Task 3: Network Traffic Analysis Report

Name: Mohammed Fadil PK **Date:** January 19, 2026

1. Introduction

Network analysis is the process of capturing and inspecting data packets as they move across a network. For this task, I used **Wireshark** to analyse TCP handshakes, DNS queries, and the difference between secure (HTTPS) and insecure (HTTP) traffic.

2. Observations & Analysis

A. The TCP 3-Way Handshake

- **Concept:** Before data is sent, devices must establish a connection. This is called the "Handshake."
- **Observation:** I filtered for tcp and observed the three steps:
    1. **SYN:** My computer sent a request to the server to connect.
    2. **SYN-ACK:** The server acknowledged and accepted the request.
    3. **ACK:** My computer confirmed the connection.

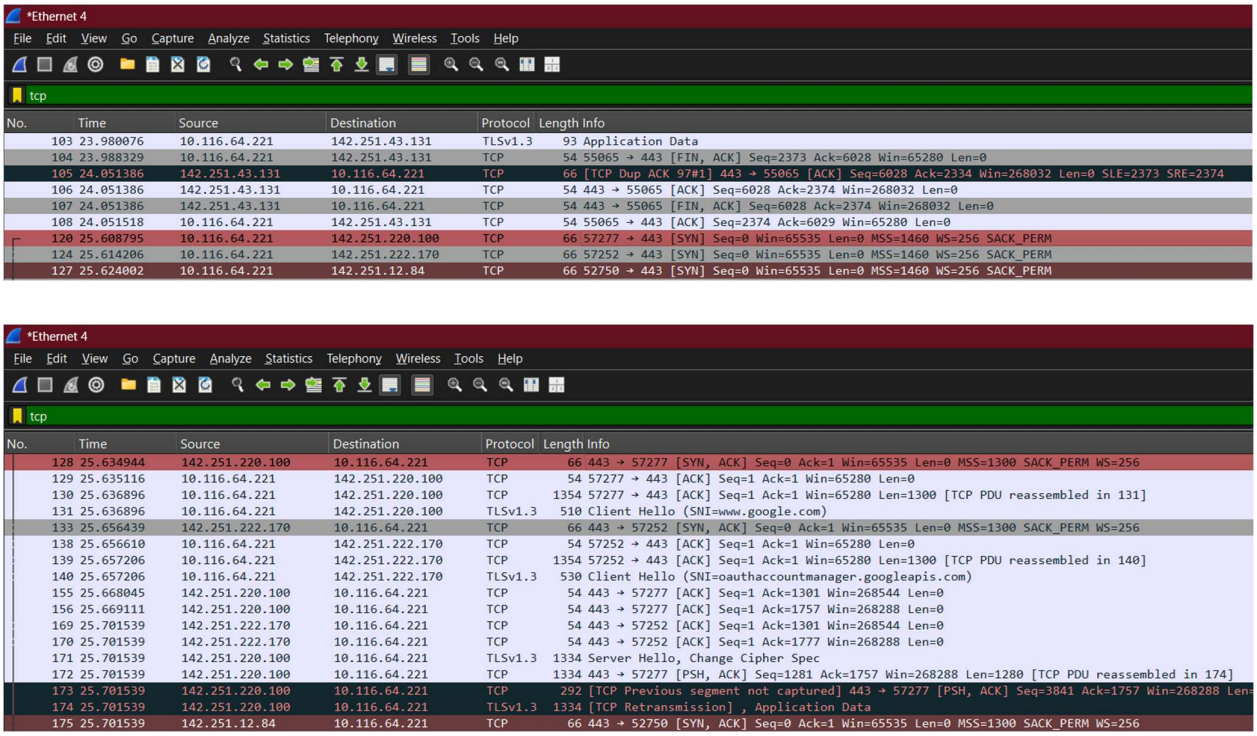

Fig 1: Wireshark capture showing the TCP 3-Way Handshake (SYN, SYN-ACK, ACK)

B. DNS Traffic Analysis

- **Concept:** DNS (Domain Name System) converts human names (like https://www.google.com/url?sa=E&source=gmail&q=google.com) into IP addresses (like 142.250.206.78).
- **Observation:** I filtered for dns and pinged a website. I captured the "Query" packet asking for the IP address and the "Response" packet providing it.

