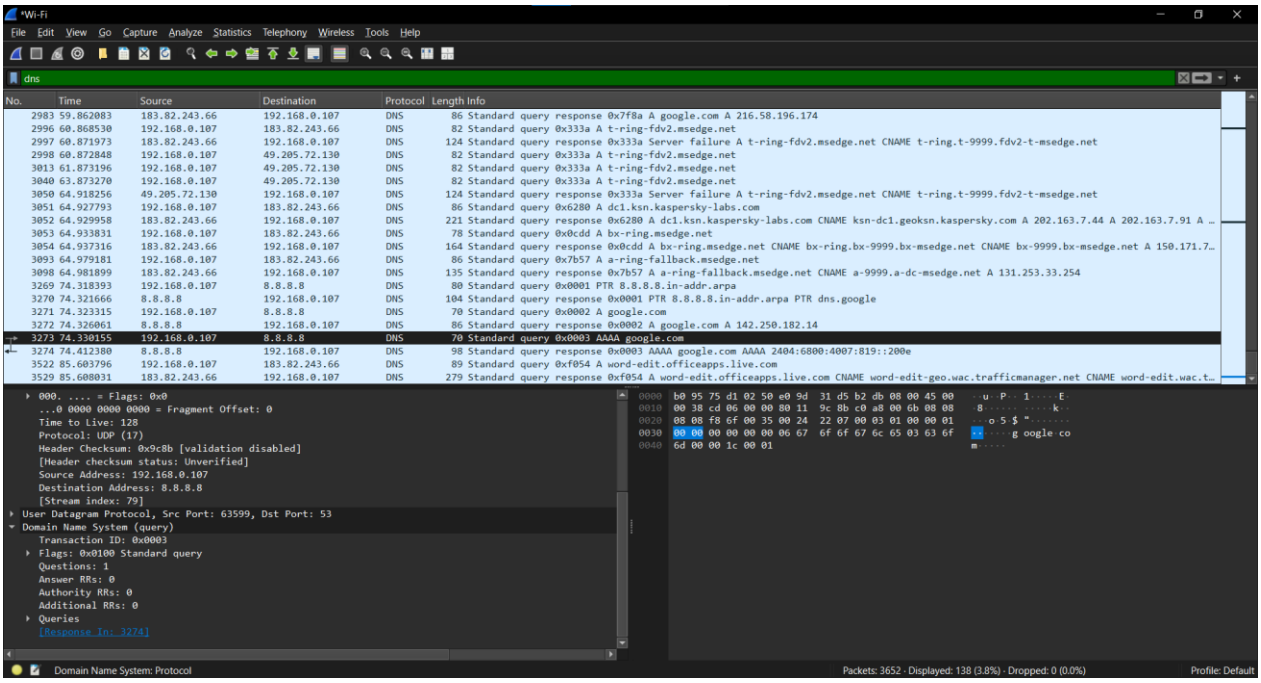
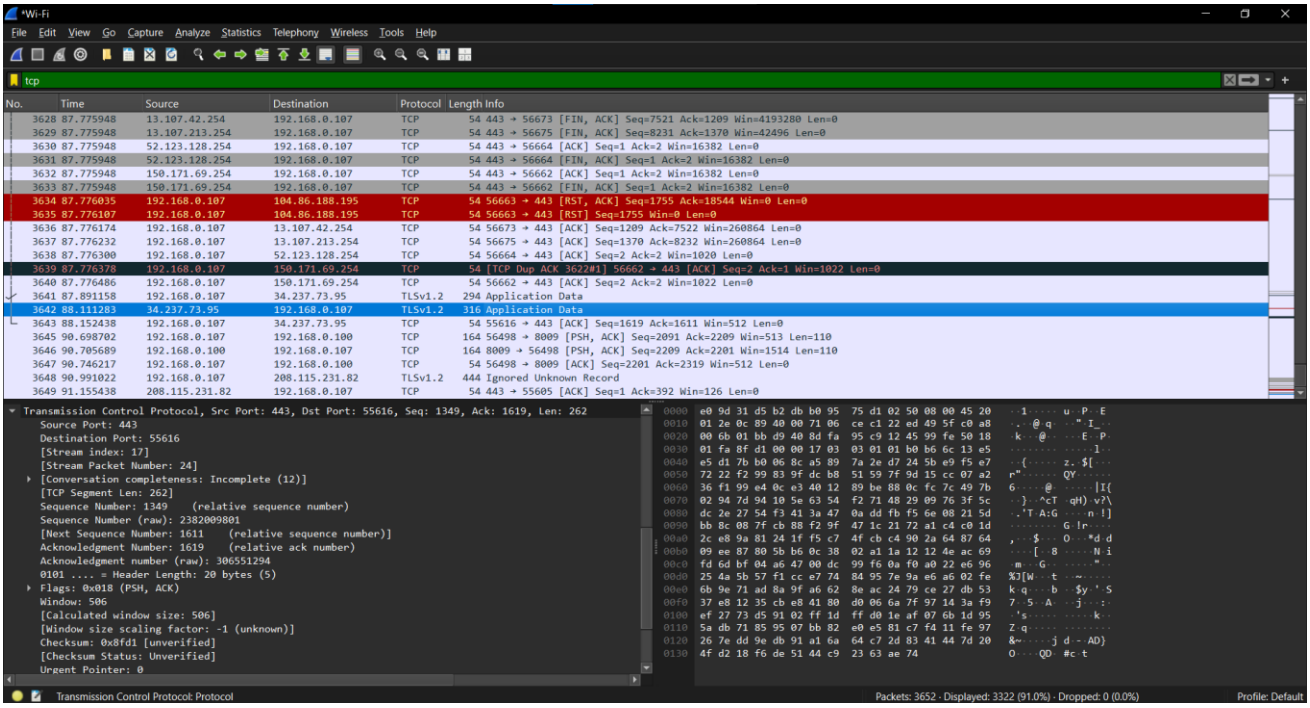
Q2) Use Wireshark to capture and analyze DNS, TCP, UDP traffic and packet header, packet flow, options and flags

