CS471 – Web Technologies (Laboratory)	Qassim University جامعة القصيم College of Computer | كلية الحاسب	Lab Week 2
		The Internet Protocols

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 (https://qu.edu.sa) 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:
- SYN: Initiates a connection.
- SYN-ACK: Acknowledges and responds to the SYN.
- 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.

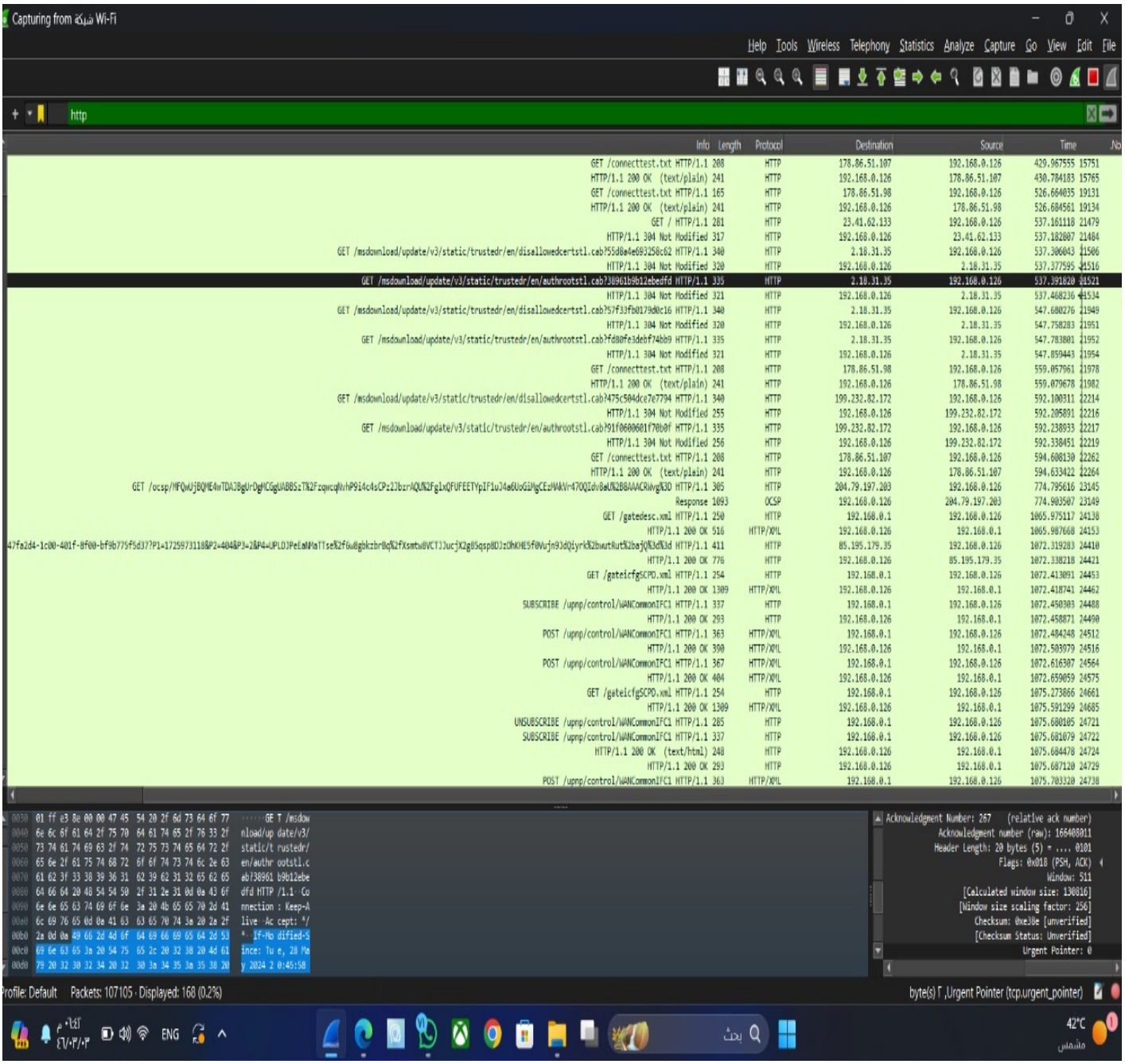
Part 4: Comparing TCP and UDP by filling in the following tables. Save your work (e.g., in an MS Word document), and upload it to your online git repo.

