

CS471 – Web Technologies (Laboratory)		Lab 1
		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 (<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:
- 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).

CS471 – Web Technologies (Laboratory)		Lab 1
		The Internet Protocols

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	Provides reliable communication by establishing a three-way handshake before data transfer. Ensures retransmission if packets are lost.
Data Integrity and Ordering	TCP	Guarantees that data arrives in the correct order and without duplication using sequence and acknowledgment numbers.

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

	TCP	UDP
Use cases	Web browsing (HTTP/HTTPS), Email (SMTP, IMAP, POP3), File transfer (FTP)	Streaming video/audio, Online gaming, Voice over IP (VoIP)
Performance	Slower due to reliability mechanisms (handshake, acknowledgments, retransmissions)	Faster because it has minimal overhead, no handshake, and does not check for reliability

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

	Info	length	Protocol	Destination	Source	Time	.No
	Who has 192.168.100.148? Tell 192.168.100.145	42	ARP	Broadcast	TPLink_85:d1:f2	12.492426	413
	Len=25 53569 → 443 87	87	UDP	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:80c::200a	12.567977	414
	HTTP/1.1 200 OK (PNG)	470	HTTP	192.168.100.18	34.223.124.45	12.649334	415
	Seq=1436 Ack=2481 Win=64536 Len=0 [ACK] 80 → 49705	54	TCP	34.223.124.45	192.168.100.18	12.697638	416
	Who has 192.168.100.156? Tell 192.168.100.154	42	ARP	Broadcast	TPLink_85:a6:b2	14.950480	417
	Who has 192.168.100.156? Tell 192.168.100.145	42	ARP	Broadcast	TPLink_85:d1:f2	15.462377	418
	Who has 192.168.100.1? Tell 192.168.100.145	42	ARP	Broadcast	TPLink_85:d1:f2	15.462520	419
	Len=29 443 → 53569	91	UDP	2a00:1450:4006:80c::200a	2001:16a3:d26:fd00:4165:175d:1761:b78d	15.771304	420
	Len=25 53569 → 443 87	87	UDP	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:80c::200a	15.887919	421
	Who has 192.168.100.156? Tell 192.168.100.154	42	ARP	Broadcast	TPLink_85:a6:b2	15.974823	422
	Who has 192.168.100.156? Tell 192.168.100.145	42	ARP	Broadcast	TPLink_85:d1:f2	16.487249	423
	Seq=1436 Ack=2481 Win=64536 Len=0 [FIN, ACK] 80 → 49705	54	TCP	34.223.124.45	192.168.100.18	16.881406	424
	Who has 192.168.100.129? Tell 192.168.100.154	42	ARP	Broadcast	TPLink_85:a6:b2	16.998528	425
	Who has 192.168.100.156? Tell 192.168.100.154	42	ARP	Broadcast	TPLink_85:a6:b2	17.100595	426
	Seq=2481 Ack=1437 Win=28944 Len=0 [FIN, ACK] 49705 → 80	54	TCP	192.168.100.18	34.223.124.45	17.118197	427

0000 98 35 ed 91 32 d3 80 91 33 9f
0010 27 8c 00 14 06 40 20 01 16 a3
0020 17 5d 17 61 b7 8d 26 00 1f 13
0030 71 65 5f c7 73 6e c2 1d 00 50
0040 ab 84 50 10 02 00 ab 2c 00 00

Frame 410: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{85C7ACD1-64EC-44E2-82D2-18060CBDA652}, id 0 <
Ethernet II, Src: AzureWaveTec_9f:fc:f1 (80:91:33:9f:fc:f1), Dst: HuaweiTechno_91:32:d3 (98:35:ed:91:32:d3) <
Internet Protocol Version 6, Src: 2001:16a3:d26:fd00:4165:175d:1761:b78d, Dst: 2600:1f13:37c:1400:ba21:7165:5fc7:736e <
Transmission Control Protocol, Src Port: 49693, Dst Port: 80, Seq: 2, Ack: 2, Len: 0 <

