Qassim University

Raneem Alrshoudi 392207752

Dr. Bashayer

This lab session covers the usage of the Wireshark application to monitor and capture the outgoing and incoming packets from a network connection (WIFI, ethernet, etc.). Specifically, students should be able to analyze HTTP, HTTPS, TCP/IP, and UDP protocols using Wireshark, a network protocol analyzer, and draw conclusions.

Pre-lab Preparation:

1. Review the basics and the structure of HTTP, TCP/IP, and UDP protocols,
2. Install Wireshark and ensure it is running on your computer,
3. Create an online, *publically accessible* Git repository to host and upload your work in the labs. We recommend you use GitHub or GitLab.

Lab Activities:

Part 1: Capturing HTTP Traffic.

Task 1: Start Wireshark and capture packets.

Step 1: Open Wireshark.
Step 2: Select the network interface connected to the internet (e.g., Ethernet or Wi-Fi).
Step 3: Click the "Start Capturing Packets" button (the shark fin icon).
Step 4: Open your favorite web browser and navigate to (http://neverssl.com/) website.
Step 5: After the website has fully loaded, stop capturing packets by clicking the red stop button in Wireshark.

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.

Part 2: Analyzing TCP/IP Traffic.

Task 1: Filter TCP packets

Step 1: Clear the previous filter and type TCP to focus on TCP packets.
Step 2: Select a TCP packet related to your HTTP request/response.
Step 3: Right-click on the packet and select "Follow" -> "TCP Stream".
Step 4: This shows the entire conversation between the client and server.

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

Step 1: Find and select packets related to the TCP three-way handshake: o
SYN: Initiates a connection. o SYN-ACK: Acknowledges and responds to the SYN.
o ACK: Acknowledges the SYN-ACK and establishes the connection.
Step 2: Note the sequence and acknowledgment numbers. Screenshot and upload your image to your online git repository.
Step 3: Observe the data packets exchanged between the client and server. Take a screenshot and upload it to your online git repo.

Step 4: Look at the TCP termination process (FIN, ACK packets).

Part 3: Capturing and Analyzing UDP Traffic

Task 1: Generate UDP traffic and capture packets

Step 1: Open a network application that uses UDP (e.g., streaming video, VoIP software, or custom script).
Step 2: Start the application to generate UDP traffic.
Step 3: Start capturing packets in Wireshark while the UDP application is running. **Step 4:** After sufficient traffic is generated, stop capturing packets.

Task 2: Filter and analysis UDP Packets
Step 1: In the filter bar, type UDP and press Enter.
Step 2: This filters out only the UDP packets from the capture.
Step 3: Select any UDP packet to view its details.
Step 4: Observe the source and destination ports, length, and data. **Step 5:** Compare the simplicity of UDP headers with TCP headers.

Part 4: Comparing TCP and UDP by filling in the following tables. Save your work (e.g., in an MS Word document), and upload it to your online git repo.

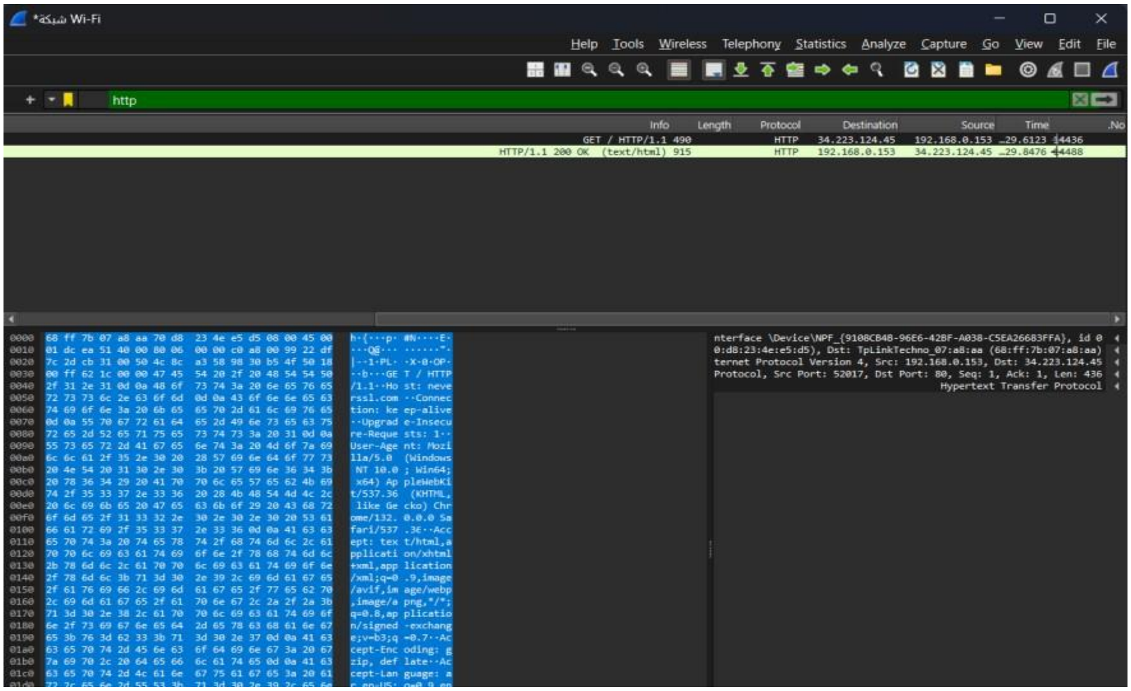
Task 1: Fill in the following table and provide reasons.