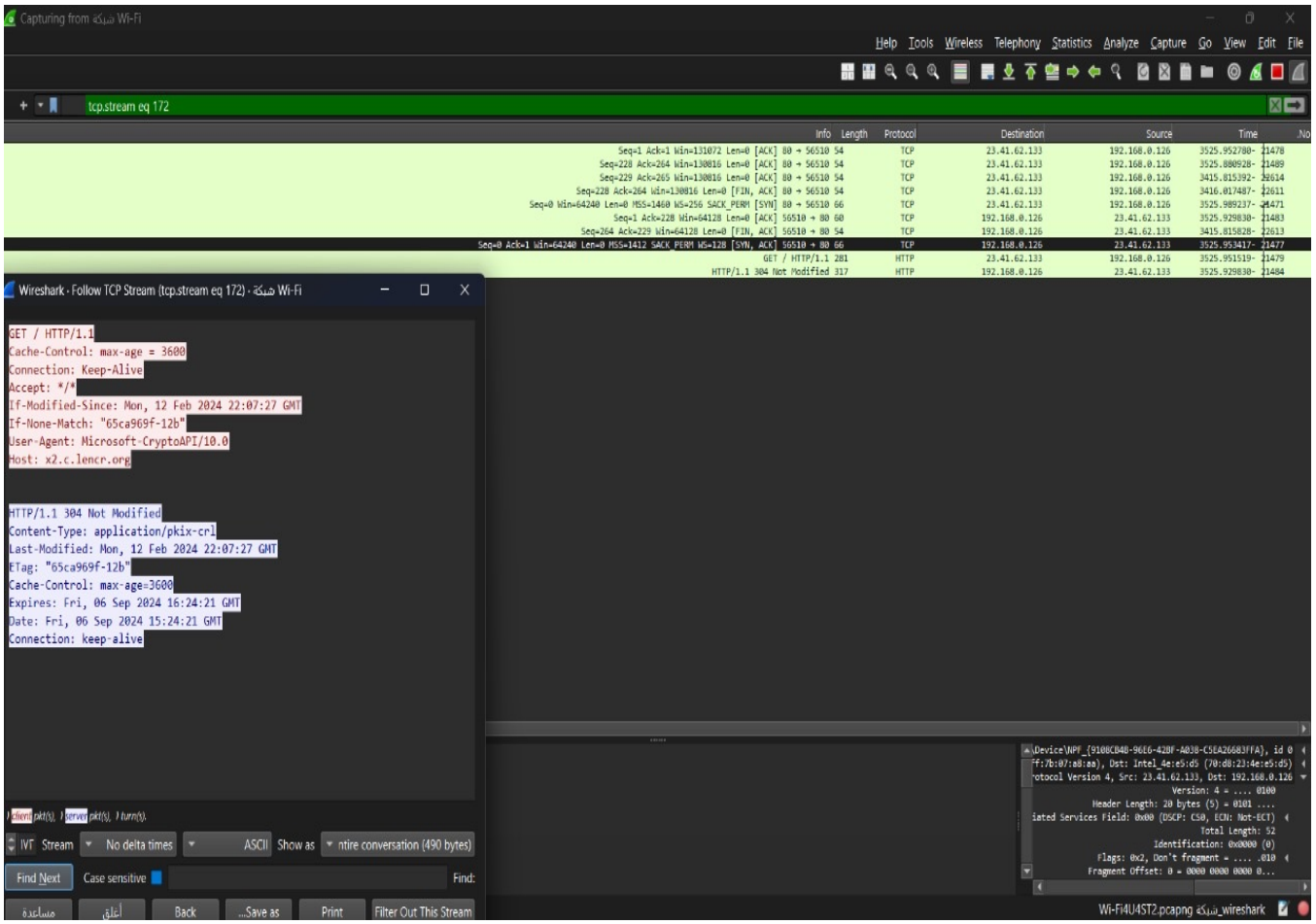
Task 1: Fill in the following table and provide reasons.

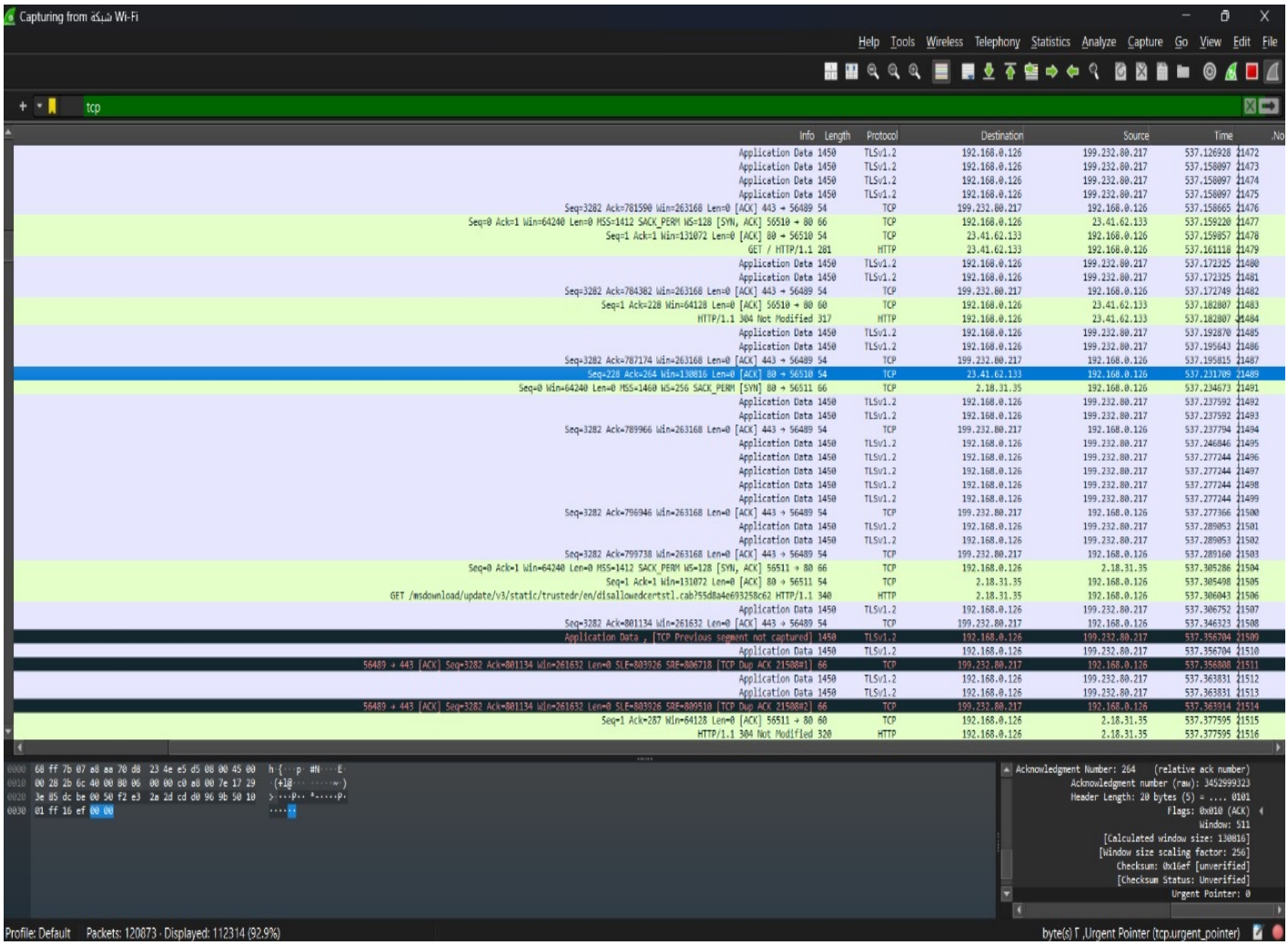
	TCP or UDP	Reasons
Reliability and Connection Establishment	TCP	is reliable because it uses a three-way handshake to establish a connection and ensures data delivery.