task 2

Wi-Fi

HelpToolsWirelessTelephonyStatisticsAnalyzeCaptureGoViewEditFile

http

Info	ength	Protocol	Destination	Source	Time	.No
GET / HTTP/1.1	510	HTTP	2600:1f13:37c:1400:ba21:7165:5fc7:736e	2001:16a3:d26:fd00:4165:175d:1761:b78d	3.216414	171
HTTP/1.1 200 OK (text/html)	1047	HTTP	2001:16a3:d26:fd00:4165:175d:1761:b78d	2600:1f13:37c:1400:ba21:7165:5fc7:736e	3.486228	172
GET /online HTTP/1.1	553	HTTP	34.223.124.45	192.168.100.18	11.406553	384
HTTP/1.1 301 Moved Permanently (text/html)	599	HTTP	192.168.100.18	34.223.124.45	11.650459	387
GET /online/ HTTP/1.1	554	HTTP	34.223.124.45	192.168.100.18	11.660579	390
HTTP/1.1 200 OK (text/html)	273	HTTP	192.168.100.18	34.223.124.45	11.895569	405
GET /favicon.ico HTTP/1.1	490	HTTP	34.223.124.45	192.168.100.18	12.415646	411
HTTP/1.1 200 OK (PNG)	470	HTTP	192.168.100.18	34.223.124.45	12.649334	415

000098 35 ed 91 32 d3 80 91 33
00104f 84 01 c8 06 40 20 01 16
002017 5d 17 61 b7 8d 26 00 1f
003071 65 5f c7 73 6e c2 21 00
0040e3 24 50 18 fd b8 4d 7e 00
005048 54 54 50 2f 31 2e 31 0d
00606e 65 76 65 72 73 73 6c 2e
00706e 6e 65 63 74 69 6f 6e 3a
00806c 69 76 65 0d 0a 55 70 67
009073 65 63 75 72 65 2d 52 65
00a020 31 0d 0a 55 73 65 72 2d
00b04d 6f 7a 69 6c 6c 61 2f 35
00c064 6f 77 73 20 4e 54 20 31
00d06e 36 34 3b 20 78 36 34 29
00e065 62 4b 69 74 2f 35 33 37
00f054 4d 4c 2c 20 6c 69 6b 65
010020 43 68 72 6f 6d 65 2f 31
011030 20 53 61 66 61 72 69 2f
01200a 41 63 63 65 70 74 3a 20

Frame 171: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits) on interface \Device\NPF_{85C7ACD1-64EC-44E2-82D2-18060CBDA652}, id 0
Ethernet II, Src: AzureWaveTec_9f:fc:f1 (80:91:33:9f:fc:f1), Dst: HuaweiTechno_91:32:d3 (98:35:ed:91:32:d3)
Internet Protocol Version 6, Src: 2001:16a3:d26:fd00:4165:175d:1761:b78d, Dst: 2600:1f13:37c:1400:ba21:7165:5fc7:736e
Transmission Control Protocol, Src Port: 49697, Dst Port: 80, Seq: 1, Ack: 1, Len: 436
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: neverssl.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\r\n
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\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ar,en-US;q=0.9,en;q=0.8\r\n
r\n
[Response in frame: 210]
[Full request URI: http://neverssl.com]

Profile: Default | Packets: 427 · Displayed: 8 (1.9%) · Dropped: 0 (0.0%) | Hypertext Transfer Protocol: Protocol

Wi-Fi

+ tcp.stream eq 9

...Seq=0 Win=64952 Len=0 MSS=1412
Seq=0 Ack=1 Win=26883 Len=0
Seq=1 Ack=1 Wi
Seq=1 Ack=437 Wi
...Seq=1 Ack=437 Win=26800 Len=130
Seq=437 Ack=2274 Wi
Seq=437 Ack=2274 Win=649
Seq=2274 Ack=438 Win=268
Seq=438 Ack=2275 Wi

0000 98 35 ed 91 32 d3 80 91
0010 4f 84 00 20 06 40 20 01
0020 17 5d 17 61 b7 8d 26 00
0030 71 65 5f c7 73 6e c2 21
0040 00 00 80 02 fd b8 cf ef
0050 03 08 01 01 04 02