	TCP or UDP	**Reasons**
Reliability and Connection Establishment		
Data Integrity and Ordering		

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

	TCP	**UDP**
Use cases		
Performance		

Part1

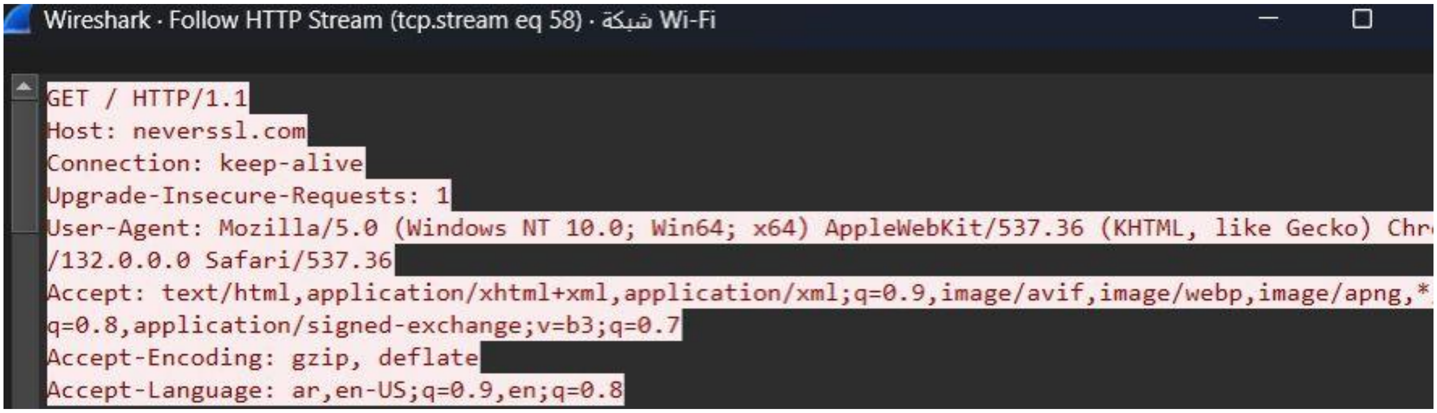

*شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
http

```
                                  Info    Length   Protocol   Destination      Source          Time       .No
                GET / HTTP/1.1 490                  HTTP      34.223.124.45    192.168.0.153   …29.6123   4436
HTTP/1.1 200 OK  (text/html) 915                    HTTP      192.168.0.153    34.223.124.45   …29.8476   4488
```

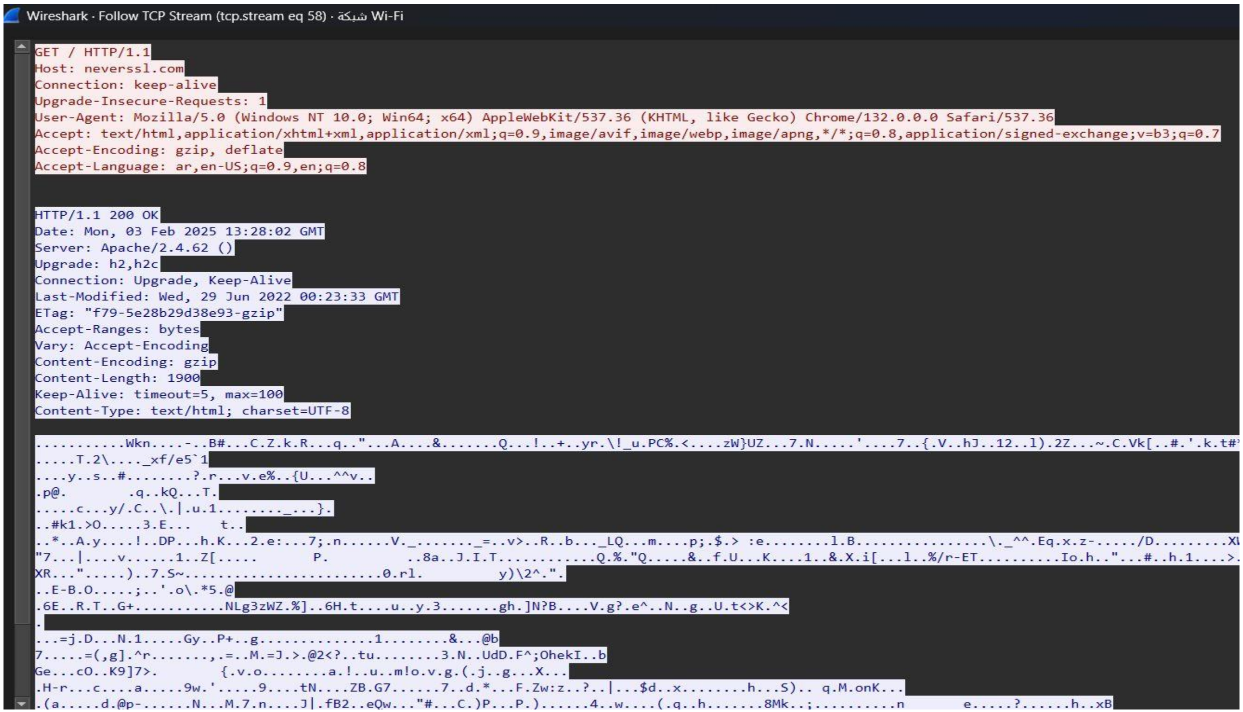
```
0000  68 ff 7b 07 a8 aa 70 d8  23 4e e5 d5 08 00 45 00   h·{···p· #N····E·
0010  01 dc ea 51 40 00 80 06  00 00 c0 a8 00 99 22 df   ···Q@··· ······"·
0020  7c 2d cb 31 00 50 4c 8c  a3 58 98 30 b5 4f 50 18   |-·1·PL· ·X·0·OP·
0030  00 ff 62 1c 00 00 47 45  54 20 2f 20 48 54 54 50   ··b···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 6e 65 76 65   /1.1··Ho st: neve
0050  72 73 73 6c 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   rssl.com ··Connec
0060  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0070  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0080  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
0090  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
00a0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
00b0  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b    NT 10.0 ; Win64;
00c0  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69    x64) Ap pleWebKi
00d0  74 2f 35 33 37 2e 33 36  20 28 4b 48 54 4d 4c 2c   t/537.36  (KHTML,
00e0  20 6c 69 6b 65 20 47 65  63 6b 6f 29 20 43 68 72    like Ge cko) Chr
00f0  6f 6d 65 2f 31 33 32 2e  30 2e 30 2e 30 20 53 61   ome/132. 0.0.0 Sa
0100  66 61 72 69 2f 35 33 37  2e 33 36 0d 0a 41 63 63   fari/537 .36··Acc
0110  65 70 74 3a 20 74 65 78  74 2f 68 74 6d 6c 2c 61   ept: tex t/html,a
0120  70 70 6c 69 63 61 74 69  6f 6e 2f 78 68 74 6d 6c   pplicati on/xhtml
0130  2b 78 6d 6c 2c 61 70 70  6c 69 63 61 74 69 6f 6e   +xml,app lication
0140  2f 78 6d 6c 3b 71 3d 30  2e 39 2c 69 6d 61 67 65   /xml;q=0 .9,image
0150  2f 61 76 69 66 2c 69 6d  61 67 65 2f 77 65 62 70   /avif,im age/webp
0160  2c 69 6d 61 67 65 2f 61  70 6e 67 2c 2a 2f 2a 3b   ,image/a png,*/*;
0170  71 3d 30 2e 38 2c 61 70  70 6c 69 63 61 74 69 6f   q=0.8,ap plicatio
0180  6e 2f 73 69 67 6e 65 64  2d 65 78 63 68 61 6e 67   n/signed -exchang
0190  65 3b 76 3d 62 33 3b 71  3d 30 2e 37 0d 0a 41 63   e;v=b3;q =0.7··Ac
01a0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
01b0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 41 63   zip, def late··Ac
01c0  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 61   cept-Lan guage: a
01d0  72 2c 65 6e 2d 55 53 3b  71 3d 30 2e 39 2c 65 6e   r,en-US; q=0.9,en
```

```
nterface \Device\NPF_{9108CB48-96E6-428F-A038-C5EA26683FFA}, id 0
0:d8:23:4e:e5:d5), Dst: TpLinkTechno_07:a8:aa (68:ff:7b:07:a8:aa)
ternet Protocol Version 4, Src: 192.168.0.153, Dst: 34.223.124.45
Protocol, Src Port: 52017, Dst Port: 80, Seq: 1, Ack: 1, Len: 436
                                       Hypertext Transfer Protocol
```

