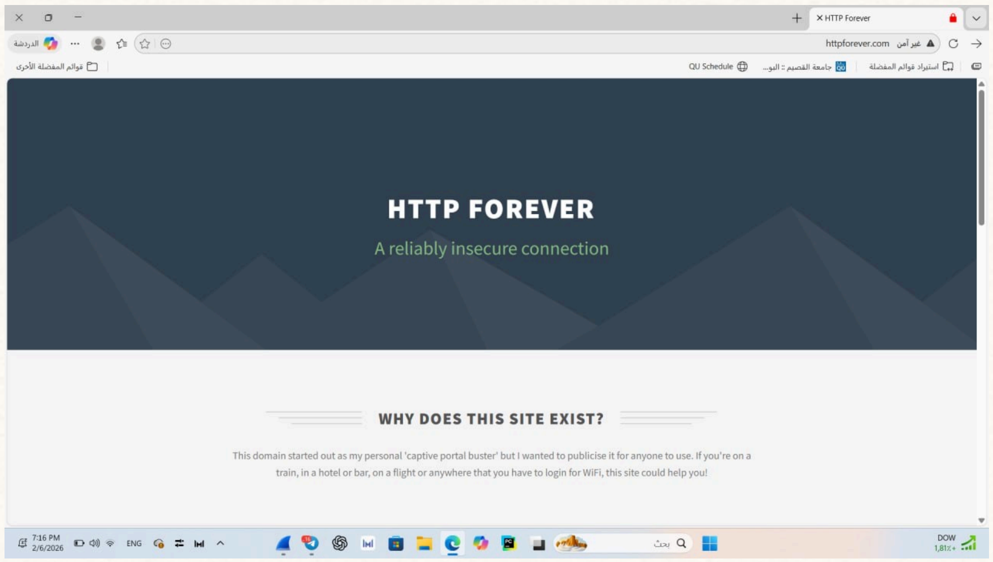
Part 1: Capturing HTTP Traffic.

Task 1:

http://httpforever.com

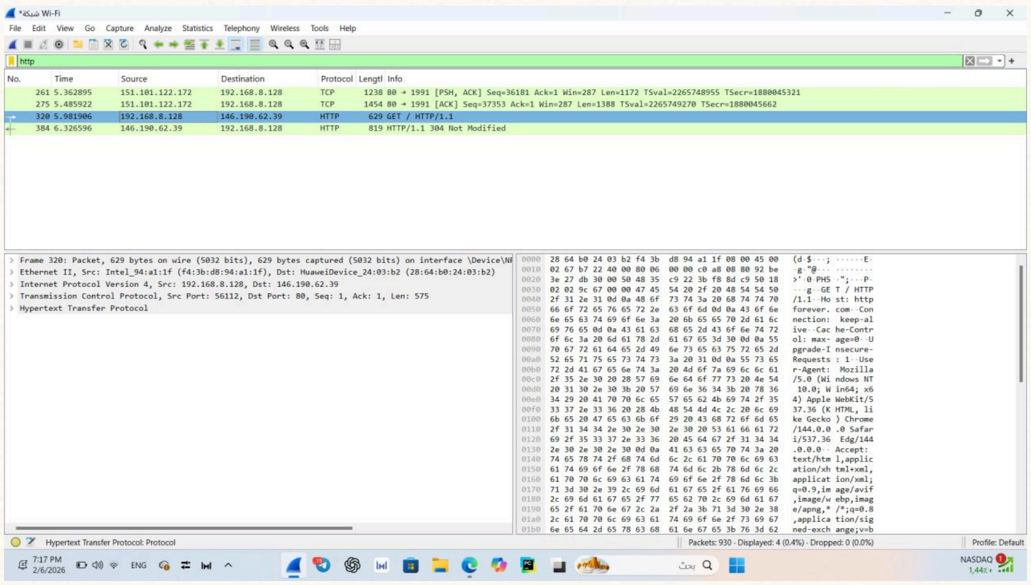


HTTP FOREVER

A reliably insecure connection

WHY DOES THIS SITE EXIST?

This domain started out as my personal 'captive portal buster' but I wanted to publicise it for anyone to use. If you're on a train, in a hotel or bar, on a flight or anywhere that you have to login for WiFi, this site could help you!


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

Filter: http

```
No.  Time      Source          Destination     Protocol Lengtl Info
261  5.362895  151.101.122.172 192.168.8.128   TCP      1238  80 → 1991 [PSH, ACK] Seq=36181 Ack=1 Win=287 Len=1172 TSval=2265748955 TSecr=1880045321
275  5.485922  151.101.122.172 192.168.8.128   TCP      1454  80 → 1991 [ACK] Seq=37353 Ack=1 Win=287 Len=1388 TSval=2265749270 TSecr=1880045662
320  5.981906  192.168.8.128   146.190.62.39   HTTP      629  GET / HTTP/1.1
384  6.326596  146.190.62.39   192.168.8.128   HTTP      819  HTTP/1.1 304 Not Modified
```

```
> Frame 320: Packet, 629 bytes on wire (5032 bits), 629 bytes captured (5032 bits) on interface \Device\NF
> Ethernet II, Src: Intel_94:a1:1f (f4:3b:d8:94:a1:1f), Dst: HuaweiDevice_24:03:b2 (28:64:b0:24:03:b2)
> Internet Protocol Version 4, Src: 192.168.8.128, Dst: 146.190.62.39
> Transmission Control Protocol, Src Port: 56112, Dst Port: 80, Seq: 1, Ack: 1, Len: 575
> Hypertext Transfer Protocol
```