Wireshark · Follow TCP Stream (tcp.stream eq 9) · Wi-Fi

part 2 task 1

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/140.0.0.0 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: Sat, 13 Sep 2025 19:37:55 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..1).2Z...~.C.Vk[...#.'.k.t#*...+.....0.R.{.T.&\$..zB^?...9Pz.E^...x.[m...=.*.Q%.V.+...'.T.2\...
_xf/e5`1
...y..s..#.....?..r...v.e%..{U...^v..
.p@...q..kQ...T..
.....c..y/.C..\.|..u.i....._...}..
..#k1.>0....3.E... t..
..*.A.y.....!..DP...h.K...2.e:...7;n.....V....._...=.v>..R..b..._LQ...m...p;\$.> :e.....1.B.....
....\..^Eq.x.z...../D.....XW...b..N...O..#Q.q1....G....1M.....'.x..Kom(...N..W...f...Z"7...|...v..
....1..Z[.....P.....8a..J.I.T.....Q.%."Q.....&.f.U...K...1..&.X.i[...1..%/r-ET.....
...Io.h..."#..h.1...>..2...b...g..G..R..._h{..._d|.E.-.Z...U
xp " \ 7 5

Packet 209. I client pkt(s). I server pkt(s). I turn(s). Click to select.

Stream No delta times ASCII Show as Entire conversation (2709 bytes)

Find Next Case sensitive ☐ Find:

مساعدة أعلق Back ...Save as Print Filter Out This Stream

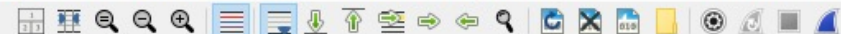
Statistics Analyze Capture Go View Edit File

Source	Time	.No
0:4165:175d:1761:b78d	2.971845	93
0:ba21:7165:5fc7:736e	3.215607	169
0:4165:175d:1761:b78d	3.215673	170
0:4165:175d:1761:b78d	3.216414	171
0:ba21:7165:5fc7:736e	3.462261	206
0:ba21:7165:5fc7:736e	3.485087	209
0:ba21:7165:5fc7:736e	3.486228	210
0:4165:175d:1761:b78d	3.486270	211
0:4165:175d:1761:b78d	6.789086	291
0:ba21:7165:5fc7:736e	7.029346	306
0:4165:175d:1761:b78d	7.029386	307

5C7ACD1-64EC-44E2-82D2-18060CBDA652}, id 0 <
HuaweiTechno_91:32:d3 (98:35:ed:91:32:d3) <
st: 2600:1f13:37c:1400:ba21:7165:5fc7:736e <
Port: 49697, Dst Port: 80, Seq: 0, Len: 0 <