Part2


Wireshark · Follow HTTP Stream (tcp.stream eq 58) · شبكة Wi-Fi

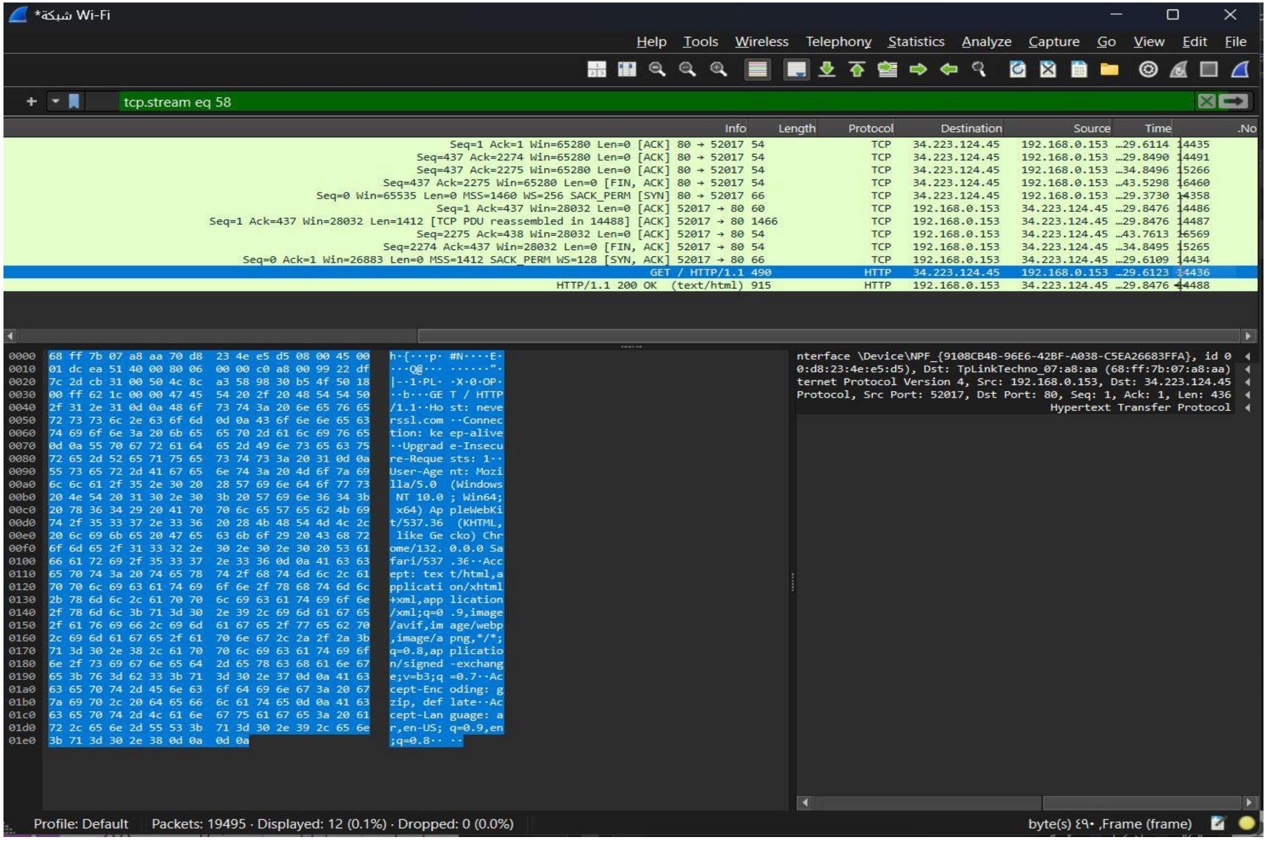
```
GET / HTTP/1.1
Host: neverssl.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
```


