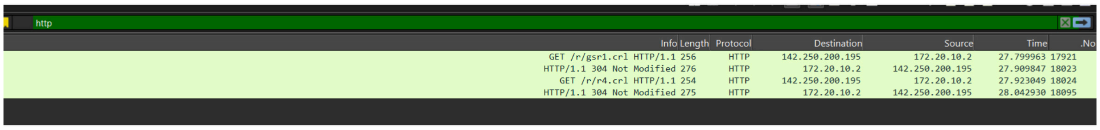
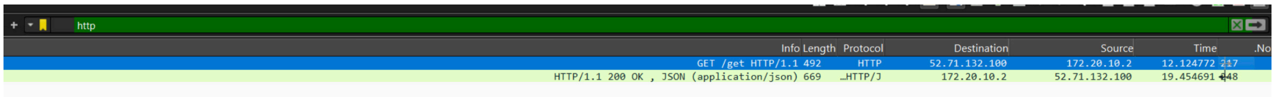
Dania Almethen
421215943

Lab Week 2

Task 2: Filter HTTP packets and analyze them.
Step 1: In the filter bar, type http and press Enter. This filters out only the HTTP packets from the capture.
Step 2: Select any HTTP packet to view its details.
Step 3: Observe the HTTP request and response messages. Note the method (GET, POST), URL, response codes (200 OK, 404 Not Found), etc.

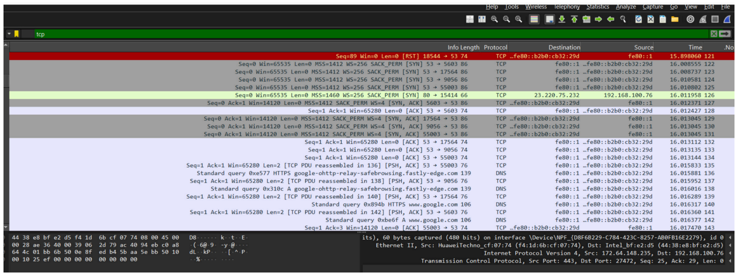


```
http
                                    Info Length  Protocol      Destination            Source        Time   .No
              GET /r/gsr1.crl HTTP/1.1 256     HTTP     142.250.200.195        172.20.10.2  27.799963 17921
         HTTP/1.1 304 Not Modified 276     HTTP         172.20.10.2    142.250.200.195  27.909847 18023
               GET /r/r4.crl HTTP/1.1 254     HTTP     142.250.200.195        172.20.10.2  27.923049 18024
         HTTP/1.1 304 Not Modified 275     HTTP         172.20.10.2    142.250.200.195  28.042930 18095
```



```
http
                                           Info Length  Protocol      Destination          Source        Time  .No
                              GET /get HTTP/1.1 492     HTTP     52.71.132.100     172.20.10.2   12.124772 217
    HTTP/1.1 200 OK , JSON (application/json) 669   …HTTP/J      172.20.10.2    52.71.132.100   19.454691 448
```

