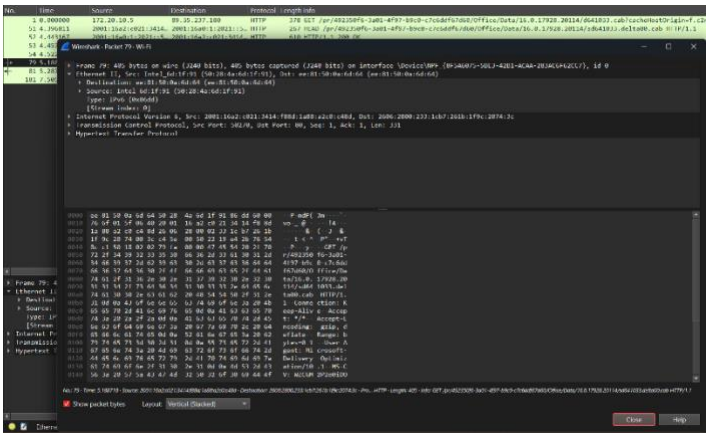
Lab week 2

Task 2:

Step 1:

Step 2:

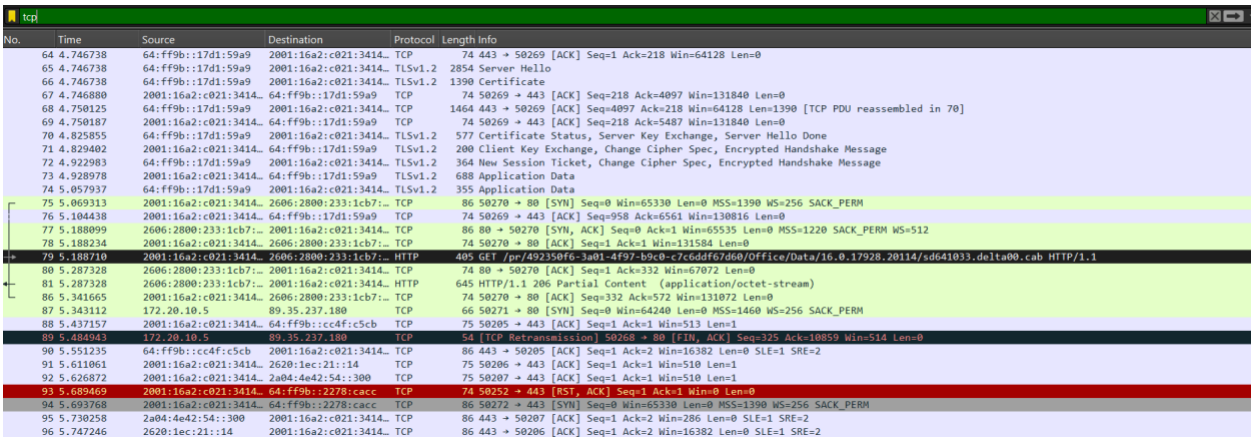


Step 3:

1. The methods
   GET
2. URL
   https://myqu.qu.edu.sa
3. Response code
   HTTP 405 HTTP /1/ 200 OK

Part 2:

Step 2:



tcp

No.	Time	Source	Destination	Protocol	Length	Info
64	4.746738	64:ff9b::17d1:59a9	2001:16a2:c021:3414…	TCP	74	443 → 50269 [ACK] Seq=1 Ack=218 Win=64128 Len=0
65	4.746738	64:ff9b::17d1:59a9	2001:16a2:c021:3414…	TLSv1.2	2854	Server Hello
66	4.746738	64:ff9b::17d1:59a9	2001:16a2:c021:3414…	TLSv1.2	1390	Certificate
67	4.746880	2001:16a2:c021:3414…	64:ff9b::17d1:59a9	TCP	74	50269 → 443 [ACK] Seq=218 Ack=4097 Win=131840 Len=0
68	4.750125	64:ff9b::17d1:59a9	2001:16a2:c021:3414…	TCP	1464	443 → 50269 [ACK] Seq=4097 Ack=218 Win=64128 Len=1390 [TCP PDU reassembled in 70]
69	4.750187	2001:16a2:c021:3414…	64:ff9b::17d1:59a9	TCP	74	50269 → 443 [ACK] Seq=218 Ack=5487 Win=131840 Len=0
70	4.825855	64:ff9b::17d1:59a9	2001:16a2:c021:3414…	TLSv1.2	577	Certificate Status, Server Key Exchange, Server Hello Done
71	4.829402	2001:16a2:c021:3414…	64:ff9b::17d1:59a9	TLSv1.2	200	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
72	4.922983	64:ff9b::17d1:59a9	2001:16a2:c021:3414…	TLSv1.2	364	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
73	4.928978	2001:16a2:c021:3414…	64:ff9b::17d1:59a9	TLSv1.2	688	Application Data
74	5.057937	64:ff9b::17d1:59a9	2001:16a2:c021:3414…	TLSv1.2	355	Application Data
75	5.069313	2001:16a2:c021:3414…	2606:2800:233:1cb7:…	TCP	86	50270 → 80 [SYN] Seq=0 Win=65330 Len=0 MSS=1390 WS=256 SACK_PERM
76	5.104438	2001:16a2:c021:3414…	64:ff9b::17d1:59a9	TCP	74	50269 → 443 [ACK] Seq=958 Ack=6561 Win=130816 Len=0
77	5.188099	2606:2800:233:1cb7:…	2001:16a2:c021:3414…	TCP	86	80 → 50270 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1220 SACK_PERM WS=512
78	5.188234	2001:16a2:c021:3414…	2606:2800:233:1cb7:…	TCP	74	50270 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
79	5.188710	2001:16a2:c021:3414…	2606:2800:233:1cb7:…	HTTP	405	GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.17928.20114/sd641033.delta00.cab HTTP/1.1
80	5.287328	2606:2800:233:1cb7:…	2001:16a2:c021:3414…	TCP	74	80 → 50270 [ACK] Seq=1 Ack=332 Win=67072 Len=0
81	5.287328	2606:2800:233:1cb7:…	2001:16a2:c021:3414…	HTTP	645	HTTP/1.1 206 Partial Content (application/octet-stream)
86	5.341665	2001:16a2:c021:3414…	2606:2800:233:1cb7:…	TCP	74	50270 → 80 [ACK] Seq=332 Ack=572 Win=131072 Len=0
87	5.343112	172.20.10.5	89.35.237.180	TCP	66	50271 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
88	5.437157	2001:16a2:c021:3414…	64:ff9b::cc4f:c5cb	TCP	75	50205 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1
89	5.484943	172.20.10.5	89.35.237.180	TCP	54	[TCP Retransmission] 50268 → 80 [FIN, ACK] Seq=325 Ack=10859 Win=514 Len=0
90	5.551235	64:ff9b::cc4f:c5cb	2001:16a2:c021:3414…	TCP	86	443 → 50205 [ACK] Seq=1 Ack=2 Win=16382 Len=0 SLE=1 SRE=2
91	5.611061	2001:16a2:c021:3414…	2620:1ec:21::14	TCP	75	50206 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1
92	5.626872	2001:16a2:c021:3414…	2a04:4e42:54::300	TCP	75	50207 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1
93	5.689469	2001:16a2:c021:3414…	64:ff9b::2278:cacc	TCP	74	50252 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	5.693768	2001:16a2:c021:3414…	64:ff9b::2278:cacc	TCP	86	50272 → 443 [SYN] Seq=0 Win=65330 Len=0 MSS=1390 WS=256 SACK_PERM
95	5.730258	2a04:4e42:54::300	2001:16a2:c021:3414…	TCP	86	443 → 50207 [ACK] Seq=1 Ack=2 Win=286 Len=0 SLE=1 SRE=2
96	5.747246	2620:1ec:21::14	2001:16a2:c021:3414…	TCP	86	443 → 50206 [ACK] Seq=1 Ack=2 Win=16382 Len=0 SLE=1 SRE=2

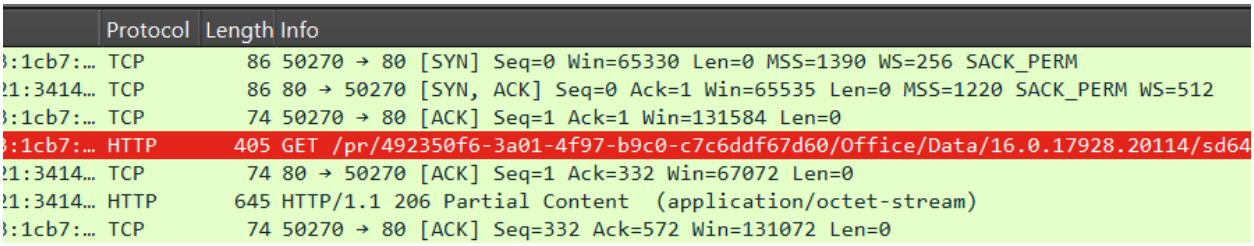
Step 3:

Task 2:

Step 1:

- SYN Initiates a connection.
- SYN-ACK Responds to the SYN.
- ACK Acknowledges the SYN-ACK and establishes the connection.