Wireshark · Follow TCP Stream (tcp.stream eq 58) · شبكة Wi-Fi

```
GET / HTTP/1.1
Host: neverssl.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8


HTTP/1.1 200 OK
Date: Mon, 03 Feb 2025 13:28:02 GMT
Server: Apache/2.4.62 ()
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Wed, 29 Jun 2022 00:23:33 GMT
ETag: "f79-5e28b29d38e93-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1900
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8

...........Wkn....-..B#...C.Z.k.R...q.."...A....&.......Q...!..+..yr.\!_u.PC%.<....zW}UZ...7.N.....'....7..{.V..hJ..12..l).2Z...~.C.Vk[..#.'.k.t#
.....T.2\...._xf/e5`1
....y..s..#........?.r...v.e%..{U...^^v..
.p@.        .q..kQ...T.
.....c...y/.C..\.|.u.1........_...}.
..#k1.>O.....3.E...    t..
..*..A.y....!..DP...h.K...2.e:...7;.n......V._......._=..v>..R..b..._LQ...m....p;.$.> :e........l.B................\._^^.Eq.x.z-...../D.........X
"7...|....v......1..Z[.....       P.          ..8a..J.I.T...........Q.%."Q.....&..f.U...K....1..&.X.i[...l..%/r-ET..........Io.h.."...#..h.1....>.
XR..."......)..7.S~.........................0.rl.          y)\2^.".
..E-B.O.....;..'.o\.*5.@
.6E..R.T..G+...........NLg3zWZ.%]..6H.t....u..y.3.......gh.]N?B....V.g?.e^..N..g..U.t<>K.^<
.
...=j.D...N.1.....Gy..P+..g..............1........&...@b
7.....=(,g].^r........,.=..M.=J.>.@2<?..tu.........3.N..UdD.F^;OhekI..b
Ge...cO..K9]7>.       {.v.o........a.!..u..m!o.v.g.(.j..g...X...
.H-r...c....a.....9w.'.....9....tN....ZB.G7......7..d.*...F.Zw:z..?..|...$d..x.........h...S).. q.M.onK...
.(a.....d.@p-......N...M.7.n....J|.fB2..eQw..."#...C.)P...P.)......4..w....(.q..h.......8Mk..;..........n        e.....?......h..xB
```