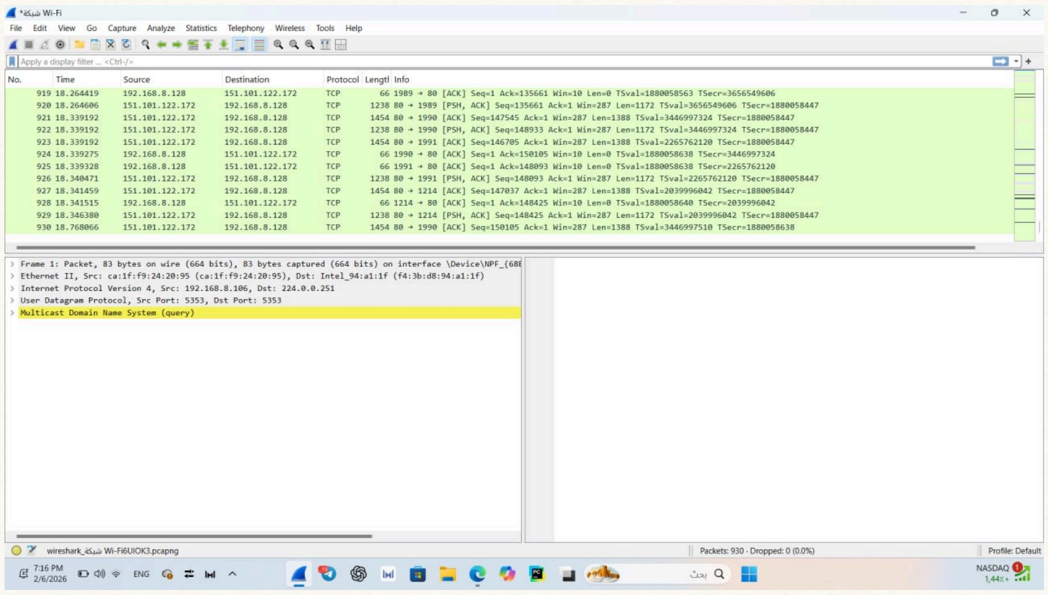
```
0000  28 64 b0 24 03 b2 f4 3b  d8 94 a1 1f 08 00 45 00   (d·$···; ······E·
0010  02 67 b7 22 40 00 80 06  00 00 c0 a8 08 80 92 be   ·g·"@··· ········
0020  3e 27 db 30 00 50 48 35  c9 22 3b f8 8d c9 50 18   >'·0·PH5 ·";···P·
0030  02 02 9c 67 00 00 47 45  54 20 2f 20 48 54 54 50   ···g··GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 74 74 70   /1.1··Ho st: http
0050  66 6f 72 65 76 65 72 2e  63 6f 6d 0d 0a 43 6f 6e   forever. com··Con
0060  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0070  69 76 65 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   ive··Cac he-Contr
0080  6f 6c 3a 20 6d 61 78 2d  61 67 65 3d 30 0d 0a 55   ol: max- age=0··U
0090  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00a0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00b0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00c0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00d0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00e0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
00f0  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0100  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0110  2f 31 34 34 2e 30 2e 30  2e 30 20 53 61 66 61 72   /144.0.0 .0 Safar
0120  69 2f 35 33 37 2e 33 36  20 45 64 67 2f 31 34 34   i/537.36  Edg/144
0130  2e 30 2e 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   .0.0.0·· Accept: 
0140  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0150  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0160  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0170  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
0180  2c 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67   ,image/w ebp,imag
0190  65 2f 61 70 6e 67 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/apng,* /*;q=0.8
01a0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 73 69 67   ,applica tion/sig
01b0  6e 65 64 2d 65 78 63 68  61 6e 67 65 3b 76 3d 62   ned-exch ange;v=b
```

Hypertext Transfer Protocol: Protocol

Packets: 930 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

Task 2: Filter HTTP packets and analyze them.



