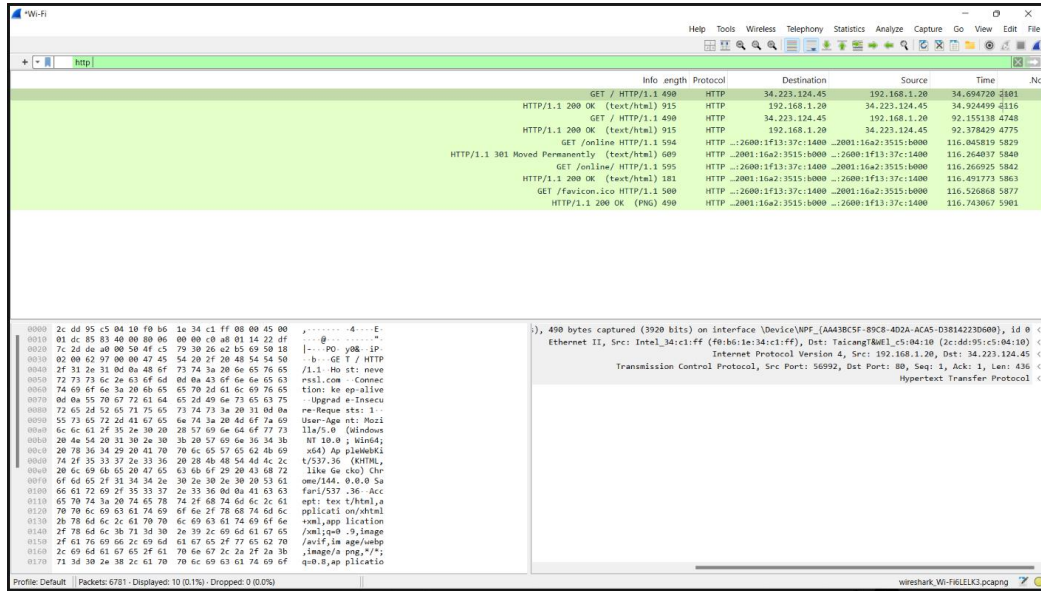


Lab1

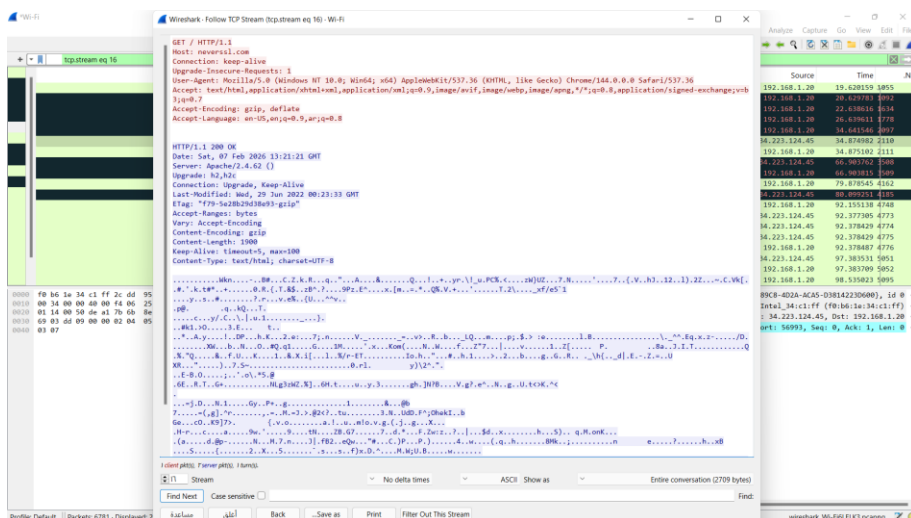
Part 1: Capturing HTTP Traffic



This screenshot shows HTTP request and response.