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

```
tcp.stream eq 58
```

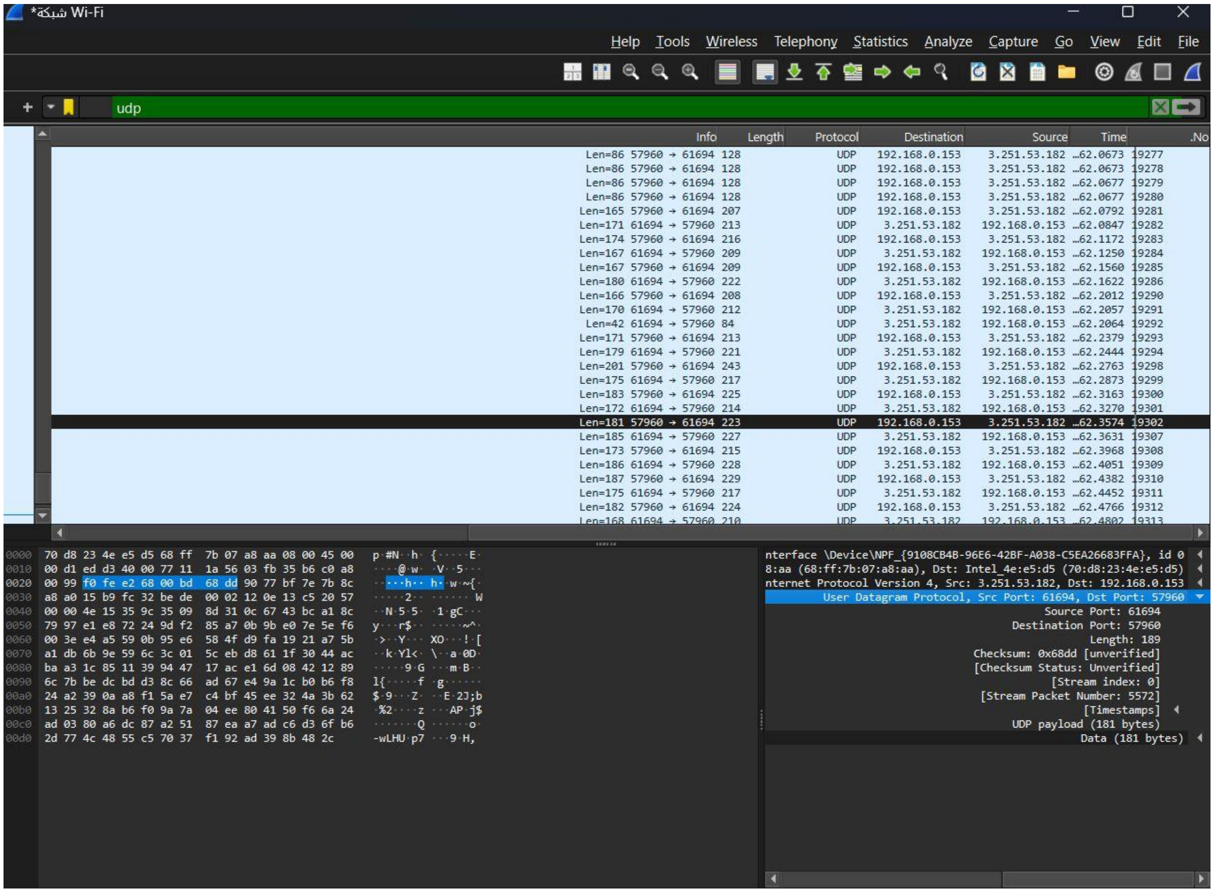
```
                                                          Info  Length  Protocol     Destination          Source     Time    .No
                  Seq=1 Ack=1 Win=65280 Len=0 [ACK] 80 → 52017 54        TCP   34.223.124.45   192.168.0.153  …29.6114  14435
              Seq=437 Ack=2274 Win=65280 Len=0 [ACK] 80 → 52017 54        TCP   34.223.124.45   192.168.0.153  …29.8490  14491
              Seq=437 Ack=2275 Win=65280 Len=0 [ACK] 80 → 52017 54        TCP   34.223.124.45   192.168.0.153  …34.8496  15266
         Seq=437 Ack=2275 Win=65280 Len=0 [FIN, ACK] 80 → 52017 54        TCP   34.223.124.45   192.168.0.153  …43.5298  16460
    Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 52017 66   TCP   34.223.124.45   192.168.0.153  …29.3730  14358
                Seq=1 Ack=437 Win=28032 Len=0 [ACK] 52017 → 80 60        TCP   192.168.0.153   34.223.124.45  …29.8476  14486
Seq=1 Ack=437 Win=28032 Len=1412 [TCP PDU reassembled in 14488] [ACK] 52017 → 80 1466   TCP   192.168.0.153   34.223.124.45  …29.8476  14487
             Seq=2275 Ack=438 Win=28032 Len=0 [ACK] 52017 → 80 54        TCP   192.168.0.153   34.223.124.45  …43.7613  16569
        Seq=2274 Ack=437 Win=28032 Len=0 [FIN, ACK] 52017 → 80 54        TCP   192.168.0.153   34.223.124.45  …34.8495  15265
 Seq=0 Ack=1 Win=26883 Len=0 MSS=1412 SACK_PERM WS=128 [SYN, ACK] 52017 → 80 66   TCP   192.168.0.153   34.223.124.45  …29.6109  14434
                                            GET / HTTP/1.1 490       HTTP   34.223.124.45   192.168.0.153  …29.6123  14436
                              HTTP/1.1 200 OK  (text/html) 915       HTTP   192.168.0.153   34.223.124.45  …29.8476  14488
```

```
0000  68 ff 7b 07 a8 aa 70 d8  23 4e e5 d5 08 00 45 00   h·{···p· #N····E·
0010  01 dc ea 51 40 00 80 06  00 00 c0 a8 00 99 22 df   ···Q@··· ······"·
0020  7c 2d cb 31 00 50 4c 8c  a3 58 98 30 b5 4f 50 18   |-·1·PL· ·X·0·OP·
0030  00 ff 62 1c 00 00 47 45  54 20 2f 20 48 54 54 50   ··b···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 6e 65 76 65   /1.1··Ho st: neve
0050  72 73 73 6c 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   rssl.com ··Connec
0060  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0070  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0080  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
0090  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
00a0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
00b0  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b    NT 10.0 ; Win64;
00c0  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69    x64) Ap pleWebKi
00d0  74 2f 35 33 37 2e 33 36  20 28 4b 48 54 4d 4c 2c   t/537.36  (KHTML,
00e0  20 6c 69 6b 65 20 47 65  63 6b 6f 29 20 43 68 72    like Ge cko) Chr
00f0  6f 6d 65 2f 31 33 32 2e  30 2e 30 2e 30 20 53 61   ome/132. 0.0.0 Sa
0100  66 61 72 69 2f 35 33 37  2e 33 36 0d 0a 41 63 63   fari/537 .36··Acc
0110  65 70 74 3a 20 74 65 78  74 2f 68 74 6d 6c 2c 61   ept: tex t/html,a
0120  70 70 6c 69 63 61 74 69  6f 6e 2f 78 68 74 6d 6c   pplicati on/xhtml
0130  2b 78 6d 6c 2c 61 70 70  6c 69 63 61 74 69 6f 6e   +xml,app lication
0140  2f 78 6d 6c 3b 71 3d 30  2e 39 2c 69 6d 61 67 65   /xml;q=0 .9,image
0150  2f 61 76 69 66 2c 69 6d  61 67 65 2f 77 65 62 70   /avif,im age/webp
0160  2c 69 6d 61 67 65 2f 61  70 6e 67 2c 2a 2f 2a 3b   ,image/a png,*/*;
0170  71 3d 30 2e 38 2c 61 70  70 6c 69 63 61 74 69 6f   q=0.8,ap plicatio
0180  6e 2f 73 69 67 6e 65 64  2d 65 78 63 68 61 6e 67   n/signed -exchang
0190  65 3b 76 3d 62 33 3b 71  3d 30 2e 37 0d 0a 41 63   e;v=b3;q =0.7··Ac
01a0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
01b0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 41 63   zip, def late··Ac
01c0  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 61   cept-Lan guage: a
01d0  72 2c 65 6e 2d 55 53 3b  71 3d 30 2e 39 2c 65 6e   r,en-US; q=0.9,en
01e0  3b 71 3d 30 2e 38 0d 0a  0d 0a                     ;q=0.8·· ··
```

```
nterface \Device\NPF_{9108CB4B-96E6-42BF-A038-C5EA26683FFA}, id 0
0:d8:23:4e:e5:d5), Dst: TpLinkTechno_07:a8:aa (68:ff:7b:07:a8:aa)
ternet Protocol Version 4, Src: 192.168.0.153, Dst: 34.223.124.45
Protocol, Src Port: 52017, Dst Port: 80, Seq: 1, Ack: 1, Len: 436
                                       Hypertext Transfer Protocol
```