wireshark_Wi-FiKBNSC3.pcapng

task 2



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

	Info	length	protocol	Destination	Source	Time	.No	
	Protected Payload (KP0)	89	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d ...:2a00:1450:4006:812	192.168.100.1	3.861032	235	
Standard query response 0xc00c A wonderfulsoldastoundingday.neverssl.com A	34.223.124.45	114	DNS	192.168.100.18	192.168.100.1	3.862398	236	
	Protected Payload (KP0), DCID=f0d39f6987b0413e	596	QUIC	2a00:1450:4006:80d::200e ...2001:16a3:d26:fd00:4	...	3.871459	237	
	Seq=0 Win=64952 Len=0 MSS=1412 WS=256 SACK_PERM [SYN]	443 → 49703	86	TCP	2600:1f13:37c:1400:ba21:7165:5fc7:736e ...2001:16a3:d26:fd00:4	...	3.873793	238
Standard query response 0xbey3 HTTPS wonderfulsoldastoundingday.neverssl.com SOA ns-1716.aw	182	DNS	192.168.100.18	192.168.100.1	3.880643	239		
	Protected Payload (KP0), DCID=f048149de78a12a8	94	QUIC	2a00:1450:4006:812::200a ...2001:16a3:d26:fd00:4	...	3.889907	240	
	Protected Payload (KP0)	324	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d ...:2a00:1450:4006:812	...	3.905545	241	
	Protected Payload (KP0)	218	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d ...:2a00:1450:4006:812	...	3.905656	242	
	Protected Payload (KP0), DCID=f048149de78a12a8	97	QUIC	2a00:1450:4006:812::200a ...2001:16a3:d26:fd00:4	...	3.906611	243	
	Protected Payload (KP0)	90	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d ...:2a00:1450:4006:80d	...	3.977616	244	
	Protected Payload (KP0)	189	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d ...:2a00:1450:4006:80d	...	3.985832	245	
	Protected Payload (KP0)	84	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d ...:2a00:1450:4006:80d	...	3.985832	246	
	Protected Payload (KP0), DCID=f0d39f6987b0413e	97	QUIC	2a00:1450:4006:80d::200e ...2001:16a3:d26:fd00:4	...	3.986032	247	
	Protected Payload (KP0)	86	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d ...:2a00:1450:4006:812	...	4.018749	248	
	Protected Payload (KP0), DCID=f0d39f6987b0413e	94	QUIC	2a00:1450:4006:80d::200e ...2001:16a3:d26:fd00:4	...	4.019090	249	
	Protected Payload (KP0)	86	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d ...:2a00:1450:4006:80d	...	4.091035	250	
	Seq=0 Ack=1 Win=26883 Len=0 MSS=1412 SACK_PERM WS=4096 [SYN, ACK]	49703 → 443	86	TCP	2001:16a3:d26:fd00:4165:175d:1761:b78d ...2600:1f13:37c:1400:b	...	4.104955	251
	Seq=1 Ack=1 Win=131072 Len=0 [ACK]	443 → 49703	74	TCP	2600:1f13:37c:1400:ba21:7165:5fc7:736e ...2001:16a3:d26:fd00:4	...	4.105078	252
	Seq=1 Ack=1 Win=131072 Len=1412 [TCP PDU reassembled in 254] [ACK]	443 → 49703	1486	TCP	2600:1f13:37c:1400:ba21:7165:5fc7:736e ...2001:16a3:d26:fd00:4	...	4.105897	253
	Client Hello (SNI=wonderousoldastoundingday.neverssl.com)	442	...TLS	2600:1f13:37c:1400:ba21:7165:5fc7:736e ...2001:16a3:d26:fd00:4	...	4.105897	254	
49699 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [TCP Retransmission]	66	TCP	34.223.124.45	192.168.100.18	4.135516	255		
49700 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [TCP Retransmission]	66	TCP	34.223.124.45	192.168.100.18	4.135866	256		
	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN]	80 → 49704	66	TCP	34.223.124.45	192.168.100.18	4.167724	257
	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN]	80 → 49705	66	TCP	34.223.124.45	192.168.100.18	4.167909	258
	Seq=1 Ack=1 Win=510 Len=1 [ACK]	5228 → 49727	75	TCP	2a00:1450:4006:80d::200e ...2001:16a3:d26:fd00:4	...	4.255660	259