Data Integrity and Ordering	UDP	is unreliable because it does not use a handshake mechanism and does not guarantee data delivery or ordering.

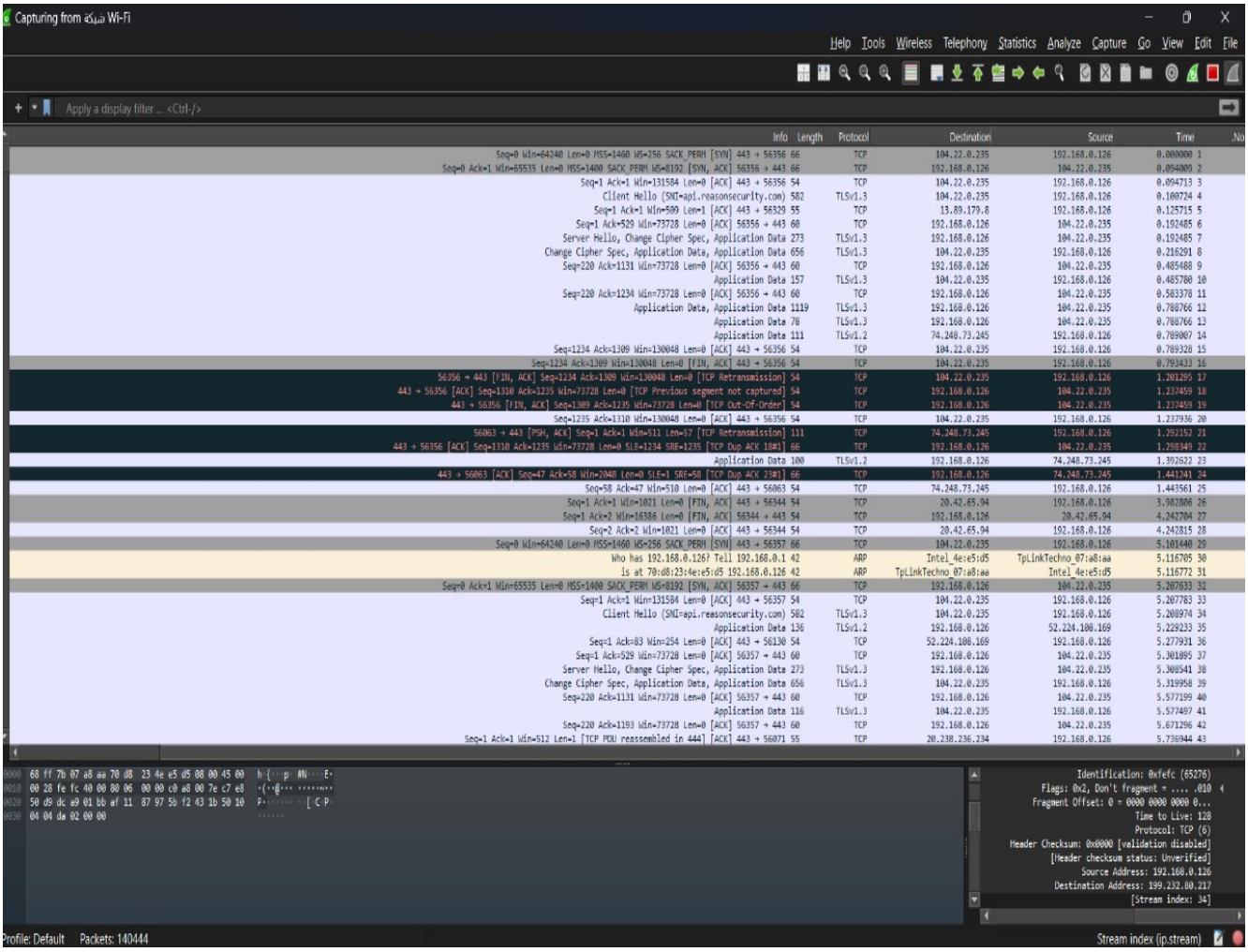
Task 2: Identify the use Cases and Performance of TCP and UDP.