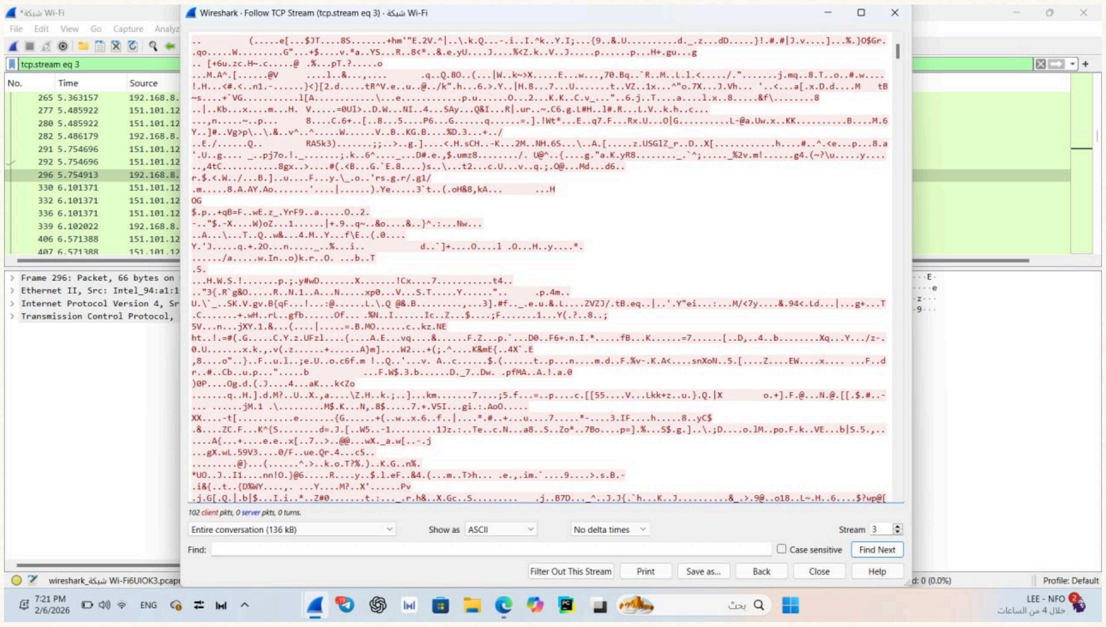
```
Apply a display filter ... <Ctrl-/>

No.   Time       Source           Destination      Protocol Lengtl Info
  919 18.264419  192.168.8.128    151.101.122.172  TCP        66 1989 → 80 [ACK] Seq=1 Ack=135661 Win=10 Len=0 TSval=1880058563 TSecr=3656549606
  920 18.264606  151.101.122.172  192.168.8.128    TCP      1238 80 → 1989 [PSH, ACK] Seq=135661 Ack=1 Win=287 Len=1172 TSval=3656549606 TSecr=1880058447
  921 18.339192  151.101.122.172  192.168.8.128    TCP      1454 80 → 1990 [ACK] Seq=147545 Ack=1 Win=287 Len=1388 TSval=3446997324 TSecr=1880058447
  922 18.339192  151.101.122.172  192.168.8.128    TCP      1238 80 → 1990 [PSH, ACK] Seq=148933 Ack=1 Win=287 Len=1172 TSval=3446997324 TSecr=1880058447
  923 18.339192  151.101.122.172  192.168.8.128    TCP      1454 80 → 1991 [ACK] Seq=146705 Ack=1 Win=287 Len=1388 TSval=2265762120 TSecr=1880058447
  924 18.339275  192.168.8.128    151.101.122.172  TCP        66 1990 → 80 [ACK] Seq=1 Ack=150105 Win=10 Len=0 TSval=1880058638 TSecr=3446997324
  925 18.339328  192.168.8.128    151.101.122.172  TCP        66 1991 → 80 [ACK] Seq=1 Ack=148093 Win=10 Len=0 TSval=1880058638 TSecr=2265762120
  926 18.340471  151.101.122.172  192.168.8.128    TCP      1238 80 → 1991 [PSH, ACK] Seq=148093 Ack=1 Win=287 Len=1172 TSval=2265762120 TSecr=1880058447
  927 18.341459  151.101.122.172  192.168.8.128    TCP      1454 80 → 1214 [ACK] Seq=147037 Ack=1 Win=287 Len=1388 TSval=2039996042 TSecr=1880058447
  928 18.341515  192.168.8.128    151.101.122.172  TCP        66 1214 → 80 [ACK] Seq=1 Ack=148425 Win=10 Len=0 TSval=1880058640 TSecr=2039996042
  929 18.346380  151.101.122.172  192.168.8.128    TCP      1238 80 → 1214 [PSH, ACK] Seq=148425 Ack=1 Win=287 Len=1172 TSval=2039996042 TSecr=1880058447
  930 18.768066  151.101.122.172  192.168.8.128    TCP      1454 80 → 1990 [ACK] Seq=150105 Ack=1 Win=287 Len=1388 TSval=3446997510 TSecr=1880058638

> Frame 1: Packet, 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{68E
> Ethernet II, Src: ca:1f:f9:24:20:95 (ca:1f:f9:24:20:95), Dst: Intel_94:a1:1f (f4:3b:d8:94:a1:1f)
> Internet Protocol Version 4, Src: 192.168.8.106, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

wireshark_شبكة Wi-Fi6UIOK3.pcapng    Packets: 930 · Dropped: 0 (0.0%)    Profile: Default
```

*شبكة Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
7:16 PM 2/6/2026
ENG
بحث
NASDAQ 1.44%+

In this task, HTTP packets were filtered using Wireshark. The captured packets show an HTTP GET request sent from the client to the server and the corresponding HTTP response. The request includes the requested URL and headers such as Host and User-Agent. The server response shows the HTTP status code (304 Not Modified), indicating that the requested resource has not changed. This demonstrates how HTTP communication occurs over TCP.

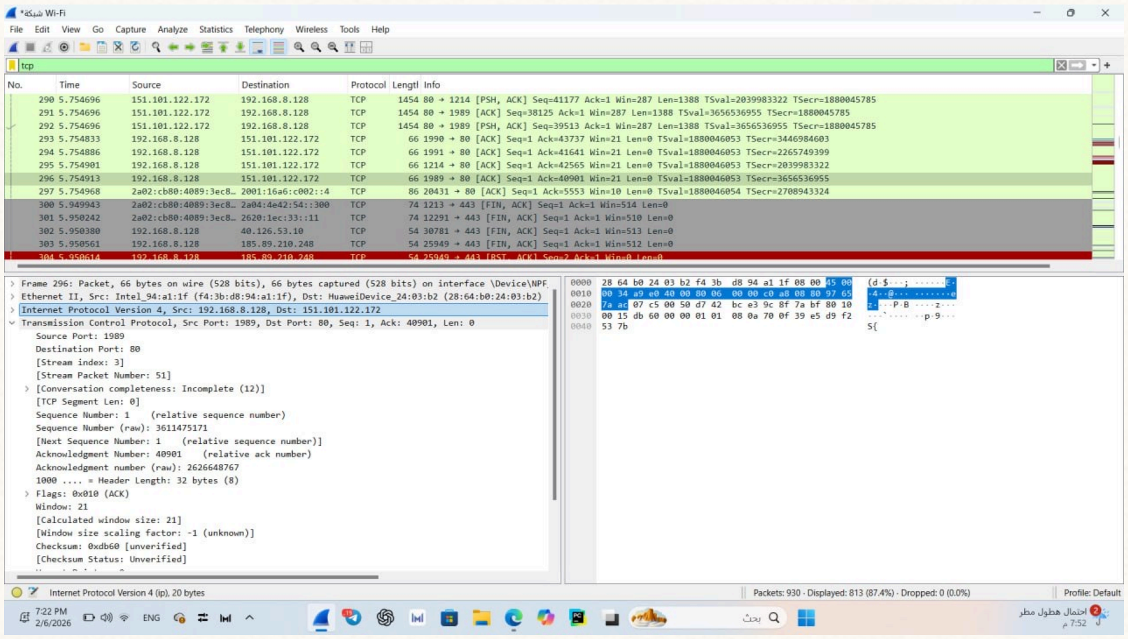
Part 2: Analyzing TCP/IP Traffic.