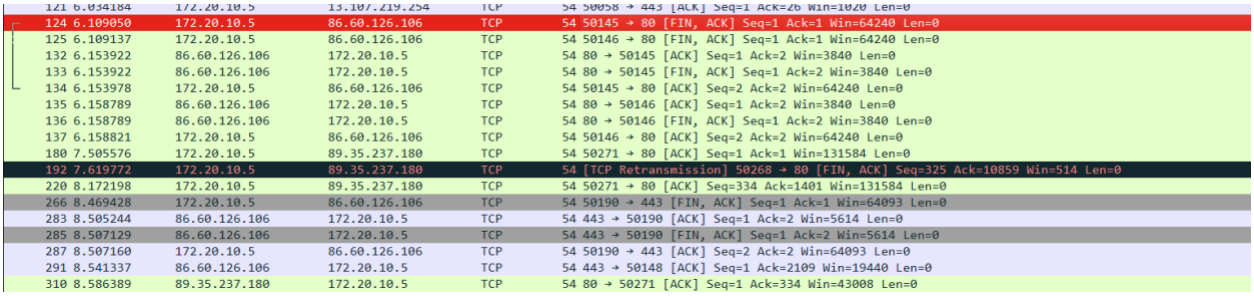
Step 2:



	Protocol	Length	Info
:1cb7:…	TCP	86	50270 → 80 [SYN] Seq=0 Win=65330 Len=0 MSS=1390 WS=256 SACK_PERM
21:3414…	TCP	86	80 → 50270 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1220 SACK_PERM WS=512
:1cb7:…	TCP	74	50270 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
:1cb7:…	HTTP	405	GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.17928.20114/sd64
21:3414…	TCP	74	80 → 50270 [ACK] Seq=1 Ack=332 Win=67072 Len=0
21:3414…	HTTP	645	HTTP/1.1 206 Partial Content (application/octet-stream)
:1cb7:…	TCP	74	50270 → 80 [ACK] Seq=332 Ack=572 Win=131072 Len=0

1. **First Packet (SYN from client):**
    - Seq=0, Ack=0
    - The client initiates the connection.
2. **Second Packet (SYN-ACK from server):**
    - Seq=0, Ack=1
    - The server acknowledges the SYN packet from the client.
3. **Third Packet (ACK from client):**
    - Seq=1, Ack=1
    - The client acknowledges the SYN-ACK packet from the server.

Step 4:



124	6.109050	172.20.10.5	86.60.126.106	TCP	54 50145 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
125	6.109137	172.20.10.5	86.60.126.106	TCP	54 50146 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
132	6.153922	86.60.126.106	172.20.10.5	TCP	54 80 → 50145 [ACK] Seq=1 Ack=2 Win=3840 Len=0
133	6.153922	86.60.126.106	172.20.10.5	TCP	54 80 → 50145 [FIN, ACK] Seq=1 Ack=2 Win=3840 Len=0
134	6.153978	172.20.10.5	86.60.126.106	TCP	54 50145 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
135	6.158789	86.60.126.106	172.20.10.5	TCP	54 80 → 50146 [ACK] Seq=1 Ack=2 Win=3840 Len=0
136	6.158789	86.60.126.106	172.20.10.5	TCP	54 80 → 50146 [FIN, ACK] Seq=1 Ack=2 Win=3840 Len=0
137	6.158821	172.20.10.5	86.60.126.106	TCP	54 50146 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
180	7.505576	172.20.10.5	89.35.237.180	TCP	54 50271 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
192	7.619772	172.20.10.5	89.35.237.180	TCP	54 [TCP Retransmission] 50268 → 80 [FIN, ACK] Seq=325 Ack=10859 Win=514 Len=0
220	8.172198	172.20.10.5	89.35.237.180	TCP	54 50271 → 80 [ACK] Seq=334 Ack=1401 Win=131584 Len=0
266	8.469428	172.20.10.5	86.60.126.106	TCP	54 50190 → 443 [FIN, ACK] Seq=1 Ack=1 Win=64093 Len=0
283	8.505244	86.60.126.106	172.20.10.5	TCP	54 443 → 50190 [ACK] Seq=1 Ack=2 Win=5614 Len=0
285	8.507129	86.60.126.106	172.20.10.5	TCP	54 443 → 50190 [FIN, ACK] Seq=1 Ack=2 Win=5614 Len=0
287	8.507160	172.20.10.5	86.60.126.106	TCP	54 50190 → 443 [ACK] Seq=2 Ack=2 Win=64093 Len=0
291	8.541337	86.60.126.106	172.20.10.5	TCP	54 443 → 50148 [ACK] Seq=1 Ack=2109 Win=19440 Len=0
310	8.586389	89.35.237.180	172.20.10.5	TCP	54 80 → 50271 [ACK] Seq=1 Ack=334 Win=43008 Len=0