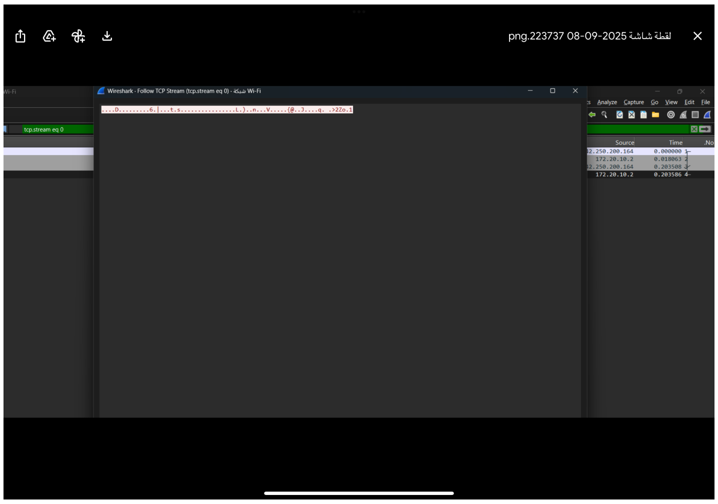
Task 1: Filter TCP packets



```
tcp
                                                                 Info Length  Protocol  Destination              Source                 Time        .No
                                Seq=89 Win=0 Len=0 [RST] 18544 → 53 74      TCP  …fe80::b2b0:cb32:29d       fe80::1              15.898060 121
   Seq=0 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM [SYN] 53 → 5603 86       TCP         fe80::1  …fe80::b2b0:cb32:29d         16.008555 122
  Seq=0 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM [SYN] 53 → 17564 86       TCP         fe80::1  …fe80::b2b0:cb32:29d         16.008737 123
   Seq=0 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM [SYN] 53 → 9056 86       TCP         fe80::1  …fe80::b2b0:cb32:29d         16.010581 124
  Seq=0 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM [SYN] 53 → 55003 86       TCP         fe80::1  …fe80::b2b0:cb32:29d         16.010802 125
  Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 15414 66       TCP    23.220.75.232        192.168.100.76         16.011958 126
Seq=0 Ack=1 Win=14120 Len=0 MSS=1412 SACK_PERM WS=4 [SYN, ACK] 5603 → 53 86       TCP  …fe80::b2b0:cb32:29d       fe80::1              16.012371 127
                          Seq=1 Ack=1 Win=65280 Len=0 [ACK] 53 → 5603 74      TCP         fe80::1  …fe80::b2b0:cb32:29d         16.012427 128
Seq=0 Ack=1 Win=14120 Len=0 MSS=1412 SACK_PERM WS=4 [SYN, ACK] 17564 → 53 86      TCP  …fe80::b2b0:cb32:29d       fe80::1              16.013045 129
Seq=0 Ack=1 Win=14120 Len=0 MSS=1412 SACK_PERM WS=4 [SYN, ACK] 9056 → 53 86       TCP  …fe80::b2b0:cb32:29d       fe80::1              16.013045 130
Seq=0 Ack=1 Win=14120 Len=0 MSS=1412 SACK_PERM WS=4 [SYN, ACK] 55003 → 53 86      TCP  …fe80::b2b0:cb32:29d       fe80::1              16.013045 131
                         Seq=1 Ack=1 Win=65280 Len=0 [ACK] 53 → 17564 74      TCP         fe80::1  …fe80::b2b0:cb32:29d         16.013112 132
                          Seq=1 Ack=1 Win=65280 Len=0 [ACK] 53 → 9056 74      TCP         fe80::1  …fe80::b2b0:cb32:29d         16.013135 133
                         Seq=1 Ack=1 Win=65280 Len=0 [ACK] 53 → 55003 74      TCP         fe80::1  …fe80::b2b0:cb32:29d         16.013144 134
 Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 136] [PSH, ACK] 53 → 55003 76   TCP   fe80::1  …fe80::b2b0:cb32:29d         16.015833 135
   Standard query 0xe577 HTTPS google-ohttp-relay-safebrowsing.fastly-edge.com 139   DNS   fe80::1  …fe80::b2b0:cb32:29d         16.015881 136
  Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 138] [PSH, ACK] 53 → 9056 76   TCP   fe80::1  …fe80::b2b0:cb32:29d         16.015952 137
      Standard query 0x310c A google-ohttp-relay-safebrowsing.fastly-edge.com 139    DNS   fe80::1  …fe80::b2b0:cb32:29d         16.016016 138
 Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 140] [PSH, ACK] 53 → 17564 76   TCP   fe80::1  …fe80::b2b0:cb32:29d         16.016289 139
                               Standard query 0x894b HTTPS www.google.com 106   DNS   fe80::1  …fe80::b2b0:cb32:29d         16.016317 140
  Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 142] [PSH, ACK] 53 → 5603 76   TCP   fe80::1  …fe80::b2b0:cb32:29d         16.016360 141
                                  Standard query 0xbe6f A www.google.com 106   DNS   fe80::1  …fe80::b2b0:cb32:29d         16.016377 142
                         Seq=1 Ack=3 Win=14120 Len=0 [ACK] 55003 → 53 74      TCP  …fe80::b2b0:cb32:29d       fe80::1              16.017470 143

44 38 e8 bf e2 d5 f4 1d  6b cf 07 74 08 00 45 00   D8······k··t··E·
00 28 ae 36 40 00 39 06  2d 79 ac 40 94 eb c0 a8   ·(·6@·9· -y·@····
64 4c 01 bb 6b 50 0e 8f  ed b4 5b aa 5e bb 50 10   dL··kP·· ··[·^·P·
00 10 25 ef 00 00 00 00  00 00 00 00               ··%····· ····

its), 60 bytes captured (480 bits) on interface \Device\NPF_{D8F6B229-C784-423C-8257-AB0FB16E2279}, id 0
  Ethernet II, Src: HuaweiTechno_cf:07:74 (f4:1d:6b:cf:07:74), Dst: Intel_bf:e2:d5 (44:38:e8:bf:e2:d5)
                  Internet Protocol Version 4, Src: 172.64.148.235, Dst: 192.168.100.76
          Transmission Control Protocol, Src Port: 443, Dst Port: 27472, Seq: 25, Ack: 29, Len: 0
```



