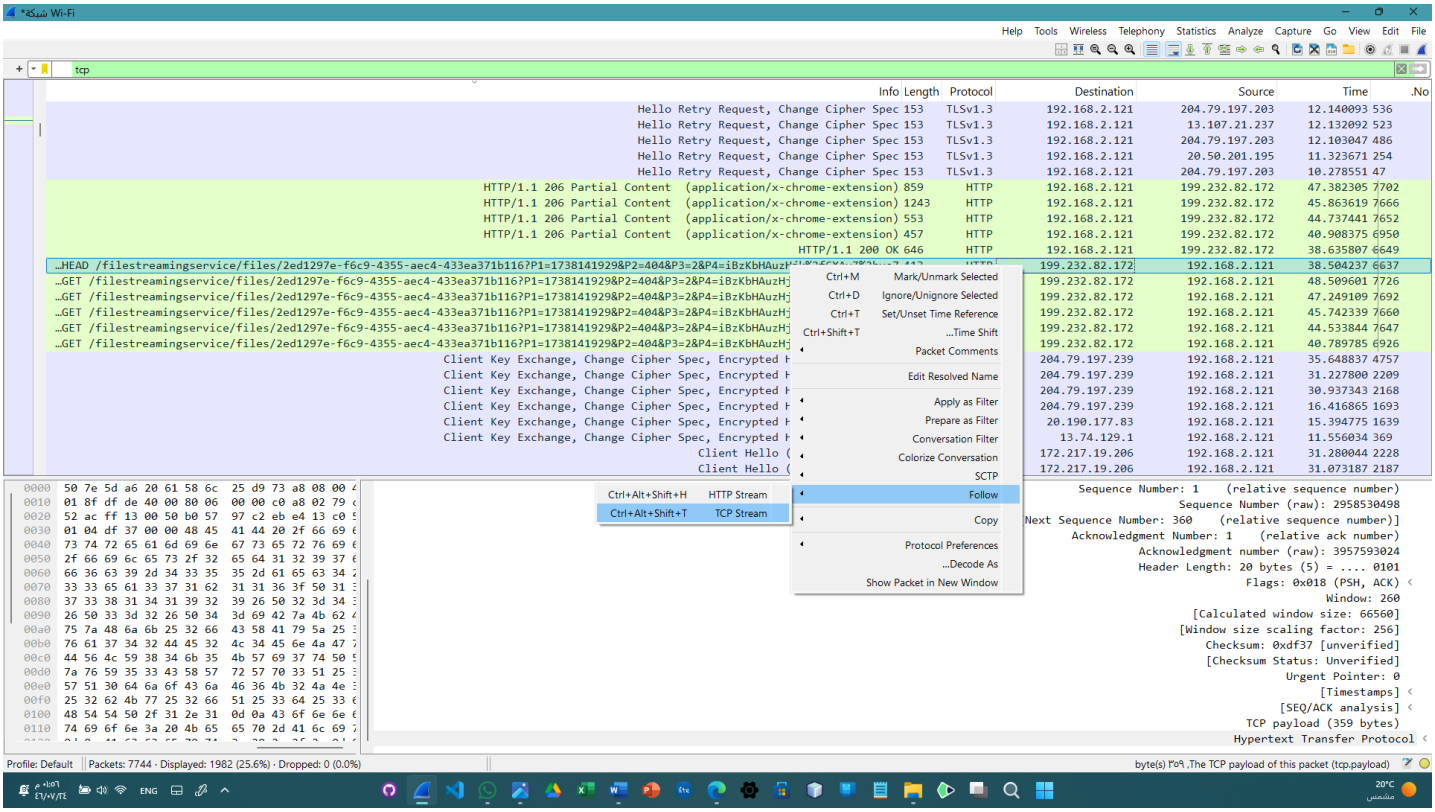


Part 2: Analyzing TCP/IP Traffic.