Task 1: Filter TCP packets



```
tcp.stream eq 3

No.   Time       Source
  265 5.363157   192.168.8.
  277 5.485922   151.101.12
  280 5.485922   151.101.12
  282 5.486179   192.168.8.
  291 5.754696   151.101.12
  292 5.754696   151.101.12
  296 5.754913   192.168.8.
  330 6.101371   151.101.12
  332 6.101371   151.101.12
  336 6.101371   151.101.12
  339 6.102022   192.168.8.
  406 6.571388   151.101.12
  407 6.571388   151.101.12

> Frame 296: Packet, 66 bytes on
> Ethernet II, Src: Intel_94:a1:1
> Internet Protocol Version 4, Sr
> Transmission Control Protocol,
```

```
Wireshark · Follow TCP Stream (tcp.stream eq 3) · شبكة Wi-Fi

[illegible]

102 client pkts, 0 server pkts, 0 turns.

Entire conversation (136 kB)    Show as ASCII    No delta times    Stream 3
Find:    Case sensitive    Find Next
Filter Out This Stream  Print  Save as...  Back  Close  Help
```

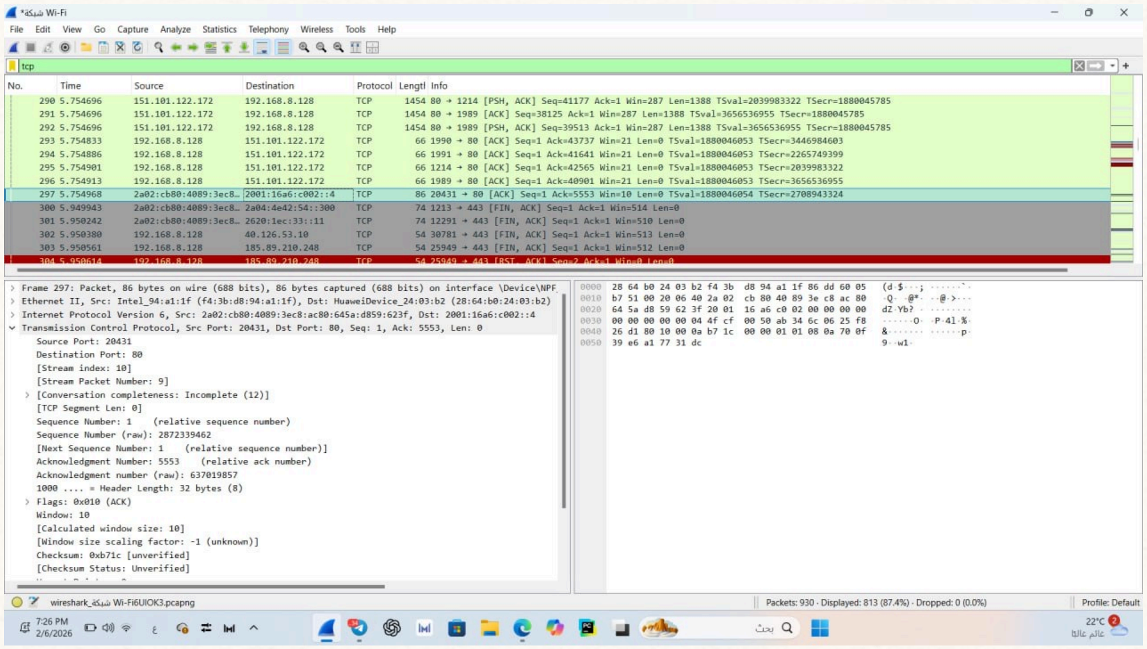

*شبكة Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time      Source               Destination        Protocol Lengtl Info
  290 5.754696  151.101.122.172      192.168.8.128      TCP      1454 80 → 1214 [PSH, ACK] Seq=41177 Ack=1 Win=287 Len=1388 TSval=2039983322 TSecr=1880045785
  291 5.754696  151.101.122.172      192.168.8.128      TCP      1454 80 → 1989 [ACK] Seq=38125 Ack=1 Win=287 Len=1388 TSval=3656536955 TSecr=1880045785
  292 5.754696  151.101.122.172      192.168.8.128      TCP      1454 80 → 1989 [PSH, ACK] Seq=39513 Ack=1 Win=287 Len=1388 TSval=3656536955 TSecr=1880045785
  293 5.754833  192.168.8.128        151.101.122.172    TCP        66 1990 → 80 [ACK] Seq=1 Ack=43737 Win=21 Len=0 TSval=1880046053 TSecr=3446984603
  294 5.754886  192.168.8.128        151.101.122.172    TCP        66 1991 → 80 [ACK] Seq=1 Ack=41641 Win=21 Len=0 TSval=1880046053 TSecr=2265749399
  295 5.754901  192.168.8.128        151.101.122.172    TCP        66 1214 → 80 [ACK] Seq=1 Ack=42565 Win=21 Len=0 TSval=1880046053 TSecr=2039983322
  296 5.754913  192.168.8.128        151.101.122.172    TCP        66 1989 → 80 [ACK] Seq=1 Ack=40901 Win=21 Len=0 TSval=1880046053 TSecr=3656536955
  297 5.754968  2a02:cb80:4089:3ec8… 2001:16a6:c002::4  TCP        86 20431 → 80 [ACK] Seq=1 Ack=5553 Win=10 Len=0 TSval=1880046054 TSecr=2708943324
  300 5.949943  2a02:cb80:4089:3ec8… 2a04:4e42:54::300  TCP        74 1213 → 443 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
  301 5.950242  2a02:cb80:4089:3ec8… 2620:1ec:33::11    TCP        74 12291 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  302 5.950380  192.168.8.128        40.126.53.10       TCP        54 30781 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
  303 5.950561  192.168.8.128        185.89.210.248     TCP        54 25949 → 443 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0
  304 5.950614  192.168.8.128        185.89.210.248     TCP        54 25949 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
```