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

	Info	Length	Protocol	Destination	Source	Time	No.
	Seq=0 Ack=1 Win=26883 Len=0 MSS=1412 [SYN, ACK] 49705 → 80	58	TCP	192.168.100.18	34.223.124.45	11.405632	382
	Seq=1 Ack=1 Win=64240 Len=0 [ACK] 80 → 49705	54	TCP	34.223.124.45	192.168.100.18	11.405877	383
	GET /online HTTP/1.1	553	HTTP	34.223.124.45	192.168.100.18	11.406553	384
...Standard query 0x0000 PTR _raop._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" qu		91	MDNS	224.0.0.251	192.168.100.149	11.571554	385
	Seq=1 Ack=500 Win=26800 Len=0 [ACK] 49705 → 80	54	TCP	192.168.100.18	34.223.124.45	11.649930	386
	HTTP/1.1 301 Moved Permanently (text/html)	599	HTTP	192.168.100.18	34.223.124.45	11.650459	387
	Protected Payload (KP0), DCID=f048149de78a12a8	223	QUIC	2a00:1450:4006:812::200a	...2001:16a3:d26:fd00:4	11.655530	388
	Protected Payload (KP0), DCID=f0d39f6987b0413e	710	QUIC	2a00:1450:4006:80d::200e	...2001:16a3:d26:fd00:4	11.660390	389
	GET /online/ HTTP/1.1	554	HTTP	34.223.124.45	192.168.100.18	11.660579	390
...Standard query 0x0000 PTR _raop._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" qu		111	MDNS	ff02::fb	...fe80::94:1c3:4cf1:b4	11.674368	391
	Protected Payload (KP0)	90	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	...:2a00:1450:4006:812	11.763560	392
	Protected Payload (KP0)	90	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	...:2a00:1450:4006:80d	11.769679	393
	Protected Payload (KP0)	190	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	...:2a00:1450:4006:80d	11.779853	394
	Protected Payload (KP0), DCID=f0d39f6987b0413e	97	QUIC	2a00:1450:4006:80d::200e	...2001:16a3:d26:fd00:4	11.780252	395
	Protected Payload (KP0)	84	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	...:2a00:1450:4006:80d	11.780624	396
	Protected Payload (KP0)	344	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	...:2a00:1450:4006:812	11.785771	397
	Protected Payload (KP0), DCID=f048149de78a12a8	97	QUIC	2a00:1450:4006:812::200a	...2001:16a3:d26:fd00:4	11.786253	398
	Protected Payload (KP0)	189	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	...:2a00:1450:4006:812	11.786861	399
	Protected Payload (KP0), DCID=f0d39f6987b0413e	94	QUIC	2a00:1450:4006:80d::200e	...2001:16a3:d26:fd00:4	11.817977	400
	Protected Payload (KP0), DCID=f048149de78a12a8	94	QUIC	2a00:1450:4006:812::200a	...2001:16a3:d26:fd00:4	11.818127	401
	Seq=1 Ack=1 Win=131072 Len=0 [FIN, ACK] 80 → 49693	74	TCP	2600:1f13:37c:1400:ba21:7165:5fc7:736e	...2001:16a3:d26:fd00:4	11.874479	402
	Protected Payload (KP0)	86	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	...:2a00:1450:4006:80d	11.892245	403
	Seq=546 Ack=1000 Win=27872 Len=1300 [TCP PDU reassembled in 405] [ACK] 49705 → 80	1354	TCP	192.168.100.18	34.223.124.45	11.895569	404
	HTTP/1.1 200 OK (text/html)	273	HTTP	192.168.100.18	34.223.124.45	11.895569	405
	Protected Payload (KP0)	86	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	...:2a00:1450:4006:812	11.895569	406