Profile: Default
Packets: 19495 · Displayed: 12 (0.1%) · Dropped: 0 (0.0%)
byte(s) ٤٩٠ ,Frame (frame)

Part3



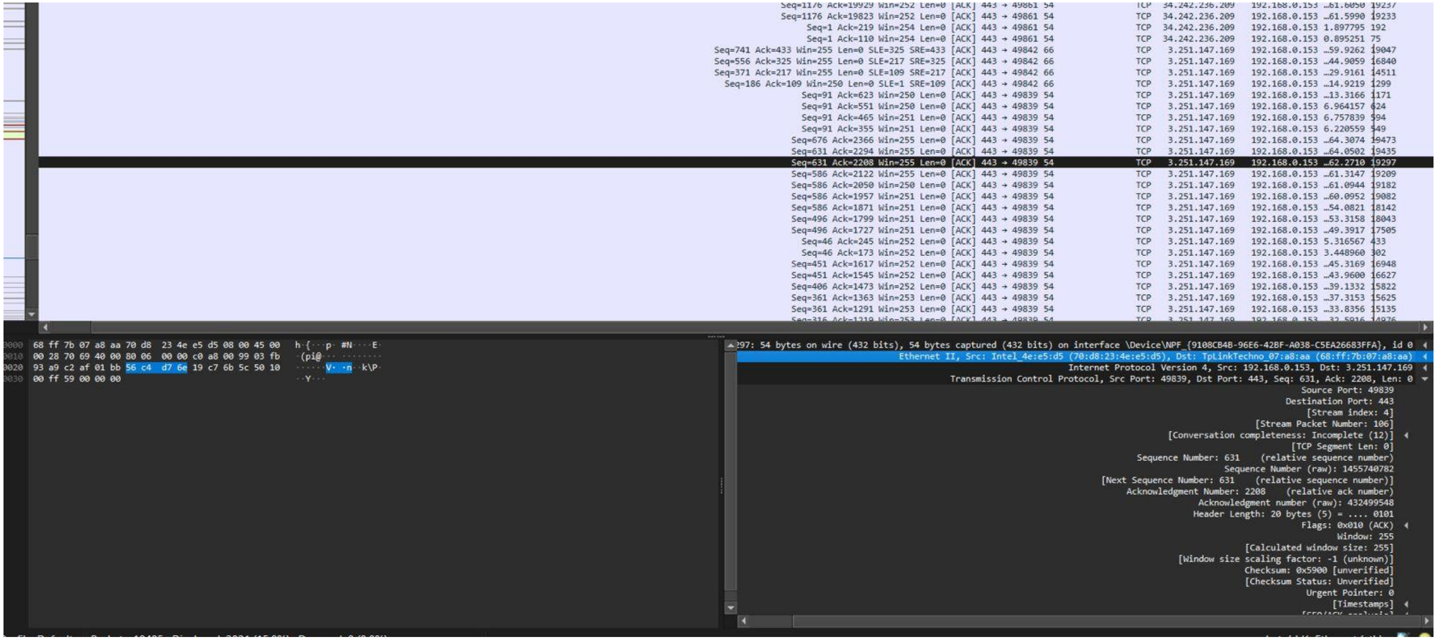
*شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File

```
udp
```

```
                               Info  Length  Protocol   Destination         Source      Time    .No
   Len=86 57960 → 61694 128                   UDP   192.168.0.153   3.251.53.182  …62.0673  19277
   Len=86 57960 → 61694 128                   UDP   192.168.0.153   3.251.53.182  …62.0673  19278
   Len=86 57960 → 61694 128                   UDP   192.168.0.153   3.251.53.182  …62.0677  19279
   Len=86 57960 → 61694 128                   UDP   192.168.0.153   3.251.53.182  …62.0677  19280
  Len=165 57960 → 61694 207                   UDP   192.168.0.153   3.251.53.182  …62.0792  19281
  Len=171 61694 → 57960 213                   UDP    3.251.53.182  192.168.0.153  …62.0847  19282
  Len=174 57960 → 61694 216                   UDP   192.168.0.153   3.251.53.182  …62.1172  19283
  Len=167 61694 → 57960 209                   UDP    3.251.53.182  192.168.0.153  …62.1250  19284
  Len=167 57960 → 61694 209                   UDP   192.168.0.153   3.251.53.182  …62.1560  19285
  Len=180 61694 → 57960 222                   UDP    3.251.53.182  192.168.0.153  …62.1622  19286
  Len=166 57960 → 61694 208                   UDP   192.168.0.153   3.251.53.182  …62.2012  19290
  Len=170 61694 → 57960 212                   UDP    3.251.53.182  192.168.0.153  …62.2057  19291
   Len=42 61694 → 57960 84                    UDP    3.251.53.182  192.168.0.153  …62.2064  19292
  Len=171 57960 → 61694 213                   UDP   192.168.0.153   3.251.53.182  …62.2379  19293
  Len=179 61694 → 57960 221                   UDP    3.251.53.182  192.168.0.153  …62.2444  19294
  Len=201 57960 → 61694 243                   UDP   192.168.0.153   3.251.53.182  …62.2763  19298
  Len=175 61694 → 57960 217                   UDP    3.251.53.182  192.168.0.153  …62.2873  19299
  Len=183 57960 → 61694 225                   UDP   192.168.0.153   3.251.53.182  …62.3163  19300
  Len=172 61694 → 57960 214                   UDP    3.251.53.182  192.168.0.153  …62.3270  19301
  Len=181 57960 → 61694 223                   UDP   192.168.0.153   3.251.53.182  …62.3574  19302
  Len=185 61694 → 57960 227                   UDP    3.251.53.182  192.168.0.153  …62.3631  19307
  Len=173 57960 → 61694 215                   UDP   192.168.0.153   3.251.53.182  …62.3968  19308