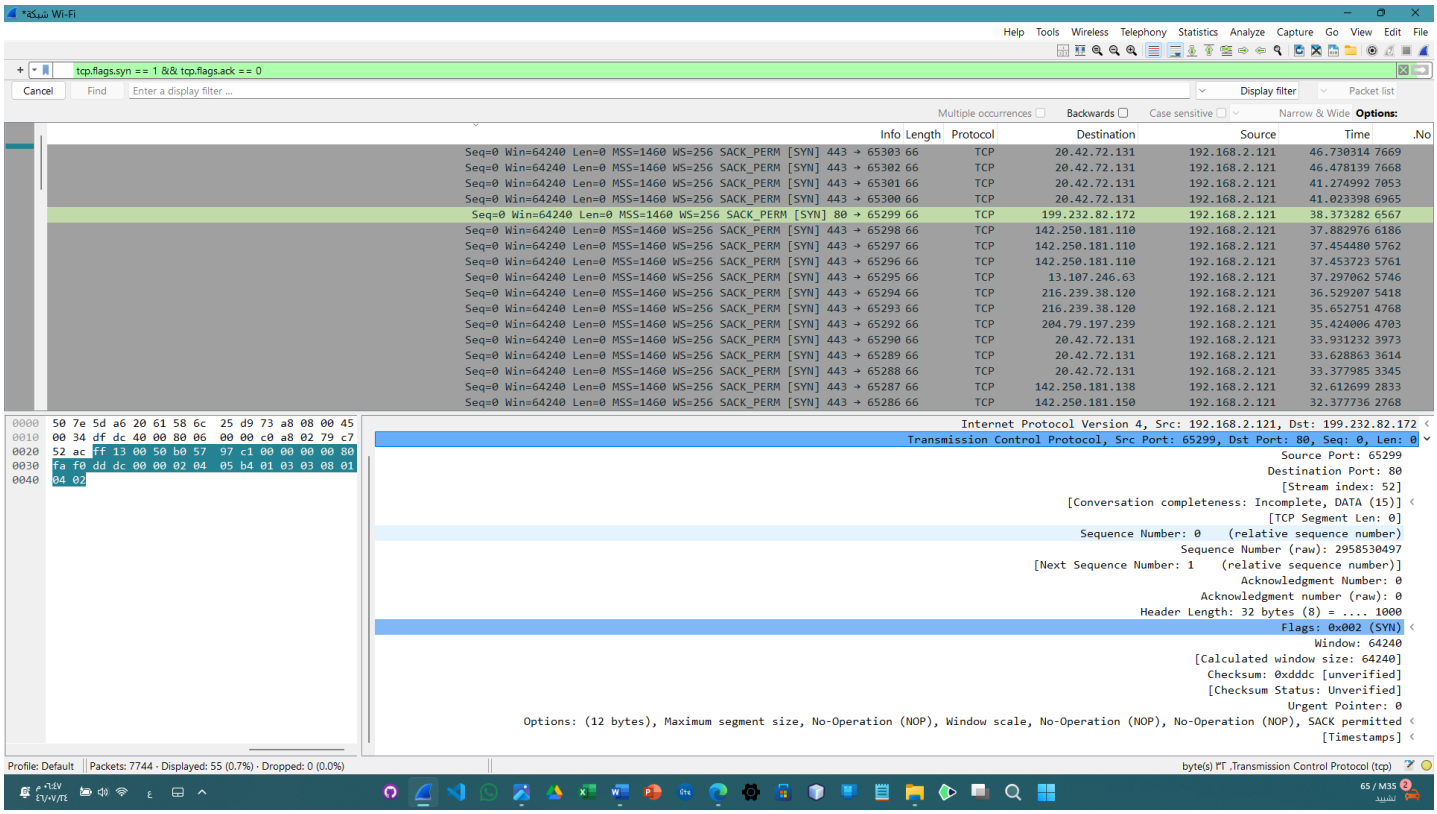
Task 1: Filter TCP packets

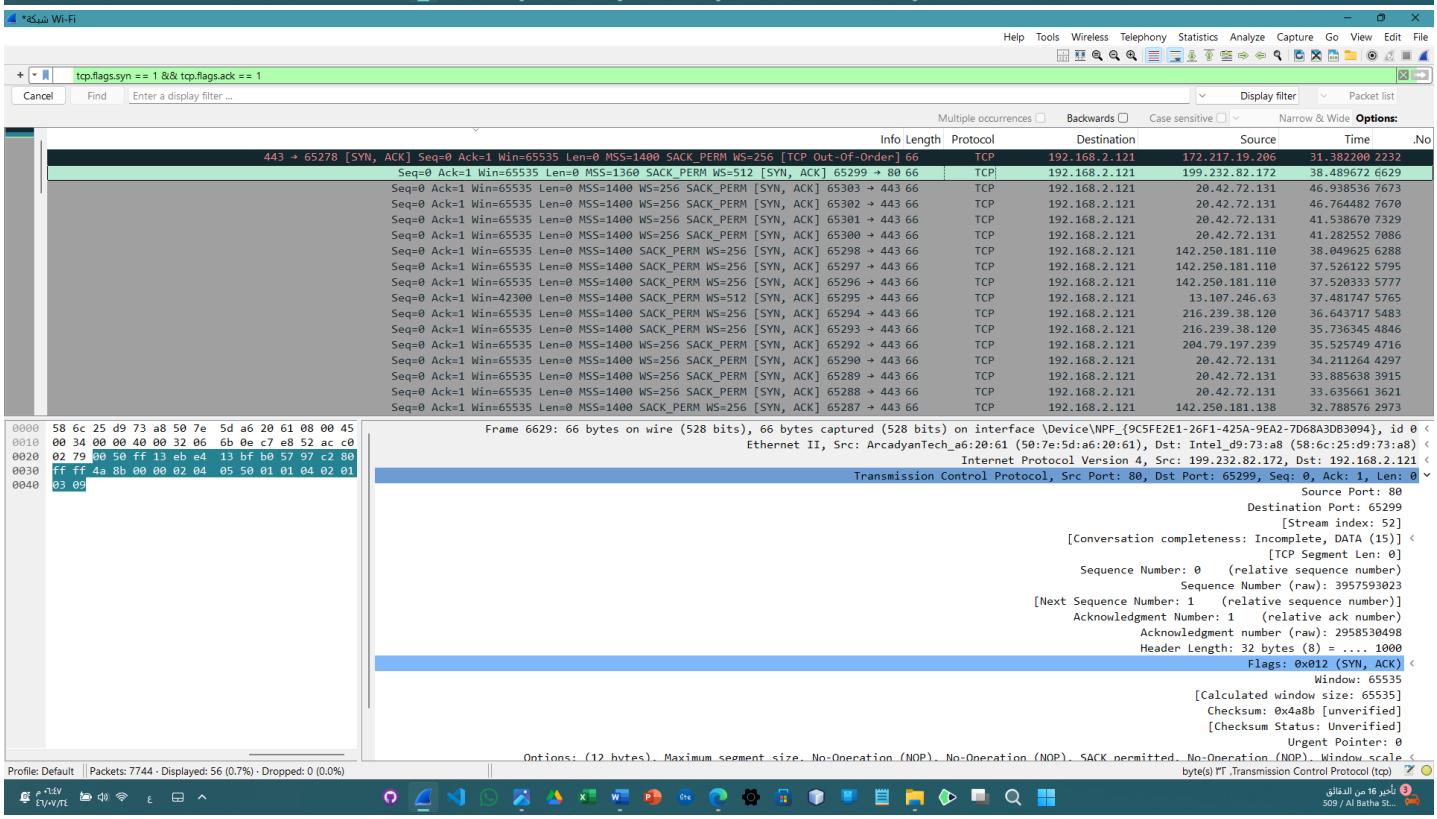


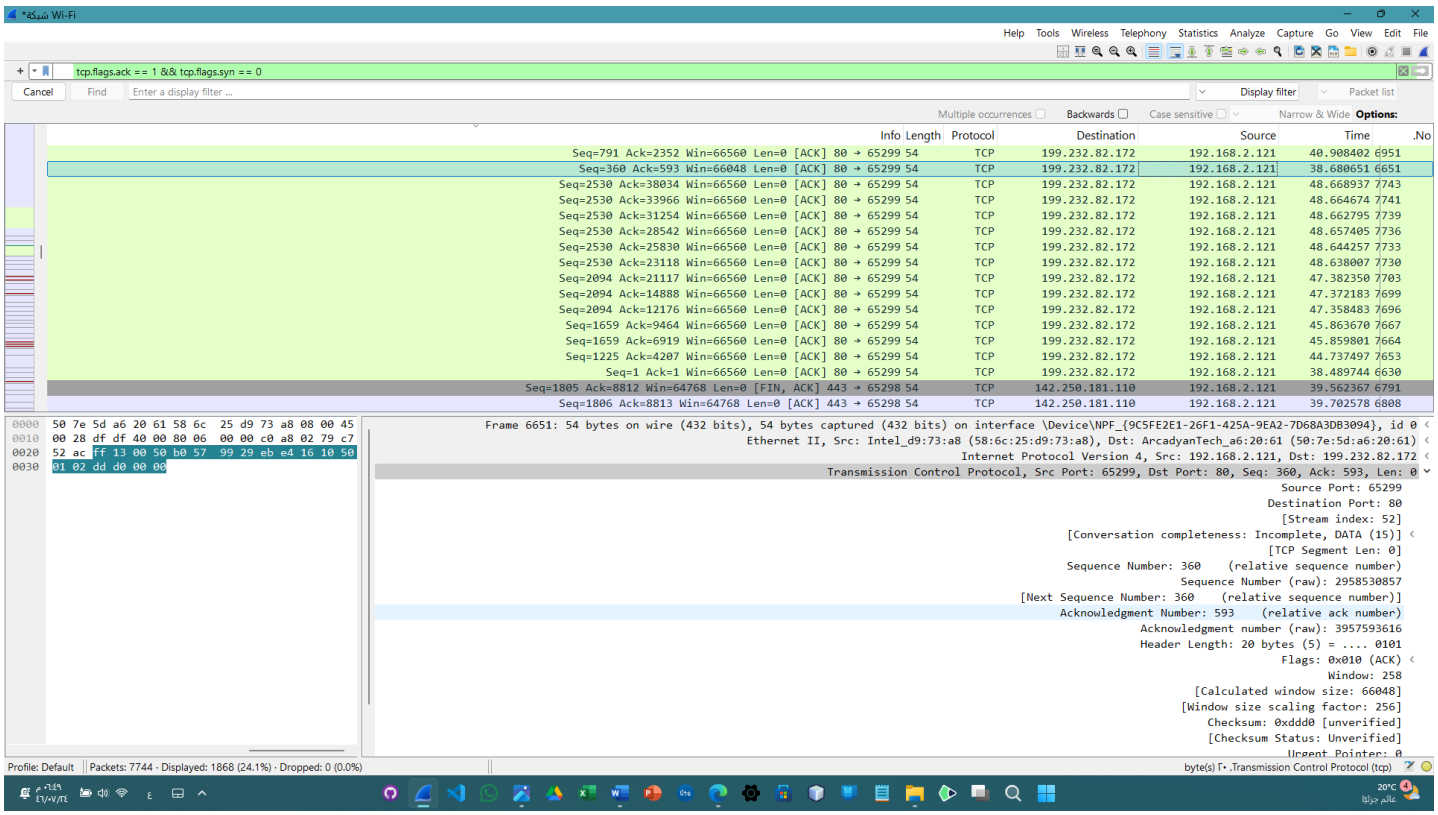



Wireshark · Follow TCP Stream (tcp.stream eq 52) · شبكة Wi-Fi
HEAD /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738141929&P2=404&P3=2&P4=iBzKbHAuzHjk%2fCXAyZ%2bva742DE2L4EnJGr3DVLY84k5KWi7tPSQzvY53CXWrWp3Q%2bWQ0djoCjF6K2JN8G%2bKw%2fQ%3d%3d HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.8
Host: msedge.b.tlu.dl.delivery.mp.microsoft.com
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 67802
Cache-Control: public, max-age=17280000
Content-Type: application/x-chrome-extension
Last-Modified: Mon, 09 Dec 2024 15:33:51 GMT
ETag: "vFma5hGP+crcpZiZfSnPaK02MWs="
MS-CorrelationId: a6d108e7-a319-427a-9c6a-38efc2ffeea2
MS-RequestId: 78d035e9-83df-428f-98a0-58e34bce1a45
MS-CV: CW+xBF1hCku//HUM.0
Accept-Ranges: bytes
Date: Fri, 24 Jan 2025 10:16:04 GMT
Via: 1.1 varnish
Age: 2096436
X-Served-By: cache-mrs10544-MRS
X-Cache: HIT
X-Cache-Hits: 11885013
X-Timer: S1737713765.709754,VS0,VE0
X-CID: 3
X-CCC: FR
GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738141929&P2=404&P3=2&P4=iBzKbHAuzHjk%2fCXAyZ%2bva742DE2L4EnJGr3DVLY84k5KWi7tPSQzvY53CXWrWp3Q%2bWQ0djoCjF6K2JN8G%2bKw%2fQ%3d%3d HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
If-Unmodified-Since: Mon, 09 Dec 2024 15:33:51 GMT
Range: bytes=0-1119
User-Agent: Microsoft BITS/7.8
Host: msedge.b.tlu.dl.delivery.mp.microsoft.com
HTTP/1.1 206 Partial Content
Connection: keep-alive
Content-Length: 1120
Find Next
Case sensitive
Find:
Back
Save as
Print
Filter Out This Stream