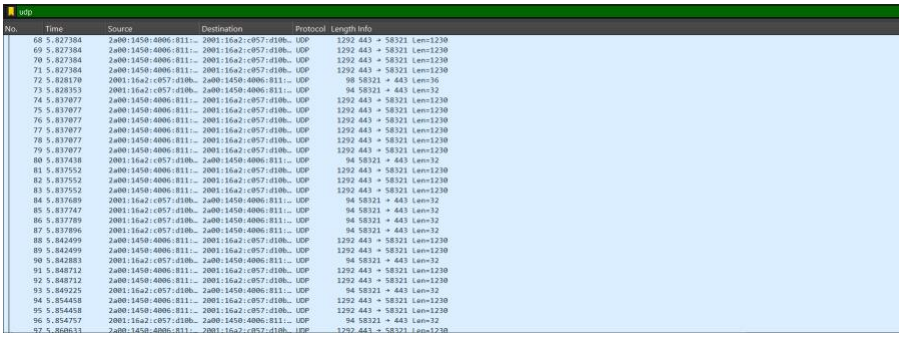
1. **Client FIN Packet:**
    - **Description:** The client initiates the termination by sending a FIN, ACK packet.
    - **Packet:** [FIN, ACK] Seq=1 Ack=1 Win=62420 Len=0
2. **Server ACK Packet:**
    - **Description:** Server acknowledges client's FIN

- **Packet:** [ACK] Seq=1 Ack=2 Win=3840 Len=0

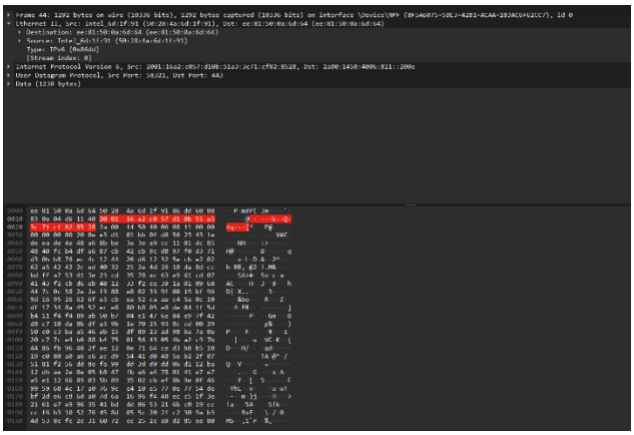
3. **Server FIN Packet:**
   - **Description:** Server initiates termination
   - **Packet:** [FIN, ACK] Seq=1 Ack=2 Win=3840 Len=0
4. **Client ACK Packet:**
   - **Description:** Client acknowledges server's FIN
   - **Packet:** [ACK] Seq=2 Ack=2 Win=62420 Len=0

Part 3:

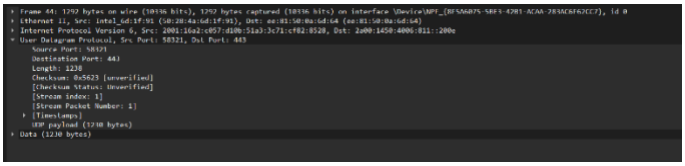
Task 2:



Step 3:



Step 4:



Step 5:

UDP headers are minimal, totaling only 8 bytes and containing fields like Source Port, Destination Port, Length, and Checksum. In contrast, TCP headers are more detailed, beginning at 20 bytes and featuring extra fields such as Sequence Number, Acknowledgment Number.

Part 4:

Task 1:

Category		Reasons
Reliability and Connection Establishment	**TCP**	**TCP is a connection-oriented protocol, which means it establishes a connection using a three-way handshake (SYN, SYN-ACK, ACK). It ensures reliable data transmission by acknowledging received packets and re-sending lost packets.**
Data Integrity and Ordering	**TCP**	**TCP ensures data integrity and maintains the correct order of packets. It assigns sequence numbers to packets, ensuring that data is received in the order it was sent. If any packets are missing or out of order, TCP will correct this by reordering or retransmitting them.**

Task 2:

	TCP	UDP
Use Cases	**File Transfer**	**Streaming**
Performance	**Slower due to connection establishment (3-way handshake), packet retransmission, and error checking.**	**Faster because it is connectionless and does not require acknowledgments or retransmissions.**