  Len=186 61694 → 57960 228                   UDP    3.251.53.182  192.168.0.153  …62.4051  19309
  Len=187 57960 → 61694 229                   UDP   192.168.0.153   3.251.53.182  …62.4382  19310
  Len=175 61694 → 57960 217                   UDP    3.251.53.182  192.168.0.153  …62.4452  19311
  Len=182 57960 → 61694 224                   UDP   192.168.0.153   3.251.53.182  …62.4766  19312
  Len=168 61694 → 57960 210                   UDP    3.251.53.182  192.168.0.153  …62.4802  19313
```

```
0000  70 d8 23 4e e5 d5 68 ff  7b 07 a8 aa 08 00 45 00   p·#N··h· {·····E·
0010  00 d1 ed d3 40 00 77 11  1a 56 03 fb 35 b6 c0 a8   ····@·w· ·V··5···
0020  00 99 f0 fe e2 68 00 bd  68 dd 90 77 bf 7e 7b 8c   ·····h·· h··w·~{·
0030  a8 a0 15 b9 fc 32 be de  00 02 12 0e 13 c5 20 57   ·····2·· ······ W
0040  00 00 4e 15 35 9c 35 09  8d 31 0c 67 43 bc a1 8c   ··N·5·5· ·1·gC···
0050  79 97 e1 e8 72 24 9d f2  85 a7 0b 9b e0 7e 5e f6   y···r$·· ·····~^·
0060  00 3e e4 a5 59 0b 95 e6  58 4f d9 fa 19 21 a7 5b   ·>··Y··· XO···!·[
0070  a1 db 6b 9e 59 6c 3c 01  5c eb d8 61 1f 30 44 ac   ··k·Yl<· \··a·0D·
0080  ba a3 1c 85 11 39 94 47  17 ac e1 6d 08 42 12 89   ·····9·G ···m·B··
0090  6c 7b be dc bd d3 8c 66  ad 67 e4 9a 1c b0 b6 f8   l{·····f ·g······
00a0  24 a2 39 0a a8 f1 5a e7  c4 bf 45 ee 32 4a 3b 62   $·9···Z· ··E·2J;b
00b0  13 25 32 8a b6 f0 9a 7a  04 ee 80 41 50 f6 6a 24   ·%2····z ···AP·j$
00c0  ad 03 80 a6 dc 87 a2 51  87 ea a7 ad c6 d3 6f b6   ·······Q ······o·
00d0  2d 77 4c 48 55 c5 70 37  f1 92 ad 39 8b 48 2c      -wLHU·p7 ···9·H,
```

```
nterface \Device\NPF_{9108CB4B-96E6-42BF-A038-C5EA26683FFA}, id 0
8:aa (68:ff:7b:07:a8:aa), Dst: Intel_4e:e5:d5 (70:d8:23:4e:e5:d5)
nternet Protocol Version 4, Src: 3.251.53.182, Dst: 192.168.0.153
      User Datagram Protocol, Src Port: 61694, Dst Port: 57960
                                        Source Port: 61694
                                   Destination Port: 57960
                                               Length: 189
                            Checksum: 0x68dd [unverified]
                           [Checksum Status: Unverified]
                                        [Stream index: 0]
                           [Stream Packet Number: 5572]
                                             [Timestamps]
                                    UDP payload (181 bytes)
                                                Data (181 bytes)
```