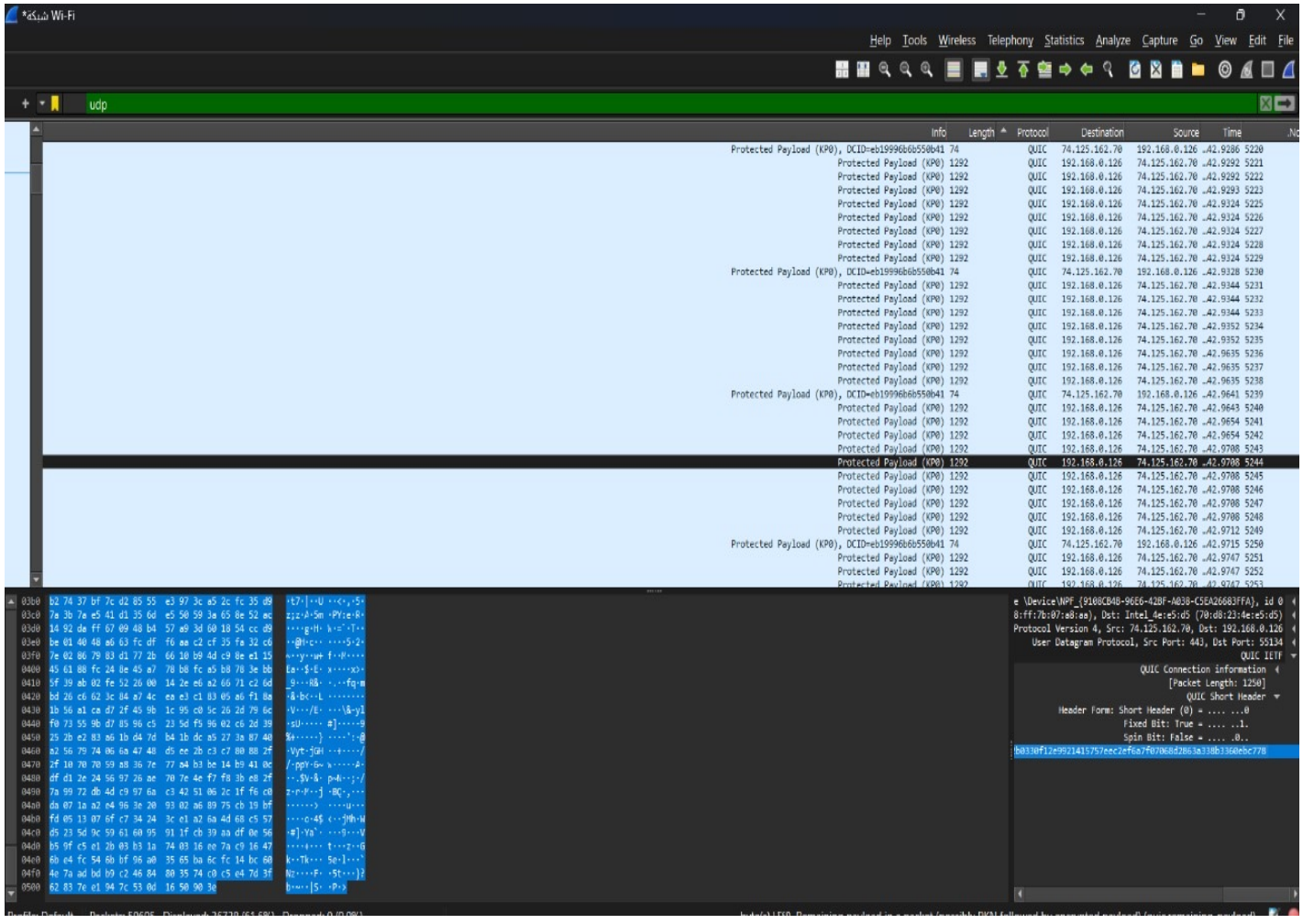
	TCP	UDP
Use cases		
Performance		


Capturing from شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
http
Info Length Protocol Destination Source Time No
GET /connecttest.txt HTTP/1.1 208 HTTP 178.86.51.107 192.168.0.126 429.967555 15751
HTTP/1.1 200 OK (text/plain) 241 HTTP 192.168.0.126 178.86.51.107 430.784183 15765
GET /connecttest.txt HTTP/1.1 165 HTTP 178.86.51.98 192.168.0.126 526.664035 19131
HTTP/1.1 200 OK (text/plain) 241 HTTP 192.168.0.126 178.86.51.98 526.684561 19134
GET / HTTP/1.1 281 HTTP 23.41.62.133 192.168.0.126 537.161118 21479
HTTP/1.1 304 Not Modified 317 HTTP 192.168.0.126 23.41.62.133 537.182807 21484
GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?55d8a4e693258c62 HTTP/1.1 340 HTTP 2.18.31.35 192.168.0.126 537.306043 21506
HTTP/1.1 304 Not Modified 320 HTTP 192.168.0.126 2.18.31.35 537.377595 21516
GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?38961b9b12ebedfd HTTP/1.1 335 HTTP 2.18.31.35 192.168.0.126 537.391820 21521
HTTP/1.1 304 Not Modified 321 HTTP 192.168.0.126 2.18.31.35 537.468236 21534
GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?57f33fb0179d0c16 HTTP/1.1 340 HTTP 2.18.31.35 192.168.0.126 547.680276 21949
HTTP/1.1 304 Not Modified 320 HTTP 192.168.0.126 2.18.31.35 547.758283 21951
GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?fd80fe3debf74bb9 HTTP/1.1 335 HTTP 2.18.31.35 192.168.0.126 547.783801 21952
HTTP/1.1 304 Not Modified 321 HTTP 192.168.0.126 2.18.31.35 547.859443 21954
GET /connecttest.txt HTTP/1.1 208 HTTP 178.86.51.98 192.168.0.126 559.057961 21978
HTTP/1.1 200 OK (text/plain) 241 HTTP 192.168.0.126 178.86.51.98 559.079678 21982
GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?475c504dce7e7794 HTTP/1.1 340 HTTP 199.232.82.172 192.168.0.126 592.100311 22214
HTTP/1.1 304 Not Modified 255 HTTP 192.168.0.126 199.232.82.172 592.205891 22216
GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?91f0600601f70b0f HTTP/1.1 335 HTTP 199.232.82.172 192.168.0.126 592.238933 22217
HTTP/1.1 304 Not Modified 256 HTTP 192.168.0.126 199.232.82.172 592.338451 22219
GET /connecttest.txt HTTP/1.1 208 HTTP 178.86.51.107 192.168.0.126 594.608130 22262
HTTP/1.1 200 OK (text/plain) 241 HTTP 192.168.0.126 178.86.51.107 594.633422 22264
GET /ocsp/MFQwUjBQME4wTDAJBgUrDgMCGgUABBSzTk2FzqvcqNvhP9i4c4sCPz2bzrAQUk2FglxQFUFEETYpIF1uJ4a6UoGiNgCEzHAkVr47OQIdv8eU%2B8AAACRAvgA3D HTTP/1.1 305 HTTP 204.79.197.203 192.168.0.126 774.795616 23145
Response 1093 OCSP 192.168.0.126 204.79.197.203 774.903507 23149
GET /gatedesc.xml HTTP/1.1 250 HTTP 192.168.0.1 192.168.0.126 1065.975117 24138
HTTP/1.1 200 OK 516 HTTP/XML 192.168.0.126 192.168.0.1 1065.987668 24153
47fa2d4-1c00-401f-8f00-bf9b775f5d37?P1=1725973118&P2=404&P3=2&P4=UPLDJPeEaWaTTseK2f6u8gbkzbr8qK2fXsmtu8VCTJJucjX2g85qsp8DJzOhKHE5f0Vujn9JdQiyrk%2bwutKut%2baJQ%3d%3d HTTP/1.1 411 HTTP 85.195.179.35 192.168.0.126 1072.319283 24410
HTTP/1.1 200 OK 776 HTTP 192.168.0.126 85.195.179.35 1072.338218 24421
GET /gateicfgSCPD.xml HTTP/1.1 254 HTTP 192.168.0.1 192.168.0.126 1072.413091 24453
HTTP/1.1 200 OK 1309 HTTP/XML 192.168.0.126 192.168.0.1 1072.418741 24462
SUBSCRIBE /upnp/control/WANCommonIFC1 HTTP/1.1 337 HTTP 192.168.0.1 192.168.0.126 1072.450303 24488
HTTP/1.1 200 OK 293 HTTP 192.168.0.126 192.168.0.1 1072.458871 24490
POST /upnp/control/WANCommonIFC1 HTTP/1.1 363 HTTP/XML 192.168.0.1 192.168.0.126 1072.484248 24512
HTTP/1.1 200 OK 390 HTTP/XML 192.168.0.126 192.168.0.1 1072.503979 24516
POST /upnp/control/WANCommonIFC1 HTTP/1.1 367 HTTP/XML 192.168.0.1 192.168.0.126 1072.616307 24564
HTTP/1.1 200 OK 404 HTTP/XML 192.168.0.126 192.168.0.1 1072.659059 24575
GET /gateicfgSCPD.xml HTTP/1.1 254 HTTP 192.168.0.1 192.168.0.126 1075.273866 24661
HTTP/1.1 200 OK 1309 HTTP/XML 192.168.0.126 192.168.0.1 1075.591299 24685