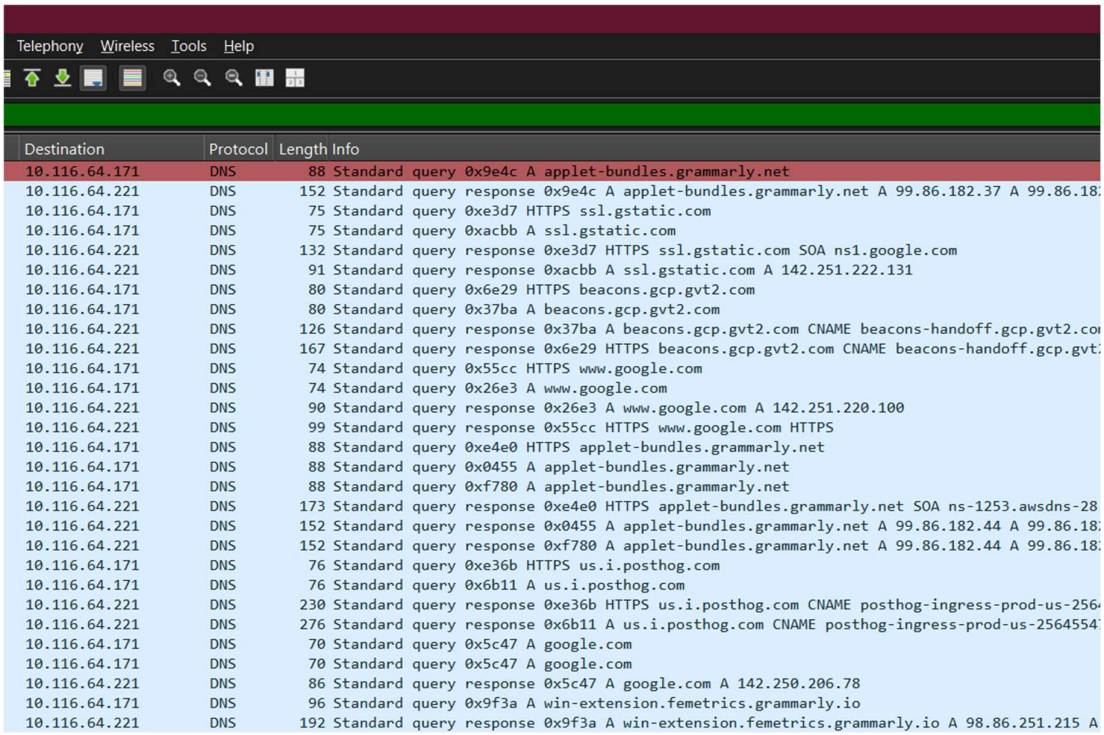

Fig 2: DNS Traffic analysis showing the standard query and response for https://www.google.com/search?q=google.com

C. HTTP vs. HTTPS (Security Check)

- **HTTP (Port 80):** Traffic is sent in **plain text**. If I entered a password on an HTTP site, a hacker using Wireshark could read it easily.
- **HTTPS (Port 443):** Traffic is **encrypted** using TLS/SSL. In Wireshark, the data looks like random scrambled characters ("Application Data"), making it secure from sniffing.

3. Interview Questions & Answers

1. **What is the TCP Handshake?** It is the process used to establish a reliable connection between a client and server. It involves three steps: SYN (Synchronise), SYN-ACK (Synchronise-Acknowledge), and ACK (Acknowledge).
2. **What is the difference between TCP and UDP?**
    - **TCP (Transmission Control Protocol):** Reliable. It checks if data arrived correctly (used for emails, websites).
    - **UDP (User Datagram Protocol):** Fast but unreliable. It sends data without checking if it arrived (used for video streaming, gaming).
3. **What is packet sniffing?** The act of capturing and monitoring data packets flowing across a network using tools like Wireshark. It can be used for debugging (by admins) or stealing data (by hackers).
4. **Why is HTTPS more secure than HTTP?** HTTPS uses encryption (TLS) to scramble data. Even if a hacker captures the packets, they cannot read the contents. HTTP sends data in plain text, which is easily readable.