```
> Frame 296: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF
> Ethernet II, Src: Intel_94:a1:1f (f4:3b:d8:94:a1:1f), Dst: HuaweiDevice_24:03:b2 (28:64:b0:24:03:b2)
> Internet Protocol Version 4, Src: 192.168.8.128, Dst: 151.101.122.172
v Transmission Control Protocol, Src Port: 1989, Dst Port: 80, Seq: 1, Ack: 40901, Len: 0
    Source Port: 1989
    Destination Port: 80
    [Stream index: 3]
    [Stream Packet Number: 51]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3611475171
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 40901    (relative ack number)
    Acknowledgment number (raw): 2626648767
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 21
    [Calculated window size: 21]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xdb60 [unverified]
    [Checksum Status: Unverified]
```

```
0000  28 64 b0 24 03 b2 f4 3b  d8 94 a1 1f 08 00 45 00   (d·$···;  ······E·
0010  00 34 a9 e0 40 00 80 06  00 00 c0 a8 08 80 97 65   ·4··@···  ·······e
0020  7a ac 07 c5 00 50 d7 42  bc e3 9c 8f 7a bf 80 10   z····P·B  ····z···
0030  00 15 db 60 00 00 01 01  08 0a 70 0f 39 e5 d9 f2   ···`····  ··p·9···
0040  53 7b                                              S{
```

```
Internet Protocol Version 4 (ip), 20 bytes    Packets: 930 · Displayed: 813 (87.4%) · Dropped: 0 (0.0%)    Profile: Default
7:22 PM 2/6/2026
```


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

```
No.   Time      Source               Destination        Protocol Lengtl Info
  290 5.754696  151.101.122.172      192.168.8.128      TCP      1454 80 → 1214 [PSH, ACK] Seq=41177 Ack=1 Win=287 Len=1388 TSval=2039983322 TSecr=1880045785
  291 5.754696  151.101.122.172      192.168.8.128      TCP      1454 80 → 1989 [ACK] Seq=38125 Ack=1 Win=287 Len=1388 TSval=3656536955 TSecr=1880045785
  292 5.754696  151.101.122.172      192.168.8.128      TCP      1454 80 → 1989 [PSH, ACK] Seq=39513 Ack=1 Win=287 Len=1388 TSval=3656536955 TSecr=1880045785
  293 5.754833  192.168.8.128        151.101.122.172    TCP        66 1990 → 80 [ACK] Seq=1 Ack=43737 Win=21 Len=0 TSval=1880046053 TSecr=3446984603
  294 5.754886  192.168.8.128        151.101.122.172    TCP        66 1991 → 80 [ACK] Seq=1 Ack=41641 Win=21 Len=0 TSval=1880046053 TSecr=2265749399
  295 5.754901  192.168.8.128        151.101.122.172    TCP        66 1214 → 80 [ACK] Seq=1 Ack=42565 Win=21 Len=0 TSval=1880046053 TSecr=2039983322
  296 5.754913  192.168.8.128        151.101.122.172    TCP        66 1989 → 80 [ACK] Seq=1 Ack=40901 Win=21 Len=0 TSval=1880046053 TSecr=3656536955
  297 5.754968  2a02:cb80:4089:3ec8… 2001:16a6:c002::4  TCP        86 20431 → 80 [ACK] Seq=1 Ack=5553 Win=10 Len=0 TSval=1880046054 TSecr=2708943324
  300 5.949943  2a02:cb80:4089:3ec8… 2a04:4e42:54::300  TCP        74 1213 → 443 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
  301 5.950242  2a02:cb80:4089:3ec8… 2620:1ec:33::11    TCP        74 12291 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  302 5.950380  192.168.8.128        40.126.53.10       TCP        54 30781 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
  303 5.950561  192.168.8.128        185.89.210.248     TCP        54 25949 → 443 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0
  304 5.950614  192.168.8.128        185.89.210.248     TCP        54 25949 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
```

```
> Frame 297: Packet, 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF
> Ethernet II, Src: Intel_94:a1:1f (f4:3b:d8:94:a1:1f), Dst: HuaweiDevice_24:03:b2 (28:64:b0:24:03:b2)
> Internet Protocol Version 6, Src: 2a02:cb80:4089:3ec8:ac80:645a:d859:623f, Dst: 2001:16a6:c002::4
v Transmission Control Protocol, Src Port: 20431, Dst Port: 80, Seq: 1, Ack: 5553, Len: 0
    Source Port: 20431
    Destination Port: 80
    [Stream index: 10]
    [Stream Packet Number: 9]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2872339462
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 5553    (relative ack number)
    Acknowledgment number (raw): 637019857
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 10
    [Calculated window size: 10]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xb71c [unverified]
    [Checksum Status: Unverified]
```