UNSUBSCRIBE /upnp/control/WANCommonIFC1 HTTP/1.1 285 HTTP 192.168.0.1 192.168.0.126 1075.680105 24721
SUBSCRIBE /upnp/control/WANCommonIFC1 HTTP/1.1 337 HTTP 192.168.0.1 192.168.0.126 1075.681079 24722
HTTP/1.1 200 OK (text/html) 248 HTTP 192.168.0.126 192.168.0.1 1075.684478 24724
HTTP/1.1 200 OK 293 HTTP 192.168.0.126 192.168.0.1 1075.687120 24729
POST /upnp/control/WANCommonIFC1 HTTP/1.1 363 HTTP/XML 192.168.0.1 192.168.0.126 1075.703320 24738
0030 01 ff e3 8e 00 00 47 45 54 20 2f 6d 73 64 6f 77 ····· GE T /msdow
0040 6e 6c 6f 61 64 2f 75 70 64 61 74 65 2f 76 33 2f nload/up date/v3/
0050 73 74 61 74 69 63 2f 74 72 75 73 74 65 64 72 2f static/t rustedr/
0060 65 6e 2f 61 75 74 68 72 6f 6f 74 73 74 6c 2e 63 en/authr ootstl.c
0070 61 62 3f 33 38 39 36 31 62 39 62 31 32 65 62 65 ab?38961 b9b12ebe
0080 64 66 64 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f dfd HTTP /1.1 · Co
0090 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 nnection : Keep-A
00a0 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f live · Ac cept: */
00b0 2a 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 * · If-Mo dified-S
00c0 69 6e 63 65 3a 20 54 75 65 2c 20 32 38 20 4d 61 ince: Tu e, 28 Ma
00d0 79 20 32 30 32 34 20 32 30 3a 34 35 3a 35 38 20 y 2024 2 0:45:58
Acknowledgement Number: 267 (relative ack number)
Acknowledgment number (raw): 166408011
Header Length: 20 bytes (5) = ... 0101
Flags: 0x018 (PSH, ACK)
Window: 511
[Calculated window size: 130816]
[Window size scaling factor: 256]
Checksum: 0xe30e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Profile: Default Packets: 107105 · Displayed: 168 (0.2%)
byte(s) T ,Urgent Pointer (tcp.urgent_pointer)
ENG
بحث
42°C
مشمس


Capturing from شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
tcp.stream eq 172
Info Length Protocol Destination Source Time .No
Seq=1 Ack=1 Win=131072 Len=0 [ACK] 80 → 56510 54 TCP 23.41.62.133 192.168.0.126 3525.952780- 21478
Seq=228 Ack=264 Win=130816 Len=0 [ACK] 80 → 56510 54 TCP 23.41.62.133 192.168.0.126 3525.880928- 21489
Seq=229 Ack=265 Win=130816 Len=0 [ACK] 80 → 56510 54 TCP 23.41.62.133 192.168.0.126 3415.815392- 21614
Seq=228 Ack=264 Win=130816 Len=0 [FIN, ACK] 80 → 56510 54 TCP 23.41.62.133 192.168.0.126 3416.017487- 21611
Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 56510 66 TCP 23.41.62.133 192.168.0.126 3525.989237- 21471
Seq=1 Ack=228 Win=64128 Len=0 [ACK] 56510 → 80 60 TCP 192.168.0.126 23.41.62.133 3525.929830- 21483
Seq=264 Ack=229 Win=64128 Len=0 [FIN, ACK] 56510 → 80 54 TCP 192.168.0.126 23.41.62.133 3415.815828- 21613
Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128 [SYN, ACK] 56510 → 80 66 TCP 192.168.0.126 23.41.62.133 3525.953417- 21477
GET / HTTP/1.1 281 HTTP 23.41.62.133 192.168.0.126 3525.951519- 21479
HTTP/1.1 304 Not Modified 317 HTTP 192.168.0.126 23.41.62.133 3525.929830- 21484
Wireshark · Follow TCP Stream (tcp.stream eq 172) · شبكة Wi-Fi
GET / HTTP/1.1
Cache-Control: max-age = 3600
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Mon, 12 Feb 2024 22:07:27 GMT
If-None-Match: "65ca969f-12b"
User-Agent: Microsoft-CryptoAPI/10.0
Host: x2.c.lencr.org
HTTP/1.1 304 Not Modified
Content-Type: application/pkix-crl
Last-Modified: Mon, 12 Feb 2024 22:07:27 GMT
ETag: "65ca969f-12b"
Cache-Control: max-age=3600
Expires: Fri, 06 Sep 2024 16:24:21 GMT
Date: Fri, 06 Sep 2024 15:24:21 GMT
Connection: keep-alive
client pkt(s), 1 server pkt(s), 1 turn(s).
Entire Stream No delta times ASCII Show as ntire conversation (490 bytes)
Find Next Case sensitive Find:
مساعدة إغلاق Back Save as Print Filter Out This Stream
Wi-Fi4U4ST2.pcapng شبكة_wireshark


Capturing from شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
tcp
Info Length Protocol Destination Source Time .No
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.126928 21472
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.158097 21473