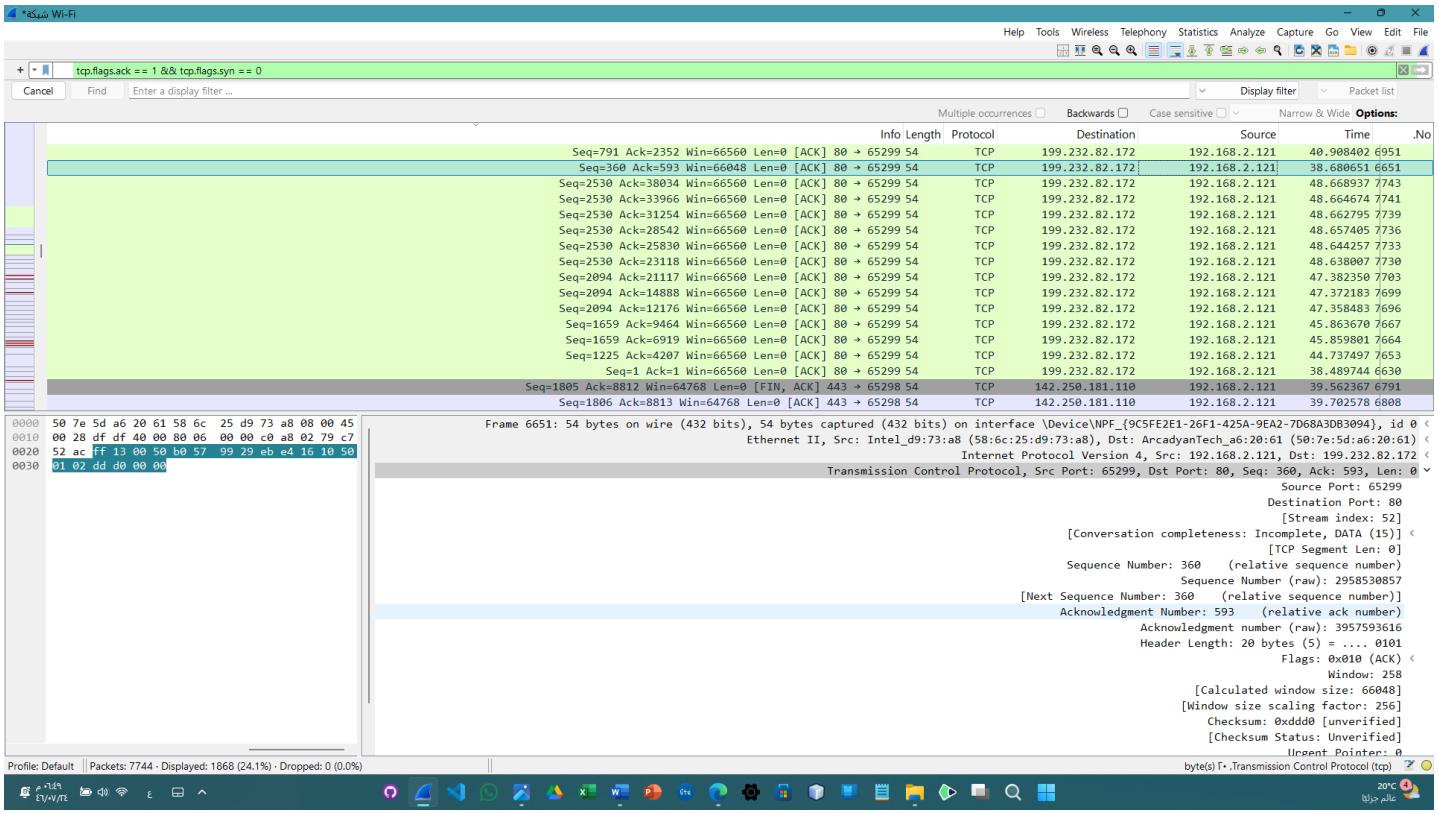
Task 2: Analyze TCP handshake and investigate Data Transfer and Termination



