Task 1: TCP 3-Way Handshake

Questions:

1. Identify the packets corresponding to SYN, SYN-ACK, and ACK.
2. What are the source and destination IP addresses and ports for each packet?
3. What are the initial sequence and acknowledgment numbers?

Task 2: TCP Payload Analysis

Questions:

1. What is the TCP payload length of the first 5 data-carrying segments?
2. Which segment carries the largest payload?
3. Are there any zero-length TCP segments?

Task 3: TCP Retransmissions

Questions:

1. Identify all TCP retransmitted segments.
2. What are the sequence numbers of retransmitted segments?
3. How much time elapsed between the original transmission and the retransmission?

Task 4: Duplicate ACKs

Questions:

1. Identify all duplicate ACK packets.
2. Which sequence numbers do the duplicate ACKs acknowledge?
3. Did duplicate ACKs trigger a fast retransmission?

Task 5: TCP Stream Analysis

Questions:

1. Follow a TCP stream and identify the application protocol.
2. How many packets are exchanged in this TCP session?
3. Identify the first data-carrying packet.

Task 6: TCP Window Size and Scaling

Questions:

1. What is the advertised TCP window size for the server and client?
2. Is window scaling used? If yes, what is the scale factor?
3. Compute the effective window size using the scale factor.

Task 7: Selective Acknowledgment (SACK)

Questions:

1. Are there any SACK options in the capture? Identify packets.
2. Which segments were received out-of-order and acknowledged using SACK?

Task 8: Round Trip Time (RTT)

Questions:

1. Measure RTT for the first 5 TCP data segments.
2. Identify the corresponding ACK packets.
3. Compute the Estimated RTT using the TCP formula.

Task 9: Out-of-Order Packets

Questions:

1. Identify all out-of-order TCP packets.
2. What sequence numbers arrived out-of-order?
3. How did TCP handle these segments?

Task 10: Connection Termination

Questions:

1. Identify FIN and FIN-ACK packets.
2. What are the sequence and acknowledgment numbers?
3. How long did it take to close the connection?

Task 11: TCP Flags Analysis

Questions:

1. List packets with unusual TCP flags (PSH, URG, RST).

2. Identify segments with both SYN and FIN set.
3. Explain the purpose of each flag observed.