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.158097 21474
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.158097 21475
Seq=3282 Ack=781590 Win=263168 Len=0 [ACK] 443 → 56489 54 TCP 199.232.80.217 192.168.0.126 537.158665 21476
Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128 [SYN, ACK] 56510 → 80 66 TCP 192.168.0.126 23.41.62.133 537.159220 21477
Seq=1 Ack=1 Win=131072 Len=0 [ACK] 80 → 56510 54 TCP 23.41.62.133 192.168.0.126 537.159857 21478
GET / HTTP/1.1 281 HTTP 23.41.62.133 192.168.0.126 537.161116 21479
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.172325 21480
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.172325 21481
Seq=3282 Ack=784382 Win=263168 Len=0 [ACK] 443 → 56489 54 TCP 199.232.80.217 192.168.0.126 537.172749 21482
Seq=1 Ack=228 Win=64128 Len=0 [ACK] 56510 → 80 60 TCP 192.168.0.126 23.41.62.133 537.182807 21483
HTTP/1.1 304 Not Modified 317 HTTP 192.168.0.126 23.41.62.133 537.182807 21484
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.192870 21485
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.195643 21486
Seq=3282 Ack=787174 Win=263168 Len=0 [ACK] 443 → 56489 54 TCP 199.232.80.217 192.168.0.126 537.195815 21487
Seq=228 Ack=264 Win=130816 Len=0 [ACK] 80 → 56510 54 TCP 23.41.62.133 192.168.0.126 537.231709 21489
Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 56511 66 TCP 2.18.31.35 192.168.0.126 537.234673 21491
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.237592 21492
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.237592 21493
Seq=3282 Ack=789966 Win=263168 Len=0 [ACK] 443 → 56489 54 TCP 199.232.80.217 192.168.0.126 537.237794 21494
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.246846 21495
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.277244 21496
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.277244 21497
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.277244 21498
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.277244 21499
Seq=3282 Ack=796946 Win=263168 Len=0 [ACK] 443 → 56489 54 TCP 199.232.80.217 192.168.0.126 537.277366 21500
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.289053 21501
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.289053 21502
Seq=3282 Ack=799738 Win=263168 Len=0 [ACK] 443 → 56489 54 TCP 199.232.80.217 192.168.0.126 537.289160 21503
Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128 [SYN, ACK] 56511 → 80 66 TCP 192.168.0.126 2.18.31.35 537.305286 21504
Seq=1 Ack=1 Win=131072 Len=0 [ACK] 80 → 56511 54 TCP 2.18.31.35 192.168.0.126 537.305498 21505
GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?55d8a4e693258c62 HTTP/1.1 340 HTTP 2.18.31.35 192.168.0.126 537.306043 21506
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.306752 21507
Seq=3282 Ack=801134 Win=261632 Len=0 [ACK] 443 → 56489 54 TCP 199.232.80.217 192.168.0.126 537.346323 21508
Application Data , [TCP Previous segment not captured] 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.356704 21509
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.356704 21510
56489 → 443 [ACK] Seq=3282 Ack=801134 Win=261632 Len=0 SLE=803926 SRE=806718 [TCP Dup ACK 21508#1] 66 TCP 199.232.80.217 192.168.0.126 537.356808 21511
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.363831 21512
Application Data 1450 TLSv1.2 192.168.0.126 199.232.80.217 537.363831 21513
56489 → 443 [ACK] Seq=3282 Ack=801134 Win=261632 Len=0 SLE=803926 SRE=809510 [TCP Dup ACK 21508#2] 66 TCP 199.232.80.217 192.168.0.126 537.363914 21514
Seq=1 Ack=287 Win=64128 Len=0 [ACK] 56511 → 80 60 TCP 192.168.0.126 2.18.31.35 537.377595 21515
HTTP/1.1 304 Not Modified 320 HTTP 192.168.0.126 2.18.31.35 537.377595 21516
Acknowledgment Number: 264 (relative ack number)
Acknowledgment number (raw): 3452999323
Header Length: 20 bytes (5) = ... 0101
Flags: 0x010 (ACK)
Window: 511
[Calculated window size: 130816]