Part 2: Analyzing TCP/IP Traffic

Task 1: Follow TCP Stream



This screenshot shows the full TCP conversation between the client and the server

Task 2: TCP Handshake and Termination

Wi-Fi

Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File

tcp

No	Time	Source	Destination	Protocol	Length	Info
0.920812	19	192.168.1.20	192.168.1.20	TCP	66	Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2 [ACK] 65119 → 443
2.970187	28	192.168.1.20	192.168.1.20	TLSv1.2	98	Application Data
2.970571	29	192.168.1.20	192.168.1.20	TLSv1.2	102	Application Data
3.073666	30	192.168.1.20	192.168.1.20	TCP	86	Seq=25 Ack=29 Win=17 Len=0 [ACK] 65101 → 443
4.116892	43	192.168.1.20	192.168.1.20	TCP	86	Seq=0 Win=64800 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 65142
4.117273	44	192.168.1.20	192.168.1.20	TCP	66	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 65143
4.127139	45	192.168.1.20	192.168.1.20	TCP	66	Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128 [SYN, ACK] 65143 → 80
4.127211	46	192.168.1.20	192.168.1.20	TCP	54	Seq=1 Ack=1 Win=6304 Len=0 [ACK] 80 → 65143
4.127488	47	192.168.1.20	192.168.1.20	HTTP	165	GET /connecttest.txt HTTP/1.1
4.127570	48	192.168.1.20	192.168.1.20	TCP	86	Seq=0 Ack=1 Win=64800 Len=0 MSS=1412 SACK_PERM WS=128 [SYN, ACK] 65142 → 80
4.127616	49	192.168.1.20	192.168.1.20	TCP	74	Seq=1 Ack=1 Win=6304 Len=0 [ACK] 80 → 65142
4.127824	50	192.168.1.20	192.168.1.20	HTTP	186	GET /connecttest.txt HTTP/1.1
4.136684	51	192.168.1.20	192.168.1.20	TCP	54	Seq=1 Ack=112 Win=64256 Len=0 [ACK] 65143 → 80
4.137484	52	192.168.1.20	192.168.1.20	HTTP	241	HTTP/1.1 200 OK (text/plain)
4.137659	53	192.168.1.20	192.168.1.20	TCP	54	Seq=112 Ack=189 Win=66048 Len=0 [FIN, ACK] 80 → 65143
4.138455	54	192.168.1.20	192.168.1.20	TCP	54	Seq=188 Ack=112 Win=64256 Len=0 [FIN, ACK] 65143 → 80
4.139411	55	192.168.1.20	192.168.1.20	TCP	54	Seq=113 Ack=189 Win=66048 Len=0 [ACK] 80 → 65143
4.139411	56	192.168.1.20	192.168.1.20	TCP	80	Seq=0 Ack=1 Win=64800 Len=0 MSS=1412 SACK_PERM WS=128 [TCP Retransmission] 80

Profile: Default | Packets: 560 - Displayed: 111 (19.8%) - Dropped: 0 (0.0%)

Transmission Control Protocol: Protocol

Part 3: Capturing and Analyzing UDP Traffic

Wi-Fi

Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File

udp

No	Time	Source	Destination	Protocol	Length	Info
0.000000	1	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.039883	2	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.080860	3	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.119816	4	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.159954	5	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.200474	6	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.240585	7	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.279144	8	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.319673	9	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.360332	10	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.370539	11	192.168.1.20	3.251.143.77	STUN	154	Binding Request user: gMaSHhzXFSHCn:R+2b
0.400184	12	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.440277	13	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.480017	14	192.168.1.20	3.251.143.77	STUN	106	Binding Success Response XOR-MAPPED-ADDRESS: 5.163.24.227
0.519428	17	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.542317	19	192.168.1.20	3.251.143.77	UDP	80	Len=38 65161 → 64627
0.559672	20	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627
0.599744	21	192.168.1.20	3.251.143.77	UDP	235	Len=193 65161 → 64627

Profile: Default | Packets: 6345 - Displayed: 5822 (91.8%) - Dropped: 0 (0.0%)

wireshark-Wi-Fi\UN713.pcapng

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	TCP is connection-oriented; it uses a three-way handshake to establish a connection and ensures all data is received via acknowledgments.
Data Integrity and Ordering	TCP	It uses sequence numbers to reassemble data packets in the correct order and requests retransmission if any data is lost or corrupted

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

	TCP	UDP
Use cases	Web browsing (HTTP/HTTPS), Email (SMTP), and File Transfer (FTP).	Video streaming, Online gaming, and Voice over IP (VoIP).
Performance	Slower but reliable. It has higher overhead due to error-checking and flow control.	Faster and efficient. It has low overhead because it doesn't wait for acknowledgments (low latency).