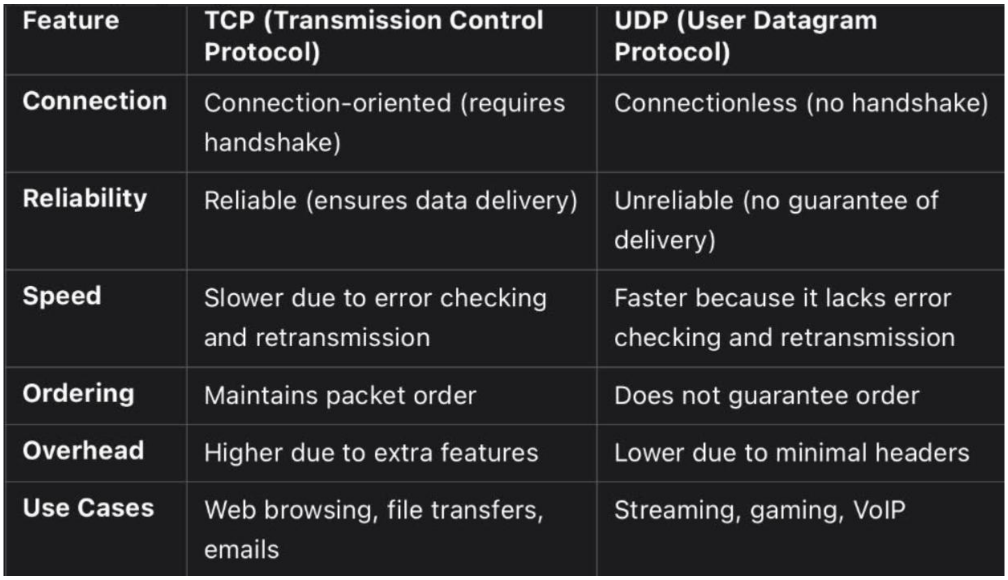


```
Seq=1176 Ack=19929 Win=252 Len=0 [ACK] 443 → 49861 54             TCP  34.242.236.209  192.168.0.153 …61.6050 19237
Seq=1176 Ack=19823 Win=252 Len=0 [ACK] 443 → 49861 54             TCP  34.242.236.209  192.168.0.153 …61.5990 19233
   Seq=1 Ack=219 Win=254 Len=0 [ACK] 443 → 49861 54               TCP  34.242.236.209  192.168.0.153 1.897795 192
   Seq=1 Ack=110 Win=254 Len=0 [ACK] 443 → 49861 54               TCP  34.242.236.209  192.168.0.153 0.895251 75
Seq=741 Ack=433 Win=255 Len=0 SLE=325 SRE=433 [ACK] 443 → 49842 66 TCP   3.251.147.169  192.168.0.153 …59.9262 19047
Seq=556 Ack=325 Win=255 Len=0 SLE=217 SRE=325 [ACK] 443 → 49842 66 TCP   3.251.147.169  192.168.0.153 …44.9059 16840
Seq=371 Ack=217 Win=255 Len=0 SLE=109 SRE=217 [ACK] 443 → 49842 66 TCP   3.251.147.169  192.168.0.153 …29.9161 14511
 Seq=186 Ack=109 Win=250 Len=0 SLE=1 SRE=109 [ACK] 443 → 49842 66  TCP   3.251.147.169  192.168.0.153 …14.9219 1299
   Seq=91 Ack=623 Win=250 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …13.3166 1171
   Seq=91 Ack=551 Win=250 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 6.964157 624
   Seq=91 Ack=465 Win=251 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 6.757839 594
   Seq=91 Ack=355 Win=251 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 6.220559 549
 Seq=676 Ack=2366 Win=255 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …64.3074 19473
 Seq=631 Ack=2294 Win=255 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …64.0502 19435
 Seq=631 Ack=2208 Win=255 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …62.2710 19297
 Seq=586 Ack=2122 Win=255 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …61.3147 19209
 Seq=586 Ack=2050 Win=250 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …61.0944 19182
 Seq=586 Ack=1957 Win=251 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …60.0952 19082
 Seq=586 Ack=1871 Win=251 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …54.0821 18142
 Seq=496 Ack=1799 Win=251 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …53.3158 18043
 Seq=496 Ack=1727 Win=251 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …49.3917 17505
   Seq=46 Ack=245 Win=252 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 5.316567 433
   Seq=46 Ack=173 Win=252 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 3.448960 302
 Seq=451 Ack=1617 Win=252 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …45.3169 16948
 Seq=451 Ack=1545 Win=252 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …43.9600 16627
 Seq=406 Ack=1473 Win=252 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …39.1332 15822
 Seq=361 Ack=1363 Win=253 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …37.3153 15625
 Seq=361 Ack=1291 Win=253 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …33.8356 15135
 Seq=316 Ack=1219 Win=253 Len=0 [ACK] 443 → 49839 54              TCP   3.251.147.169  192.168.0.153 …32.5916 14976
```

```
0000  68 ff 7b 07 a8 aa 70 d8  23 4e e5 d5 08 00 45 00   h·{···p· #N····E·
0010  00 28 70 69 40 00 80 06  00 00 c0 a8 00 99 03 fb   ·(pi@··· ········
0020  93 a9 c2 af 01 bb 56 c4  d7 6e 19 c7 6b 5c 50 10   ······V· ·n··k\P·
0030  00 ff 59 00 00 00                                  ··Y···
```

```
297: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9108CB4B-96E6-42BF-A038-C5EA26683FFA}, id 0
          Ethernet II, Src: Intel_4e:e5:d5 (70:d8:23:4e:e5:d5), Dst: TpLinkTechno_07:a8:aa (68:ff:7b:07:a8:aa)
                                  Internet Protocol Version 4, Src: 192.168.0.153, Dst: 3.251.147.169
             Transmission Control Protocol, Src Port: 49839, Dst Port: 443, Seq: 631, Ack: 2208, Len: 0
                                                                              Source Port: 49839
                                                                          Destination Port: 443
                                                                               [Stream index: 4]
                                                                      [Stream Packet Number: 106]
                                                      [Conversation completeness: Incomplete (12)]
                                                                             [TCP Segment Len: 0]
                                                  Sequence Number: 631    (relative sequence number)
                                                                Sequence Number (raw): 1455740782
                                           [Next Sequence Number: 631    (relative sequence number)]
                                                  Acknowledgment Number: 2208    (relative ack number)
                                                             Acknowledgment number (raw): 432499548
                                                              Header Length: 20 bytes (5) = .... 0101
                                                                                  Flags: 0x010 (ACK)
                                                                                         Window: 255
                                                                      [Calculated window size: 255]
                                                           [Window size scaling factor: -1 (unknown)]
                                                                       Checksum: 0x5900 [unverified]
                                                                       [Checksum Status: Unverified]
                                                                                    Urgent Pointer: 0
                                                                                        [Timestamps]
```

Part4



Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection	Connection-oriented (requires handshake)	Connectionless (no handshake)
Reliability	Reliable (ensures data delivery)	Unreliable (no guarantee of delivery)
Speed	Slower due to error checking and retransmission	Faster because it lacks error checking and retransmission
Ordering	Maintains packet order	Does not guarantee order
Overhead	Higher due to extra features	Lower due to minimal headers
Use Cases	Web browsing, file transfers, emails	Streaming, gaming, VoIP