[Window size scaling factor: 256]
Checksum: 0x16ef [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Profile: Default Packets: 120873 · Displayed: 112314 (92.9%)
byte(s) Γ ,Urgent Pointer (tcp.urgent_pointer)


Capturing from شبكة Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
Apply a display filter ... <Ctrl-/>
Info Length Protocol Destination Source Time No
Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 443 → 56356 66 TCP 104.22.0.235 192.168.0.126 0.000000 1
Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192 [SYN, ACK] 56356 → 443 66 TCP 192.168.0.126 104.22.0.235 0.094009 2
Seq=1 Ack=1 Win=131584 Len=0 [ACK] 443 → 56356 54 TCP 104.22.0.235 192.168.0.126 0.094713 3
Client Hello (SNI=api.reasonsecurity.com) 582 TLSv1.3 104.22.0.235 192.168.0.126 0.100724 4
Seq=1 Ack=1 Win=509 Len=1 [ACK] 443 → 56329 55 TCP 13.89.179.8 192.168.0.126 0.125715 5
Seq=1 Ack=529 Win=73728 Len=0 [ACK] 56356 → 443 60 TCP 192.168.0.126 104.22.0.235 0.192485 6
Server Hello, Change Cipher Spec, Application Data 273 TLSv1.3 192.168.0.126 104.22.0.235 0.192485 7
Change Cipher Spec, Application Data, Application Data 656 TLSv1.3 104.22.0.235 192.168.0.126 0.216291 8
Seq=220 Ack=1131 Win=73728 Len=0 [ACK] 56356 → 443 60 TCP 192.168.0.126 104.22.0.235 0.465488 9
Application Data 157 TLSv1.3 104.22.0.235 192.168.0.126 0.485780 10
Seq=220 Ack=1234 Win=73728 Len=0 [ACK] 56356 → 443 60 TCP 192.168.0.126 104.22.0.235 0.583378 11
Application Data, Application Data 1119 TLSv1.3 192.168.0.126 104.22.0.235 0.788766 12
Application Data 78 TLSv1.3 192.168.0.126 104.22.0.235 0.788766 13
Application Data 111 TLSv1.2 74.248.73.245 192.168.0.126 0.789007 14
Seq=1234 Ack=1309 Win=130048 Len=0 [ACK] 443 → 56356 54 TCP 104.22.0.235 192.168.0.126 0.789328 15
Seq=1234 Ack=1309 Win=130048 Len=0 [FIN, ACK] 443 → 56356 54 TCP 104.22.0.235 192.168.0.126 0.793433 16
56356 → 443 [FIN, ACK] Seq=1234 Ack=1309 Win=130048 Len=0 [TCP Retransmission] 54 TCP 104.22.0.235 192.168.0.126 1.201295 17
443 → 56356 [ACK] Seq=1310 Ack=1235 Win=73728 Len=0 [TCP Previous segment not captured] 54 TCP 192.168.0.126 104.22.0.235 1.237459 18
443 → 56356 [FIN, ACK] Seq=1309 Ack=1235 Win=73728 Len=0 [TCP Out-Of-Order] 54 TCP 192.168.0.126 104.22.0.235 1.237459 19
Seq=1235 Ack=1310 Win=130048 Len=0 [ACK] 443 → 56356 54 TCP 104.22.0.235 192.168.0.126 1.237936 20
56063 → 443 [PSH, ACK] Seq=1 Ack=1 Win=511 Len=57 [TCP Retransmission] 111 TCP 74.248.73.245 192.168.0.126 1.292152 21
443 → 56356 [ACK] Seq=1310 Ack=1235 Win=73728 Len=0 SLE=1234 SRE=1235 [TCP Dup ACK 18#1] 66 TCP 192.168.0.126 104.22.0.235 1.298349 22
Application Data 100 TLSv1.2 192.168.0.126 74.248.73.245 1.392622 23
443 → 56063 [ACK] Seq=47 Ack=58 Win=2048 Len=0 SLE=1 SRE=58 [TCP Dup ACK 23#1] 66 TCP 192.168.0.126 74.248.73.245 1.441241 24
Seq=58 Ack=47 Win=510 Len=0 [ACK] 443 → 56063 54 TCP 74.248.73.245 192.168.0.126 1.443561 25
Seq=1 Ack=1 Win=1021 Len=0 [FIN, ACK] 443 → 56344 54 TCP 20.42.65.94 192.168.0.126 3.982806 26
Seq=1 Ack=2 Win=16386 Len=0 [FIN, ACK] 56344 → 443 54 TCP 192.168.0.126 20.42.65.94 4.242704 27
Seq=2 Ack=2 Win=1021 Len=0 [ACK] 443 → 56344 54 TCP 20.42.65.94 192.168.0.126 4.242815 28
Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 443 → 56357 66 TCP 104.22.0.235 192.168.0.126 5.101440 29
Who has 192.168.0.126? Tell 192.168.0.1 42 ARP Intel_4e:e5:d5 TpLinkTechno_07:a8:aa 5.116705 30
is at 70:d8:23:4e:e5:d5 192.168.0.126 42 ARP TpLinkTechno_07:a8:aa Intel_4e:e5:d5 5.116772 31
Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192 [SYN, ACK] 56357 → 443 66 TCP 192.168.0.126 104.22.0.235 5.207633 32
Seq=1 Ack=1 Win=131584 Len=0 [ACK] 443 → 56357 54 TCP 104.22.0.235 192.168.0.126 5.207783 33
Client Hello (SNI=api.reasonsecurity.com) 582 TLSv1.3 104.22.0.235 192.168.0.126 5.208974 34
Application Data 136 TLSv1.2 192.168.0.126 52.224.108.169 5.229233 35