```
0000  28 64 b0 24 03 b2 f4 3b  d8 94 a1 1f 86 dd 60 05   (d·$···;  ······`·
0010  b7 51 00 20 06 40 2a 02  cb 80 40 89 3e c8 ac 80   ·Q· ·@*·  ··@·>···
0020  64 5a d8 59 62 3f 20 01  16 a6 c0 02 00 00 00 00   dZ·Yb? ·  ········
0030  00 00 00 00 00 04 4f cf  00 50 ab 34 6c 06 25 f8   ······O·  ·P·4l·%·
0040  26 d1 80 10 00 0a b7 1c  00 00 01 01 08 0a 70 0f   &·······  ······p·
0050  39 e6 a1 77 31 dc                                  9··w1·
```

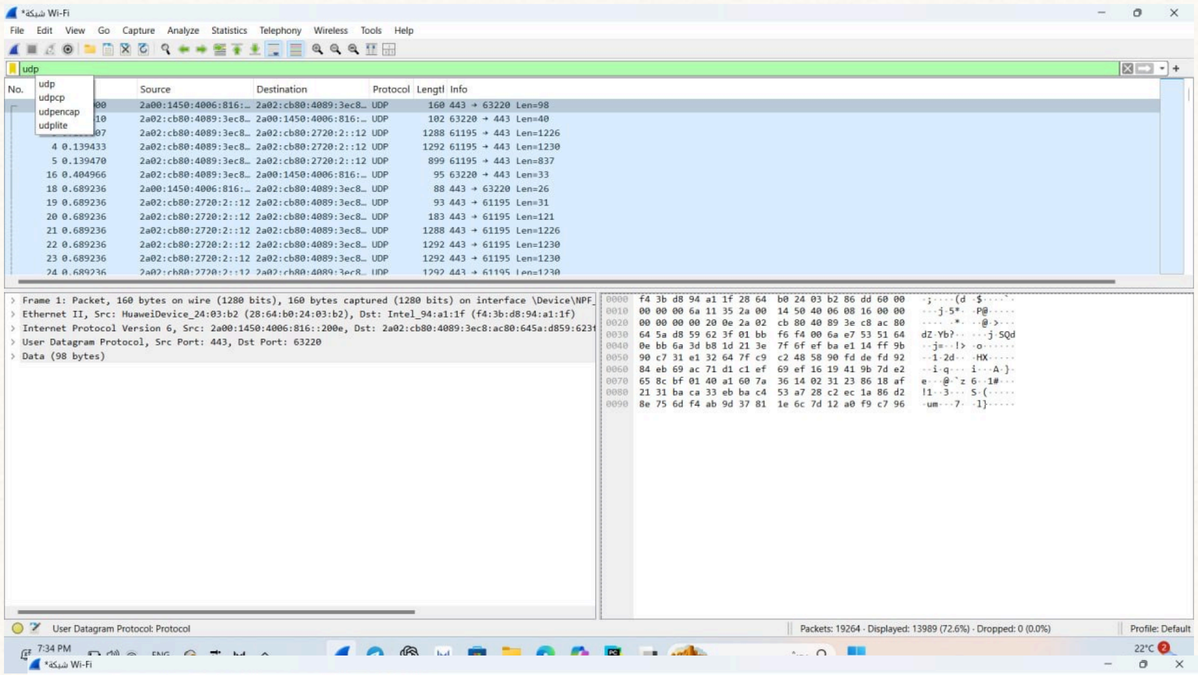
```
wireshark_شبكة Wi-Fi6UIOK3.pcapng    Packets: 930 · Displayed: 813 (87.4%) · Dropped: 0 (0.0%)    Profile: Default
7:26 PM 2/6/2026
```

In this part, TCP packets were filtered and analyzed using Wireshark. The TCP three-way handshake was observed, where the connection is established using SYN, SYN-ACK, and ACK packets. Sequence and acknowledgment numbers were examined to understand how TCP ensures reliable data delivery. Data transfer packets (PSH, ACK) were also captured, showing the exchange of data between the client and the server. Finally, the TCP connection termination process was observed through FIN and ACK packets, confirming the reliable and connection-oriented nature of TCP.

Part 3: Capturing and Analyzing UDP Traffic

Task 1: Generate UDP traffic and capture packets

Task 2: Filter and analysis UDP Packets


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

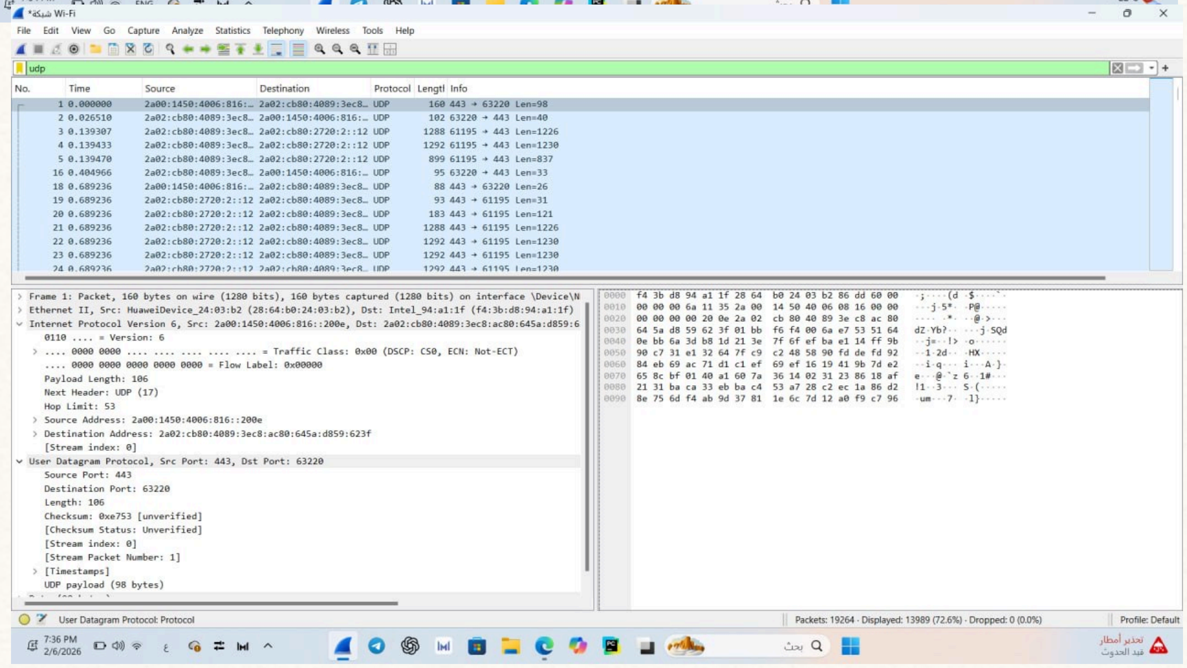
```
No.   Time       Source                Destination           Protocol Lengtl Info
      ...00      2a00:1450:4006:816:…  2a02:cb80:4089:3ec8…  UDP       160 443 → 63220 Len=98
      ...10      2a02:cb80:4089:3ec8…  2a00:1450:4006:816:…  UDP       102 63220 → 443 Len=40
      ...07      2a02:cb80:4089:3ec8…  2a02:cb80:2720:2::12  UDP      1288 61195 → 443 Len=1226
    4 0.139433   2a02:cb80:4089:3ec8…  2a02:cb80:2720:2::12  UDP      1292 61195 → 443 Len=1230
    5 0.139470   2a02:cb80:4089:3ec8…  2a02:cb80:2720:2::12  UDP       899 61195 → 443 Len=837
   16 0.404966   2a02:cb80:4089:3ec8…  2a00:1450:4006:816:…  UDP        95 63220 → 443 Len=33
   18 0.689236   2a00:1450:4006:816:…  2a02:cb80:4089:3ec8…  UDP        88 443 → 63220 Len=26
   19 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP        93 443 → 61195 Len=31
   20 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP       183 443 → 61195 Len=121
   21 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP      1288 443 → 61195 Len=1226
   22 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP      1292 443 → 61195 Len=1230
   23 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP      1292 443 → 61195 Len=1230
   24 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP      1292 443 → 61195 Len=1230
```

