Session 11 Analyzing TCP Handshakes

1. Purpose of TCP Handshake
    - Establishes a reliable connection before data transfer.
    - Synchronizes sequence numbers between client and server.
    - Ensures both sides are ready for communication.

2. Steps of the 3-Way Handshake
    1. SYN: Client sends a synchronize packet with its Initial Sequence Number (ISN).
    2. SYN-ACK: Server responds with synchronize + acknowledgment, sharing its own ISN and acknowledging the client's.
    3. ACK: Client sends acknowledgment back to the server, completing the handshake.

3. Key TCP Flags
    - SYN → Start connection.
    - ACK → Acknowledge received packet.
    - FIN → Request to terminate connection.
    - RST → Reset the connection.
    - PSH → Push data to the receiving application immediately.

4. Analyzing Handshake in Wireshark
    - Use filter: `tcp.handshake` or `tcp.flags.syn==1`.
    - Identify the 3 packets:
        1. Client → Server: SYN
        2. Server → Client: SYN, ACK
        3. Client → Server: ACK
    - Check Sequence Numbers and Acknowledgment Numbers for correctness.
    - Confirm both sides agreed on initial sequence numbers.

5. Deeper Insights
    - Window Size: Controls how much data can be sent before acknowledgment.
    - Handshake Failures:
        - SYN Flood Attack: Multiple SYNs without final ACK.
        - RST Issues: Immediate resets indicating rejection.
        - Retransmissions: Sign of packet loss or connectivity issues.

Summary:
The TCP 3-way handshake is the process that sets up a reliable connection. It is simple (SYN → SYN-ACK → ACK), but analyzing it in Wireshark provides insights into connection health, security issues, and troubleshooting network problems.