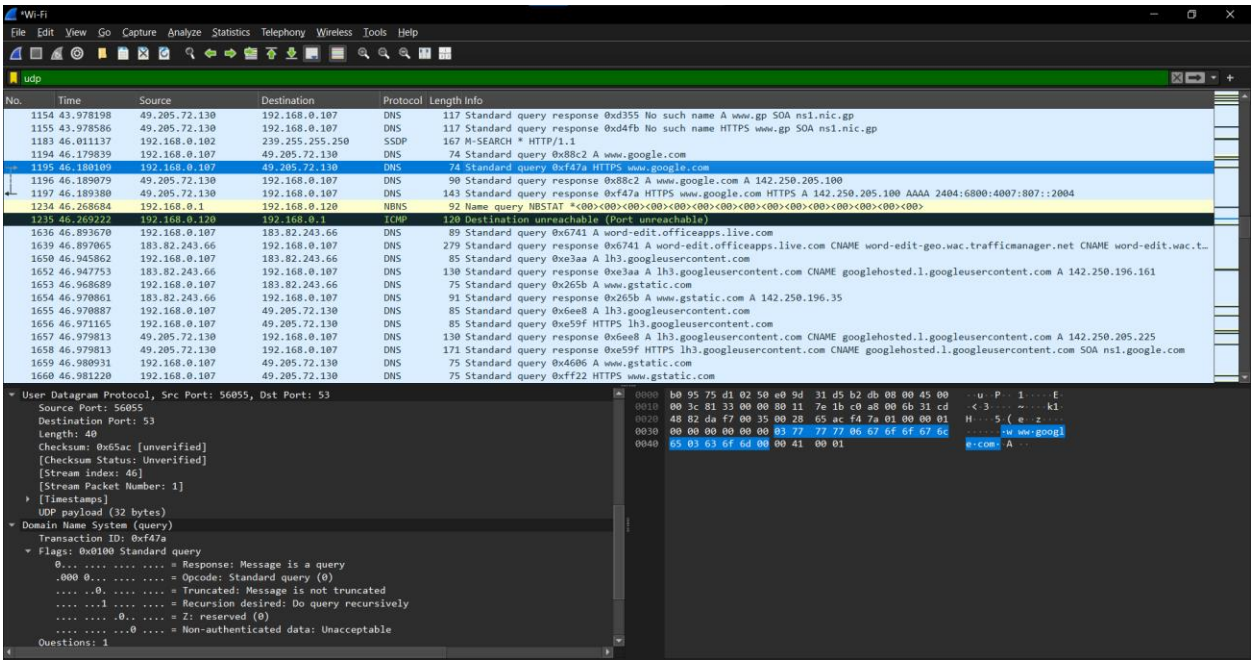
DNS



TCP



UDP



What is TCP?

- **Connection-oriented** protocol.
- Ensures **reliable** and **ordered** data transmission.
- Uses **error checking** and **retransmission** if packets are lost.
- Establishes a connection **before** sending data (3-way handshake).

How TCP Works?

1. **Three-Way Handshake** (Before data transfer)
    a. **Step 1:** Client sends SYN (synchronize) to the server.
    b. **Step 2:** Server responds with SYN-ACK (synchronize + acknowledge).
    c. **Step 3:** Client replies with ACK (acknowledge).
    d. Now, the connection is **established**, and data transfer begins.
2. **Data Transfer**
    a. Data is sent in **segments**.
    b. Each segment has a **sequence number**.
    c. The receiver **acknowledges** received segments.
    d. Lost packets are **retransmitted**.
3. **Connection Termination**
    a. Either side sends a `FIN` (finish) flag to close the connection.

What is UDP?

- **Connectionless** protocol (No handshake).
- **Faster** than TCP but **less reliable**.
- No retransmission of lost packets.

How UDP Works?

1. Sender **transmits** data without checking if the receiver is ready.
2. Receiver **processes** the data but does not send an acknowledgment.
3. If a packet is lost, **no retransmission** happens.

What is DNS?

- Converts **domain names** (e.g., `google.com`) into **IP addresses** (`142.250.190.78`).
- Uses **UDP (Port 53)** for quick responses.
- Uses **TCP** for large responses (e.g., zone transfers).

How DNS Works?

1. User types `www.google.com` in the browser.
2. The system sends a **DNS Query** to a DNS server.
3. DNS server replies with the **IP address** of `google.com`.
4. The system uses this IP address to **connect** to the website.