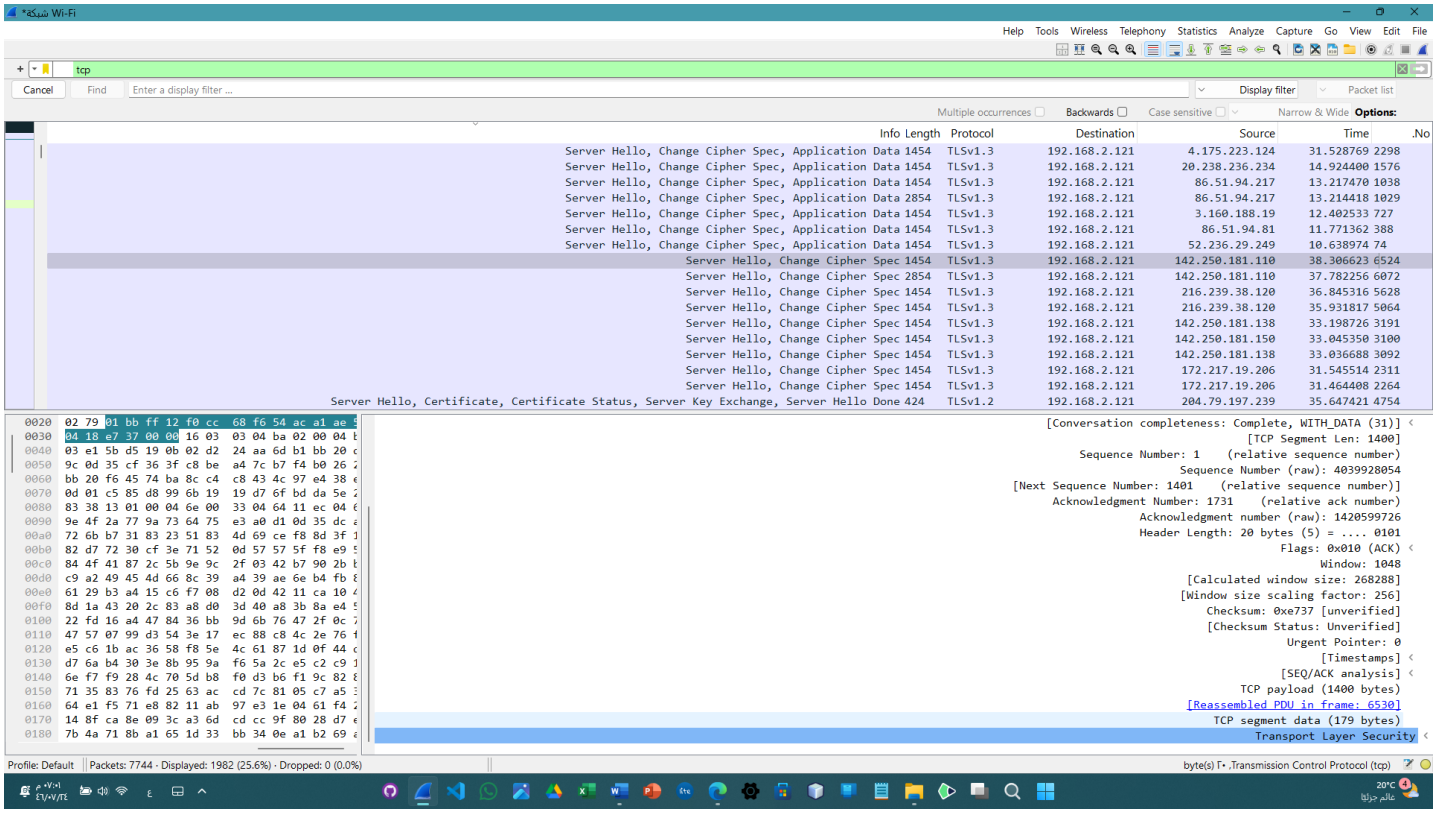



*شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
tcp.flags.ack == 1 && tcp.flags.syn == 0
Cancel Find Enter a display filter ... Display filter Packet list
Multiple occurrences Backwards Case sensitive Narrow & Wide Options:
Info Length Protocol Destination Source Time .No
Seq=791 Ack=2352 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 40.908402 6951
Seq=360 Ack=593 Win=66048 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 38.680651 6651
Seq=2530 Ack=38034 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.668937 7743
Seq=2530 Ack=33966 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.664674 7741
Seq=2530 Ack=31254 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.662795 7739
Seq=2530 Ack=28542 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.657405 7736
Seq=2530 Ack=25830 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.644257 7733
Seq=2530 Ack=23118 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.638007 7730
Seq=2094 Ack=21117 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 47.382350 7703
Seq=2094 Ack=14888 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 47.372183 7699
Seq=2094 Ack=12176 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 47.358483 7696
Seq=1659 Ack=9464 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 45.863670 7667
Seq=1659 Ack=6919 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 45.859801 7664
Seq=1225 Ack=4207 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 44.737497 7653
Seq=1 Ack=1 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 38.489744 6630
Seq=1805 Ack=8812 Win=64768 Len=0 [FIN, ACK] 443 → 65298 54 TCP 142.250.181.110 192.168.2.121 39.562367 6791
Seq=1806 Ack=8813 Win=64768 Len=0 [ACK] 443 → 65298 54 TCP 142.250.181.110 192.168.2.121 39.702578 6808
0000 50 7e 5d a6 20 61 58 6c 25 d9 73 a8 08 00 45
0010 00 28 df df 40 00 80 06 00 00 c0 a8 02 79 c7
0020 52 ac ff 13 00 50 b0 57 99 29 eb e4 16 10 50
0030 01 02 dd d0 00 00
Frame 6651: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9C5FE2E1-26F1-425A-9EA2-7D68A3DB3094}, id 0
Ethernet II, Src: Intel_d9:73:a8 (58:6c:25:d9:73:a8), Dst: ArcadyanTech_a6:20:61 (50:7e:5d:a6:20:61)
Internet Protocol Version 4, Src: 192.168.2.121, Dst: 199.232.82.172
Transmission Control Protocol, Src Port: 65299, Dst Port: 80, Seq: 360, Ack: 593, Len: 0
Source Port: 65299
Destination Port: 80
[Stream index: 52]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 360 (relative sequence number)
Sequence Number (raw): 2958530857
[Next Sequence Number: 360 (relative sequence number)]
Acknowledgment Number: 593 (relative ack number)
Acknowledgment number (raw): 3957593616
Header Length: 20 bytes (5) = ... 0101
Flags: 0x010 (ACK)
Window: 258
[Calculated window size: 66048]
[Window size scaling factor: 256]
Checksum: 0xddd0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Profile: Default
Packets: 7744 · Displayed: 1868 (24.1%) · Dropped: 0 (0.0%)
byte(s) Γ• ,Transmission Control Protocol (tcp)
20°C عالم جزئيا

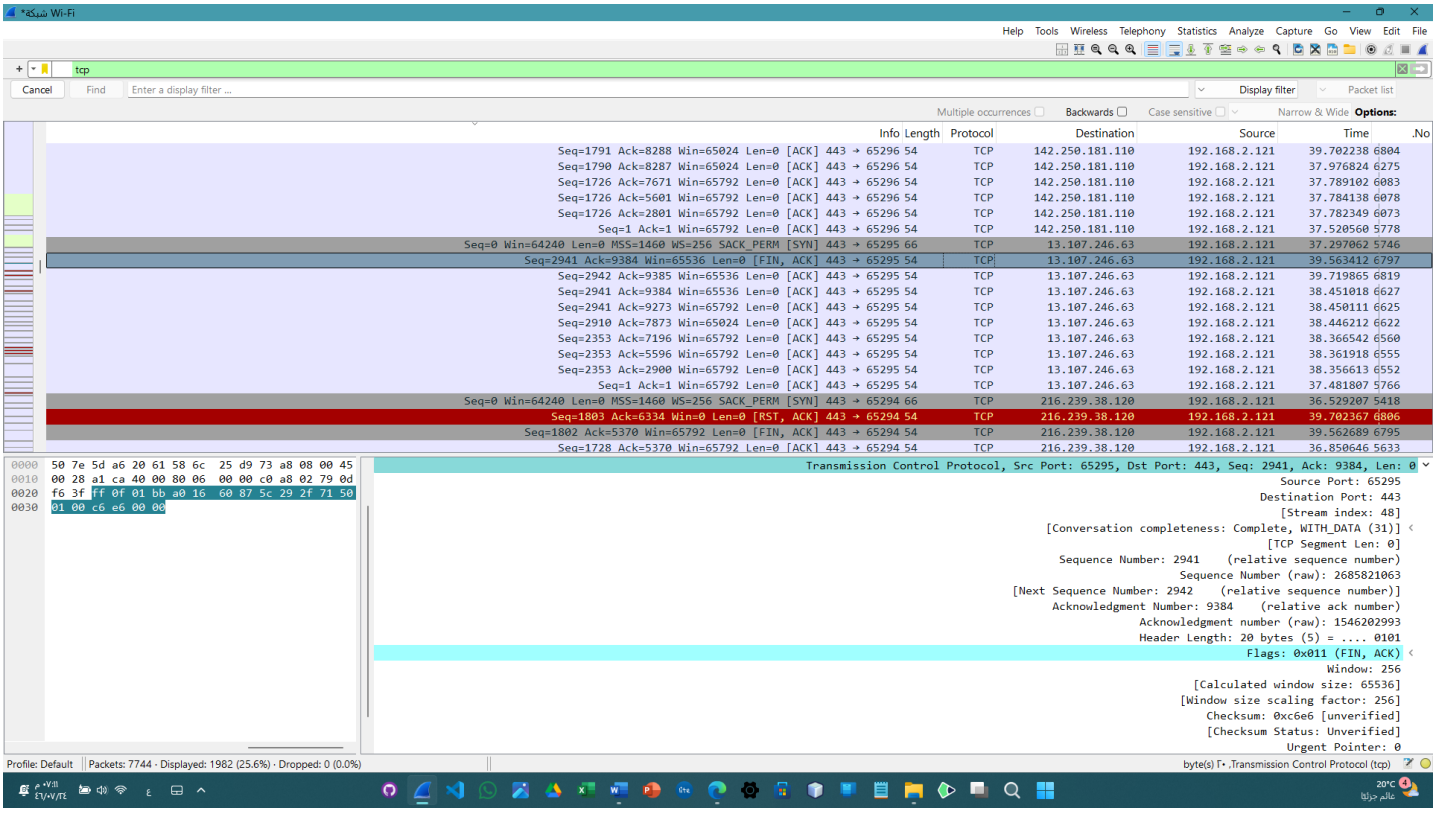
Step 2:


*شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
tcp.flags.ack == 1 && tcp.flags.syn == 0
Cancel Find Enter a display filter ... Display filter Packet list
Multiple occurrences Backwards Case sensitive Narrow & Wide Options:
Info Length Protocol Destination Source Time .No
Seq=791 Ack=2352 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 40.908402 6951
Seq=360 Ack=593 Win=66048 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 38.680651 6651
Seq=2530 Ack=38034 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.668937 7743
Seq=2530 Ack=33966 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.664674 7741
Seq=2530 Ack=31254 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.662795 7739
Seq=2530 Ack=28542 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.657405 7736
Seq=2530 Ack=25830 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.644257 7733
Seq=2530 Ack=23118 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 48.638007 7730
Seq=2094 Ack=21117 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 47.382350 7703
Seq=2094 Ack=14888 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 47.372183 7699
Seq=2094 Ack=12176 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 47.358483 7696
Seq=1659 Ack=9464 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 45.863670 7667
Seq=1659 Ack=6919 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 45.859801 7664
Seq=1225 Ack=4207 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 44.737497 7653
Seq=1 Ack=1 Win=66560 Len=0 [ACK] 80 → 65299 54 TCP 199.232.82.172 192.168.2.121 38.489744 6630
Seq=1805 Ack=8812 Win=64768 Len=0 [FIN, ACK] 443 → 65298 54 TCP 142.250.181.110 192.168.2.121 39.562367 6791
Seq=1806 Ack=8813 Win=64768 Len=0 [ACK] 443 → 65298 54 TCP 142.250.181.110 192.168.2.121 39.702578 6808
0000 50 7e 5d a6 20 61 58 6c 25 d9 73 a8 08 00 45
0010 00 28 df df 40 00 80 06 00 00 c0 a8 02 79 c7
0020 52 ac ff 13 00 50 b0 57 99 29 eb e4 16 10 50
0030 01 02 dd d0 00 00
Frame 6651: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9C5FE2E1-26F1-425A-9EA2-7D68A3DB3094}, id 0
Ethernet II, Src: Intel_d9:73:a8 (58:6c:25:d9:73:a8), Dst: ArcadyanTech_a6:20:61 (50:7e:5d:a6:20:61)
Internet Protocol Version 4, Src: 192.168.2.121, Dst: 199.232.82.172
Transmission Control Protocol, Src Port: 65299, Dst Port: 80, Seq: 360, Ack: 593, Len: 0
Source Port: 65299
Destination Port: 80
[Stream index: 52]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 360 (relative sequence number)
Sequence Number (raw): 2958530857
[Next Sequence Number: 360 (relative sequence number)]
Acknowledgment Number: 593 (relative ack number)
Acknowledgment number (raw): 3957593616
Header Length: 20 bytes (5) = ... 0101
Flags: 0x010 (ACK)
Window: 258
[Calculated window size: 66048]
[Window size scaling factor: 256]
Checksum: 0xddd0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Profile: Default
Packets: 7744 · Displayed: 1868 (24.1%) · Dropped: 0 (0.0%)
byte(s) Γ• ,Transmission Control Protocol (tcp)
20°C عالم جزئيا

Step 3:


*شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
tcp
Cancel Find Enter a display filter ... Display filter Packet list
Multiple occurrences Backwards Case sensitive Narrow & Wide Options:
Info Length Protocol Destination Source Time .No
Server Hello, Change Cipher Spec, Application Data 1454 TLSv1.3 192.168.2.121 4.175.223.124 31.528769 2298
Server Hello, Change Cipher Spec, Application Data 1454 TLSv1.3 192.168.2.121 20.238.236.234 14.924400 1576
Server Hello, Change Cipher Spec, Application Data 1454 TLSv1.3 192.168.2.121 86.51.94.217 13.217470 1038
Server Hello, Change Cipher Spec, Application Data 2854 TLSv1.3 192.168.2.121 86.51.94.217 13.214418 1029
Server Hello, Change Cipher Spec, Application Data 1454 TLSv1.3 192.168.2.121 3.160.188.19 12.402533 727
Server Hello, Change Cipher Spec, Application Data 1454 TLSv1.3 192.168.2.121 86.51.94.81 11.771362 388
Server Hello, Change Cipher Spec, Application Data 1454 TLSv1.3 192.168.2.121 52.236.29.249 10.638974 74
Server Hello, Change Cipher Spec 1454 TLSv1.3 192.168.2.121 142.250.181.110 38.306623 6524
Server Hello, Change Cipher Spec 2854 TLSv1.3 192.168.2.121 142.250.181.110 37.782256 6072
Server Hello, Change Cipher Spec 1454 TLSv1.3 192.168.2.121 216.239.38.120 36.845316 5628
Server Hello, Change Cipher Spec 1454 TLSv1.3 192.168.2.121 216.239.38.120 35.931817 5064
Server Hello, Change Cipher Spec 1454 TLSv1.3 192.168.2.121 142.250.181.138 33.198726 3191
Server Hello, Change Cipher Spec 1454 TLSv1.3 192.168.2.121 142.250.181.150 33.045350 3100
Server Hello, Change Cipher Spec 1454 TLSv1.3 192.168.2.121 142.250.181.138 33.036688 3092
Server Hello, Change Cipher Spec 1454 TLSv1.3 192.168.2.121 172.217.19.206 31.545514 2311
Server Hello, Change Cipher Spec 1454 TLSv1.3 192.168.2.121 172.217.19.206 31.464408 2264
Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done 424 TLSv1.2 192.168.2.121 204.79.197.239 35.647421 4754
0020 02 79 01 bb ff 12 f0 cc 68 f6 54 ac a1 ae
0030 04 18 e7 37 00 00 16 03 03 04 ba 02 00 04
0040 03 e1 5b d5 19 0b 02 d2 24 aa 6d b1 bb 20
0050 9c 0d 35 cf 36 3f c8 be a4 7c b7 f4 b0 26
0060 bb 20 f6 45 74 ba 8c c4 c8 43 4c 97 e4 38
0070 0d 01 c5 85 d8 99 6b 19 19 d7 6f bd da 5e
0080 83 38 13 01 00 04 6e 00 33 04 64 11 ec 04
0090 9e 4f 2a 77 9a 73 64 75 e3 a0 d1 0d 35 dc
00a0 72 6b b7 31 83 23 51 83 4d 69 ce f8 8d 3f
00b0 82 d7 72 30 cf 3e 71 52 0d 57 57 5f f8 e9
00c0 84 4f 41 87 2c 5b 9e 9c 2f 03 42 b7 90 2b
00d0 c9 a2 49 45 4d 66 8c 39 a4 39 ae 6e b4 fb
00e0 61 29 b3 a4 15 c6 f7 08 d2 0d 42 11 ca 10
00f0 8d 1a 43 20 2c 83 a8 d0 3d 40 a8 3b 8a e4
0100 22 fd 16 a4 47 84 36 bb 9d 6b 76 47 2f 0c
0110 47 57 07 99 d3 54 3e 17 ec 88 c8 4c 2e 76
0120 e5 c6 1b ac 36 58 f8 5e 4c 61 87 1d 0f 44
0130 d7 6a b4 30 3e 8b 95 9a f6 5a 2c e5 c2 c9
0140 6e f7 f9 28 4c 70 5d b8 f0 d3 b6 f1 9c 82
0150 71 35 83 76 fd 25 63 ac cd 7c 81 05 c7 a5
0160 64 e1 f5 71 e8 82 11 ab 97 e3 1e 04 61 f4
0170 14 8f ca 8e 09 3c a3 6d cd cc 9f 80 28 d7
0180 7b 4a 71 8b a1 65 1d 33 bb 34 0e a1 b2 69
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1400]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 4039928054
[Next Sequence Number: 1401 (relative sequence number)]
Acknowledgment Number: 1731 (relative ack number)
Acknowledgment number (raw): 1420599726
Header Length: 20 bytes (5) = ... 0101
Flags: 0x010 (ACK)
Window: 1048
[Calculated window size: 268288]
[Window size scaling factor: 256]
Checksum: 0xe737 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (1400 bytes)
[Reassembled PDU in frame: 6530]
TCP segment data (179 bytes)
Transport Layer Security
Profile: Default
Packets: 7744 · Displayed: 1982 (25.6%) · Dropped: 0 (0.0%)
byte(s) Γ• ,Transmission Control Protocol (tcp)

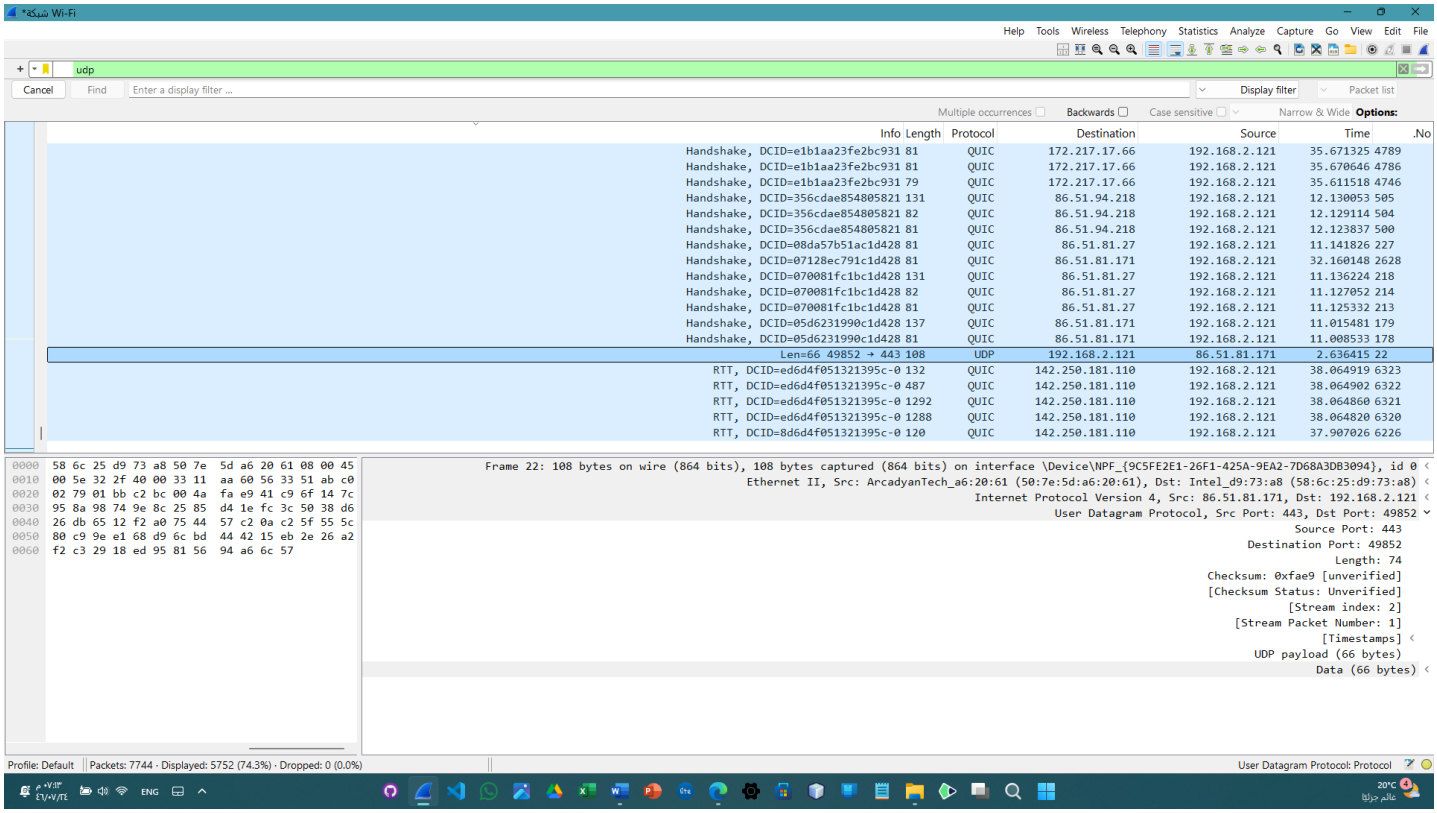
Step 4:


*شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
tcp
Cancel Find Enter a display filter ... Display filter Packet list
Multiple occurrences Backwards Case sensitive Narrow & Wide Options:
Info Length Protocol Destination Source Time .No
Seq=1791 Ack=8288 Win=65024 Len=0 [ACK] 443 → 65296 54 TCP 142.250.181.110 192.168.2.121 39.702238 6804
Seq=1790 Ack=8287 Win=65024 Len=0 [ACK] 443 → 65296 54 TCP 142.250.181.110 192.168.2.121 37.976824 6275
Seq=1726 Ack=7671 Win=65792 Len=0 [ACK] 443 → 65296 54 TCP 142.250.181.110 192.168.2.121 37.789102 6083
Seq=1726 Ack=5601 Win=65792 Len=0 [ACK] 443 → 65296 54 TCP 142.250.181.110 192.168.2.121 37.784138 6078
Seq=1726 Ack=2801 Win=65792 Len=0 [ACK] 443 → 65296 54 TCP 142.250.181.110 192.168.2.121 37.782349 6073
Seq=1 Ack=1 Win=65792 Len=0 [ACK] 443 → 65296 54 TCP 142.250.181.110 192.168.2.121 37.520560 5778
Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 443 → 65295 66 TCP 13.107.246.63 192.168.2.121 37.297062 5746
Seq=2941 Ack=9384 Win=65536 Len=0 [FIN, ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 39.563412 6797
Seq=2942 Ack=9385 Win=65536 Len=0 [ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 39.719865 6819
Seq=2941 Ack=9384 Win=65536 Len=0 [ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 38.451018 6627
Seq=2941 Ack=9273 Win=65792 Len=0 [ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 38.450111 6625
Seq=2910 Ack=7873 Win=65024 Len=0 [ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 38.446212 6622
Seq=2353 Ack=7196 Win=65792 Len=0 [ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 38.366542 6560
Seq=2353 Ack=5596 Win=65792 Len=0 [ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 38.361918 6555
Seq=2353 Ack=2900 Win=65792 Len=0 [ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 38.356613 6552
Seq=1 Ack=1 Win=65792 Len=0 [ACK] 443 → 65295 54 TCP 13.107.246.63 192.168.2.121 37.481807 5766
Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 443 → 65294 66 TCP 216.239.38.120 192.168.2.121 36.529207 5418
Seq=1803 Ack=6334 Win=0 Len=0 [RST, ACK] 443 → 65294 54 TCP 216.239.38.120 192.168.2.121 39.702367 6806
Seq=1802 Ack=5370 Win=65792 Len=0 [FIN, ACK] 443 → 65294 54 TCP 216.239.38.120 192.168.2.121 39.562689 6795
Seq=1728 Ack=5370 Win=65792 Len=0 [ACK] 443 → 65294 54 TCP 216.239.38.120 192.168.2.121 36.850646 5633
0000 50 7e 5d a6 20 61 58 6c 25 d9 73 a8 08 00 45
0010 00 28 a1 ca 40 00 80 06 00 00 c0 a8 02 79 0d
0020 f6 3f ff 0f 01 bb a0 16 60 87 5c 29 2f 71 50
0030 01 00 c6 e6 00 00
Transmission Control Protocol, Src Port: 65295, Dst Port: 443, Seq: 2941, Ack: 9384, Len: 0
Source Port: 65295
Destination Port: 443
[Stream index: 48]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 2941 (relative sequence number)
Sequence Number (raw): 2685821063
[Next Sequence Number: 2942 (relative sequence number)]
Acknowledgment Number: 9384 (relative ack number)
Acknowledgment number (raw): 1546202993
Header Length: 20 bytes (5) = ... 0101
Flags: 0x011 (FIN, ACK)
Window: 256
[Calculated window size: 65536]
[Window size scaling factor: 256]
Checksum: 0xc6e6 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Profile: Default
Packets: 7744 · Displayed: 1982 (25.6%) · Dropped: 0 (0.0%)
byte(s) Γ• ,Transmission Control Protocol (tcp)

Part 3: Capturing and Analyzing UDP Traffic

Task 1: Generate UDP traffic and capture packets

Task 2: Filter and analysis UDP Packets



Step 5: Compare the simplicity of UDP headers with TCP headers.

UDP headers are simpler:

and require less processing overhead, making UDP faster and more efficient for lightweight communication.

TCP headers are more complex:

because they include additional mechanisms to ensure reliability and proper data transmission.

Part 4:

Task 1: Fill in the following table and provide reasons.

	TCP or UDP	Reasons
Reliability and Connection Establishment	○ **TCP** relies on establishing a reliable connection before starting data transmission. ○ **TCP** is reliable .	○ It performs a **Three-Way Handshake** process between the client and the server to establish the connection. This ensures a stable and secure communication path for data transfer. ○ because it ensures data integrity, proper sequencing, and delivery, making it ideal for applications that cannot tolerate data loss, such as email or file downloads.
	○ **UDP** does not establish a prior connection between the two parties ○ **UDP** is less reliable	○ it sends data directly. This makes it simpler and faster than **TCP**. ○ it does not verify data reception or sequence, making it faster but suitable for applications that do not require complete accuracy, such as video streaming or voice calls.
Data Integrity and Ordering	○ **TCP:** Ensures data integrity and sequencing ○ **UDP:** Does not provide data integrity or sequencing	○ using sequence numbers, error-checking mechanisms, and retransmission of lost packets. ○ as it focuses on speed and simplicity, making it suitable for applications that can tolerate some packet loss.

Task 2: Identify the use Cases and Performance of TCP and UDP.

	TCP	UDP
Use cases	○ Web browsing. ○ File downloads. ○ Applications requiring reliable data transfer.	○ Streaming video and audio. ○ Voice over IP (VoIP). ○ Applications prioritizing speed over reliability.
Performance	Slower due to reliability and data ordering guarantees.	Faster as it does not rely on connection establishment or data verification.