Seq=1 Ack=83 Win=254 Len=0 [ACK] 443 → 56130 54 TCP 52.224.108.169 192.168.0.126 5.277931 36
Seq=1 Ack=529 Win=73728 Len=0 [ACK] 56357 → 443 60 TCP 192.168.0.126 104.22.0.235 5.301895 37
Server Hello, Change Cipher Spec, Application Data 273 TLSv1.3 192.168.0.126 104.22.0.235 5.308541 38
Change Cipher Spec, Application Data, Application Data 656 TLSv1.3 104.22.0.235 192.168.0.126 5.319958 39
Seq=220 Ack=1131 Win=73728 Len=0 [ACK] 56357 → 443 60 TCP 192.168.0.126 104.22.0.235 5.577199 40
Application Data 116 TLSv1.3 104.22.0.235 192.168.0.126 5.577497 41
Seq=220 Ack=1193 Win=73728 Len=0 [ACK] 56357 → 443 60 TCP 192.168.0.126 104.22.0.235 5.671296 42
Seq=1 Ack=1 Win=512 Len=1 [TCP PDU reassembled in 444] [ACK] 443 → 56071 55 TCP 20.238.236.234 192.168.0.126 5.736944 43
Identification: 0xfefc (65276)
Flags: 0x2, Don't fragment = ... .010
Fragment Offset: 0 = 0000 0000 0000 0...
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.126
Destination Address: 199.232.80.217
[Stream index: 34]
Profile: Default Packets: 140444
Stream index (ip.stream)


شبكة* Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
udp
Info Length Protocol Destination Source Time No
Protected Payload (KP0), DCID=eb19996b6b550b41 74 QUIC 74.125.162.70 192.168.0.126 42.9286 5220
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9292 5221
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9292 5222
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9293 5223
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9324 5225
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9324 5226
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9324 5227
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9324 5228
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9324 5229
Protected Payload (KP0), DCID=eb19996b6b550b41 74 QUIC 74.125.162.70 192.168.0.126 42.9328 5230
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9344 5231
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9344 5232
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9344 5233
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9352 5234
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9352 5235
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9635 5236
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9635 5237
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9635 5238
Protected Payload (KP0), DCID=eb19996b6b550b41 74 QUIC 74.125.162.70 192.168.0.126 42.9641 5239
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9643 5240
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9654 5241
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9654 5242
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9708 5243
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9708 5244
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9708 5245
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9708 5246
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9708 5247
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9708 5248
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9712 5249
Protected Payload (KP0), DCID=eb19996b6b550b41 74 QUIC 74.125.162.70 192.168.0.126 42.9715 5250
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9747 5251
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9747 5252
Protected Payload (KP0) 1292 QUIC 192.168.0.126 74.125.162.70 42.9747 5253
e \Device\NPF_{9108CB4B-96E6-42BF-A038-C5EA26683FFA}, id 0
8:ff:7b:07:a8:aa), Dst: Intel_4e:e5:d5 (70:d8:23:4e:e5:d5)
Protocol Version 4, Src: 74.125.162.70, Dst: 192.168.0.126
User Datagram Protocol, Src Port: 443, Dst Port: 55134
QUIC IETF
QUIC Connection information
[Packet Length: 1250]
QUIC Short Header
Header Form: Short Header (0) = ...0
Fixed Bit: True = ...1.
Spin Bit: False = ...0..
b0330f12e99214157 57eec2ef6a7f070688d2863a338b3360e0c778