png.223737 08-09-2025 لقطة شاشة

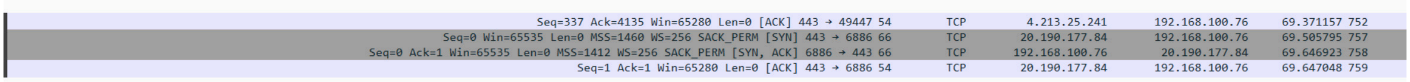
Wireshark · Follow TCP Stream (tcp.stream eq 0) · شبكة Wi-Fi

```
....D.........6.|...t.s...............L.)..n...V.....{@..J....q. .>2Zo.1
```

```
tcp.stream eq 0
          Source        Time  .No
  2.250.200.164   0.000000 1
    172.20.10.2   0.018063 2
  2.250.200.164   0.203508 3
    172.20.10.2   0.203586 4
```

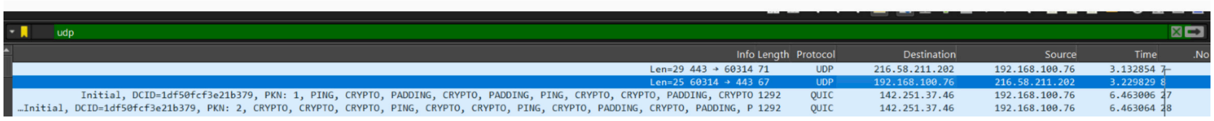
Task 2: Analyze TCP handshake and investigate Data Transfer and Termination
Step 1: Find and select packets related to the TCP three-way handshake:

- SYN: Initiates a connection.
- SYN-ACK: Acknowledges and responds to the SYN.
- ACK: Acknowledges the SYN-ACK and establishes the connection.



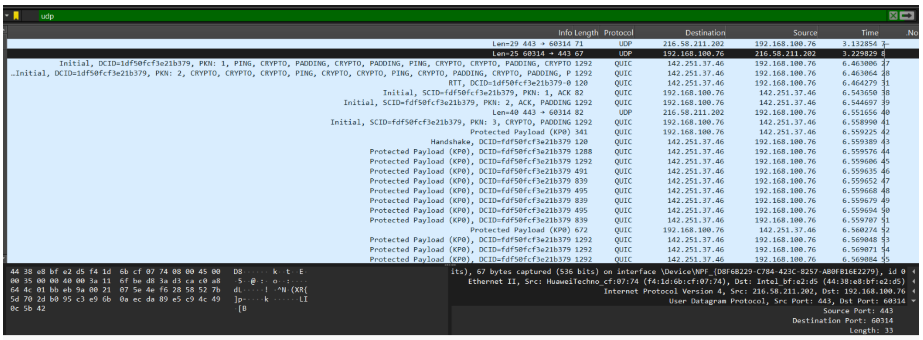
```
               Seq=337 Ack=4135 Win=65280 Len=0 [ACK] 443 → 49447 54     TCP      4.213.25.241    192.168.100.76   69.371157 752
        Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 443 → 6886 66     TCP     20.190.177.84    192.168.100.76   69.505795 757
Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM [SYN, ACK] 6886 → 443 66     TCP    192.168.100.76     20.190.177.84   69.646923 758
                    Seq=1 Ack=1 Win=65280 Len=0 [ACK] 443 → 6886 54     TCP     20.190.177.84    192.168.100.76   69.647048 759
```

Task 1: Generate UDP traffic and capture packets



```
udp
                                                                          Info Length  Protocol     Destination          Source         Time     .No
                                                               Len=29 443 → 60314 71      UDP   216.58.211.202   192.168.100.76   3.132854  7
                                                               Len=25 60314 → 443 67      UDP   192.168.100.76   216.58.211.202   3.229829  8
        Initial, DCID=1df50fcf3e21b379, PKN: 1, PING, CRYPTO, PADDING, CRYPTO, PADDING, PING, CRYPTO, CRYPTO, PADDING, CRYPTO 1292  QUIC  142.251.37.46  192.168.100.76  6.463006  27
…Initial, DCID=1df50fcf3e21b379, PKN: 2, CRYPTO, CRYPTO, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PADDING, P 1292  QUIC  142.251.37.46  192.168.100.76  6.463064  28
```

