Objective 1: **Show students the TCP header fields by generating a real TCP connection (HTTP) using the Web Browser tool in Packet Tracer.**

1 Create the Topology

- Drag **1 PC** and **1 Server** into the workspace.
- Connect them with a **Copper Straight-Through cable** (via a switch if you like).

Example:

```
PC0  <—>  Switch0  <—>  Server0
```

2 Assign IP Addresses

- Click PC0 → Desktop → IP Configuration
  - IP: 192.168.1.2
  - Subnet: 255.255.255.0
  - Gateway: 192.168.1.1 (if using router)
- Click Server0 → Desktop → IP Configuration
  - IP: 192.168.1.3
  - Subnet: 255.255.255.0

3 Turn On HTTP Service on the Server

- Click **Server0** → Services tab
- On the left, select **HTTP**
- Check **On** at the top (this enables the built-in web server)
- Optionally edit the webpage content.

4 Switch to Simulation Mode

- At the bottom-right corner, click **Simulation** (next to "Realtime").

5 Generate HTTP (TCP) Traffic from PC0

- On PC0 → Desktop → Web Browser
- In the URL bar, type: `http://192.168.1.3` (server's IP)
- Click **Go**.
- This makes a TCP connection to port 80.

6 Capture the Packet

- In Simulation mode, you'll see a packet icon appear in the **Event List** below.
- Click **Capture/Forward** step by step to move the packet.

7 Inspect the TCP Header

- In the **Event List**, click the packet event (Outbound PDU) → PDU Information window opens.

- Go to the **Inbound/Outbound PDU Details** tab.
- Expand **Layer 4 (TCP)**.
- You'll see:
  - **Source Port**
  - **Destination Port** (80)
  - **Sequence Number**
  - **Acknowledgment Number**
  - **Flags** (SYN, ACK, etc.)
  - **Window Size**, Checksum, Urgent Pointer…

Show students how these change between the SYN, SYN-ACK, and ACK packets (the three-way handshake) by stepping through multiple events.

Objective 2: **Demonstrate that DNS uses UDP, and let students inspect the UDP header fields in Packet Tracer.**

1 Build the Topology

- Drag **one PC** and **one Server** into the workspace.
- Connect them directly with a copper straight-through cable (or via a switch).

Example:

```
PC0  <──>  Server0
```

2 Configure IP Addresses

- **PC0**
  - Desktop → IP Configuration
  - IP Address: `192.168.1.2`
  - Subnet Mask: `255.255.255.0`
  - **DNS Server**: `192.168.1.3` (the server's IP)
- **Server0**
  - Desktop → IP Configuration
  - IP Address: `192.168.1.3`
  - Subnet Mask: `255.255.255.0`

3 Enable DNS Service on the Server

- Click **Server0** → Services tab → DNS
- Switch **DNS Service** to **On**.
- Under **Resource Records**, add a record:
  - Name: `test.com`
  - Address: `192.168.1.3` (or any IP you like)
  - Click **Add**

This means the server will resolve `test.com` for the PC.

4 Switch to Simulation Mode

- At the bottom-right, click **Simulation**.

5 Generate a DNS Query from the PC

- On **PC0** → Desktop → Web Browser
- In the URL bar type: `http://test.com`
- Click **Go**.

Because the PC has no cached DNS entry for `test.com`, it will first send a **DNS query** to the DNS server at `192.168.1.3` using **UDP port 53**.

6 Capture the DNS Packet

- In the **Event List** (Simulation panel) you'll see a packet with **DNS** label appear before the HTTP/TCP packets.
- Click that DNS packet to open the **PDU Information** window.
- Go to the **Inbound/Outbound PDU Details** tab.
- Expand **Layer 4 (UDP)**.
- You'll see:
    - **Source Port**: random ephemeral port (e.g. 1025)
    - **Destination Port**: 53
    - **Length**
    - **Checksum**

This is the **UDP header**.

7 (Optional) Show the DNS Reply

- Step through with **Capture/Forward**.
- When the reply comes from the server, click it and again check Layer 4 (UDP):
    - **Source Port**: 53
    - **Destination Port**: your PC's ephemeral port

This shows the full UDP request/response cycle.