```
> Frame 1: Packet, 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_
> Ethernet II, Src: HuaweiDevice_24:03:b2 (28:64:b0:24:03:b2), Dst: Intel_94:a1:1f (f4:3b:d8:94:a1:1f)
> Internet Protocol Version 6, Src: 2a00:1450:4006:816::200e, Dst: 2a02:cb80:4089:3ec8:ac80:645a:d859:623f
> User Datagram Protocol, Src Port: 443, Dst Port: 63220
> Data (98 bytes)
```

```
0000  f4 3b d8 94 a1 1f 28 64  b0 24 03 b2 86 dd 60 00   ·;····(d ·$····`·
0010  00 00 00 6a 11 35 2a 00  14 50 40 06 08 16 00 00   ···j·5*· ·P@·····
0020  00 00 00 00 20 0e 2a 02  cb 80 40 89 3e c8 ac 80   ···· ·*· ··@·>···
0030  64 5a d8 59 62 3f 01 bb  f6 f4 00 6a e7 53 51 64   dZ·Yb?·· ···j·SQd
0040  0e bb 6a 3d b8 1d 21 3e  7f 6f ef ba e1 14 ff 9b   ··j=··!> ·o······
0050  90 c7 31 e1 32 64 7f c9  c2 48 58 90 fd de fd 92   ··1·2d·· ·HX·····
0060  84 eb 69 ac 71 d1 c1 ef  69 ef 16 19 41 9b 7d e2   ··i·q··· i···A·}·
0070  65 8c bf 01 40 a1 60 7a  36 14 02 31 23 86 18 af   e···@·`z 6··1#···
0080  21 31 ba ca 33 eb ba c4  53 a7 28 c2 ec 1a 86 d2   !1··3··· S·(·····
0090  8e 75 6d f4 ab 9d 37 81  1e 6c 7d 12 a0 f9 c7 96   ·um···7· ·l}·····
```

User Datagram Protocol: Protocol | Packets: 19264 · Displayed: 13989 (72.6%) · Dropped: 0 (0.0%) | Profile: Default

7:34 PM 22°C


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

```
No.   Time       Source                Destination           Protocol Lengtl Info
    1 0.000000   2a00:1450:4006:816:…  2a02:cb80:4089:3ec8…  UDP       160 443 → 63220 Len=98
    2 0.026510   2a02:cb80:4089:3ec8…  2a00:1450:4006:816:…  UDP       102 63220 → 443 Len=40
    3 0.139307   2a02:cb80:4089:3ec8…  2a02:cb80:2720:2::12  UDP      1288 61195 → 443 Len=1226
    4 0.139433   2a02:cb80:4089:3ec8…  2a02:cb80:2720:2::12  UDP      1292 61195 → 443 Len=1230
    5 0.139470   2a02:cb80:4089:3ec8…  2a02:cb80:2720:2::12  UDP       899 61195 → 443 Len=837
   16 0.404966   2a02:cb80:4089:3ec8…  2a00:1450:4006:816:…  UDP        95 63220 → 443 Len=33
   18 0.689236   2a00:1450:4006:816:…  2a02:cb80:4089:3ec8…  UDP        88 443 → 63220 Len=26
   19 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP        93 443 → 61195 Len=31
   20 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP       183 443 → 61195 Len=121
   21 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP      1288 443 → 61195 Len=1226
   22 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP      1292 443 → 61195 Len=1230
   23 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP      1292 443 → 61195 Len=1230
   24 0.689236   2a02:cb80:2720:2::12  2a02:cb80:4089:3ec8…  UDP      1292 443 → 61195 Len=1230
```