Task 2: Filter and analysis UDP Packets



```
udp
                                                                          Info Length  Protocol     Destination          Source         Time     .No
                                                               Len=29 443 → 60314 71      UDP   216.58.211.202   192.168.100.76   3.132854  7
                                                               Len=25 60314 → 443 67      UDP   192.168.100.76   216.58.211.202   3.229829  8
        Initial, DCID=1df50fcf3e21b379, PKN: 1, PING, CRYPTO, PADDING, CRYPTO, PADDING, PING, CRYPTO, CRYPTO, PADDING, CRYPTO 1292  QUIC  142.251.37.46  192.168.100.76  6.463006  27
…Initial, DCID=1df50fcf3e21b379, PKN: 2, CRYPTO, CRYPTO, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PADDING, P 1292  QUIC  142.251.37.46  192.168.100.76  6.463064  28
                                                     RTT, DCID=1df50fcf3e21b379-0 120     QUIC   142.251.37.46   192.168.100.76   6.464279  31
                                         Initial, SCID=fdf50fcf3e21b379, PKN: 1, ACK 82   QUIC   192.168.100.76   142.251.37.46   6.543650  38
                              Initial, SCID=fdf50fcf3e21b379, PKN: 2, ACK, PADDING 1292   QUIC   192.168.100.76   142.251.37.46   6.544697  39
                                                               Len=40 443 → 60314 82      UDP   216.58.211.202   192.168.100.76   6.551656  40
                           Initial, SCID=fdf50fcf3e21b379, PKN: 3, CRYPTO, PADDING 1292   QUIC   192.168.100.76   142.251.37.46   6.558990  41
                                                         Protected Payload (KP0) 341      QUIC   192.168.100.76   142.251.37.46   6.559225  42
                                                 Handshake, DCID=fdf50fcf3e21b379 120     QUIC   142.251.37.46   192.168.100.76   6.559389  43
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 1288       QUIC   142.251.37.46   192.168.100.76   6.559576  44
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 1292       QUIC   142.251.37.46   192.168.100.76   6.559606  45
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 491        QUIC   142.251.37.46   192.168.100.76   6.559635  46
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 839        QUIC   142.251.37.46   192.168.100.76   6.559652  47
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 495        QUIC   142.251.37.46   192.168.100.76   6.559668  48
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 839        QUIC   142.251.37.46   192.168.100.76   6.559679  49
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 495        QUIC   142.251.37.46   192.168.100.76   6.559694  50
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 839        QUIC   142.251.37.46   192.168.100.76   6.559707  51
                                                         Protected Payload (KP0) 672      QUIC   192.168.100.76   142.251.37.46   6.560274  52
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 1292       QUIC   142.251.37.46   192.168.100.76   6.569048  53
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 1292       QUIC   142.251.37.46   192.168.100.76   6.569071  54
                                Protected Payload (KP0), DCID=fdf50fcf3e21b379 1292       QUIC   142.251.37.46   192.168.100.76   6.569084  55
```

```
44 38 e8 bf e2 d5 f4 1d  6b cf 07 74 08 00 45 00   D8······k··t··E·
00 35 00 00 40 00 3a 11  6f be d8 3a d3 ca c0 a8   ·5··@·:·o·:·····
64 4c 01 bb eb 9a 00 21  07 5e 4e f6 28 58 52 7b   dL·····!·^N·(XR{
5d 70 2d b0 95 c3 e9 6b  0a ec da 89 e5 c9 4c 49   ]p-····k······LI
0c 5b 42                                            ·[B
```

```
its), 67 bytes captured (536 bits) on interface \Device\NPF_{D8F6B229-C784-423C-8257-AB0FB16E2279}, id 0
            Ethernet II, Src: HuaweiTechno_cf:07:74 (f4:1d:6b:cf:07:74), Dst: Intel_bf:e2:d5 (44:38:e8:bf:e2:d5)
                                             Internet Protocol Version 4, Src: 216.58.211.202, Dst: 192.168.100.76
                                                           User Datagram Protocol, Src Port: 443, Dst Port: 60314
                                                                                              Source Port: 443
                                                                                      Destination Port: 60314
                                                                                                   Length: 33
```

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

	TCP or UDP	Reasons
Reliability and Connection Establishment	**Tcp**	**Uses handshake, acknowledgments, and retransmissions.**
Data Integrity and Ordering	**Tcp**	**Uses sequence numbers to ensure order and checksums for integrity.**

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

	TCP	UDP
Use cases	**Web, email, file transfer**	**Video streaming, VoIP, gaming**
Performance	**Slower, more overhead**	**Faster, less overhead**