Wi-Fi

HelpToolsWirelessTelephonyStatisticsAnalyzeCaptureGoViewEditFile

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

	Info	length	protocol	Destination	Source	Time	No.
...	Standard query 0x0000 PTR _raop._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" qu	91	MDNS	224.0.0.251	192.168.100.149	11.571554	385
	Seq=1 Ack=500 Win=26800 Len=0 [ACK] 49705 → 80	54	TCP	192.168.100.18	34.223.124.45	11.649930	386
	HTTP/1.1 301 Moved Permanently (text/html)	599	HTTP	192.168.100.18	34.223.124.45	11.650459	387
	Protected Payload (KP0), DCID=f048149de78a12a8	223	QUIC	2a00:1450:4006:812::200a	2001:16a3:d26:fd00:4	11.655530	388
	Protected Payload (KP0), DCID=f0d39f6987b0413e	710	QUIC	2a00:1450:4006:80d::200e	2001:16a3:d26:fd00:4	11.660390	389
	GET /online/	554	HTTP	34.223.124.45	192.168.100.18	11.660579	390
...	Standard query 0x0000 PTR _raop._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" qu	111	MDNS	ff02::fb	fe80::94:1c3:4cf1:b4	11.674368	391
	Protected Payload (KP0)	90	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:812	11.763560	392
	Protected Payload (KP0)	90	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:80d	11.769679	393
	Protected Payload (KP0)	190	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:80d	11.779853	394
	Protected Payload (KP0), DCID=f0d39f6987b0413e	97	QUIC	2a00:1450:4006:80d::200e	2001:16a3:d26:fd00:4	11.780252	395
	Protected Payload (KP0)	84	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:80d	11.780624	396
	Protected Payload (KP0)	344	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:812	11.785771	397
	Protected Payload (KP0), DCID=f048149de78a12a8	97	QUIC	2a00:1450:4006:812::200a	2001:16a3:d26:fd00:4	11.786253	398
	Protected Payload (KP0)	189	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:812	11.786861	399
	Protected Payload (KP0), DCID=f0d39f6987b0413e	94	QUIC	2a00:1450:4006:80d::200e	2001:16a3:d26:fd00:4	11.817977	400
	Protected Payload (KP0), DCID=f048149de78a12a8	94	QUIC	2a00:1450:4006:812::200a	2001:16a3:d26:fd00:4	11.818127	401
	Seq=1 Ack=1 Win=131072 Len=0 [FIN, ACK] 80 → 49693	74	TCP	2600:1f13:37c:1400:ba21:7165:5fc7:736e	2001:16a3:d26:fd00:4	11.874479	402
	Protected Payload (KP0)	86	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:80d	11.892245	403
	Seq=546 Ack=1000 Win=27872 Len=1300 [TCP PDU reassembled in 405] [ACK] 49705 → 80	1354	TCP	192.168.100.18	34.223.124.45	11.895569	404
	HTTP/1.1 200 OK (text/html)	273	HTTP	192.168.100.18	34.223.124.45	11.895569	405
	Protected Payload (KP0)	86	QUIC	2001:16a3:d26:fd00:4165:175d:1761:b78d	2a00:1450:4006:812	11.895569	406
	Seq=1000 Ack=2065 Win=64952 Len=0 [ACK] 80 → 49705	54	TCP	34.223.124.45	192.168.100.18	11.895617	407
	Who has 192.168.100.148? Tell 192.168.100.154	42	ARP	Broadcast	TPLink_85:a6:b2	11.980392	408
	Seq=1 Ack=2 Win=27808 Len=0 [FIN, ACK] 40693 → 80	74	TCP	2001:16a3:d26:fd00:4165:175d:1761:b78d	2600:1f13:37c:1400:b	12.106854	409

0000 98 35 ed 91 32 d3 80 91 33 9f

0010 27 8c 00 14 06 40 20 01 16 a3

0020 17 5d 17 61 b7 8d 26 00 1f 13

0030 71 65 5f c7 73 6e c2 1d 00 50

0040 ab 83 50 11 02 00 ab 2d 00 00

Frame 402: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{85C7ACD1-64EC-44E2-82D2-18060CBDA652}, id 0

Ethernet II, Src: AzureWaveTec_9f:fc:f1 (80:91:33:9f:fc:f1), Dst: HuaweiTechno_91:32:d3 (98:35:ed:91:32:d3)

Internet Protocol Version 6, Src: 2001:16a3:d26:fd00:4165:175d:1761:b78d, Dst: 2600:1f13:37c:1400:ba21:7165:5fc7:736e

Transmission Control Protocol, Src Port: 49693, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Profile: Default

Packets: 427 · Dropped: 0 (0.0%)

wireshark_Wi-FiKBNSC3.pcapng

0000	98 35 ed 91 32 d3 80 91 33 9f	Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{85C7ACD1-64EC-44E2-82D2-18060C8DA652}, id 0
0010	f7 86 00 25 11 40 20 01 16 a3	Ethernet II, Src: AzureWaveTec_9f:fc:f1 (80:91:33:9f:fc:f1), Dst: HuaweiTechno_91:32:d3 (98:35:ed:91:32:d3)
0020	17 5d 17 61 b7 8d 2a 00 14 50	Internet Protocol Version 6, Src: 2001:16a3:d26:fd00:4165:175d:1761:b78d, Dst: 2a00:1450:4006:812::200a
0030	00 00 00 00 20 0a d4 48 01 bb	User Datagram Protocol, Src Port: 54344, Dst Port: 443
0040	e2 de 30 7e 80 83 83 a0 7e c8	Data (29 bytes)
0050	1d f9 bc 8a 3d 57 d7 76 79 aa	