```
> Frame 1: Packet, 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\N
> Ethernet II, Src: HuaweiDevice_24:03:b2 (28:64:b0:24:03:b2), Dst: Intel_94:a1:1f (f4:3b:d8:94:a1:1f)
v Internet Protocol Version 6, Src: 2a00:1450:4006:816::200e, Dst: 2a02:cb80:4089:3ec8:ac80:645a:d859:6
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 106
    Next Header: UDP (17)
    Hop Limit: 53
  > Source Address: 2a00:1450:4006:816::200e
  > Destination Address: 2a02:cb80:4089:3ec8:ac80:645a:d859:623f
    [Stream index: 0]
v User Datagram Protocol, Src Port: 443, Dst Port: 63220
    Source Port: 443
    Destination Port: 63220
    Length: 106
    Checksum: 0xe753 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (98 bytes)
```

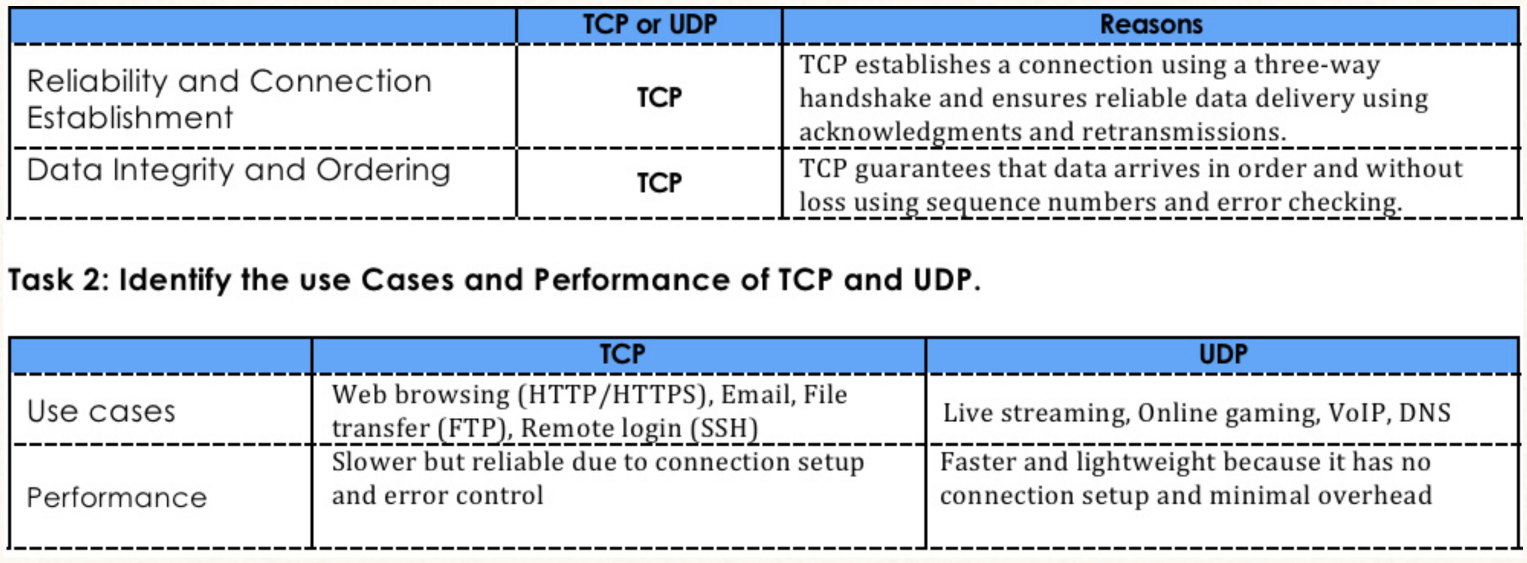
```
0000  f4 3b d8 94 a1 1f 28 64  b0 24 03 b2 86 dd 60 00   ·;····(d ·$····`·
0010  00 00 00 6a 11 35 2a 00  14 50 40 06 08 16 00 00   ···j·5*· ·P@·····
0020  00 00 00 00 20 0e 2a 02  cb 80 40 89 3e c8 ac 80   ···· ·*· ··@·>···
0030  64 5a d8 59 62 3f 01 bb  f6 f4 00 6a e7 53 51 64   dZ·Yb?·· ···j·SQd
0040  0e bb 6a 3d b8 1d 21 3e  7f 6f ef ba e1 14 ff 9b   ··j=··!> ·o······
0050  90 c7 31 e1 32 64 7f c9  c2 48 58 90 fd de fd 92   ··1·2d·· ·HX·····
0060  84 eb 69 ac 71 d1 c1 ef  69 ef 16 19 41 9b 7d e2   ··i·q··· i···A·}·
0070  65 8c bf 01 40 a1 60 7a  36 14 02 31 23 86 18 af   e···@·`z 6··1#···
0080  21 31 ba ca 33 eb ba c4  53 a7 28 c2 ec 1a 86 d2   !1··3··· S·(·····
0090  8e 75 6d f4 ab 9d 37 81  1e 6c 7d 12 a0 f9 c7 96   ·um···7· ·l}·····
```

User Datagram Protocol: Protocol | Packets: 19264 · Displayed: 13989 (72.6%) · Dropped: 0 (0.0%) | Profile: Default

7:36 PM 2/6/2026 بحث تحذير أمطار قيد الحدوث

After applying the filter udp in the filter bar, Wireshark displays only UDP packets from the capture.
By selecting one of the UDP packets, we can observe:
Source Port: 443
Destination Port: 63220
UDP Length: 106 bytes
The UDP header contains only essential information: source port, destination port, length, and checksum, which shows the simplicity of this protocol.

Part 4:



	TCP or UDP	Reasons
Reliability and Connection Establishment	TCP	TCP establishes a connection using a three-way handshake and ensures reliable data delivery using acknowledgments and retransmissions.
Data Integrity and Ordering	TCP	TCP guarantees that data arrives in order and without loss using sequence numbers and error checking.

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

	TCP	UDP
Use cases	Web browsing (HTTP/HTTPS), Email, File transfer (FTP), Remote login (SSH)	Live streaming, Online gaming, VoIP, DNS
Performance	Slower but reliable due to connection setup and error control	Faster and lightweight because it has no connection setup and minimal overhead