Wireshark Live Packet Capture Report

Task 5

From: Gautam Oza

Objective

The objective of this activity is to capture live network packets and identify basic protocols and traffic types using Wireshark. This includes analyzing various traffic types such as TCP, UDP, TLS, QUIC, and DNS, and interpreting their role in the network communication.

Tool Used

Wireshark (Free and open-source packet analyzer).

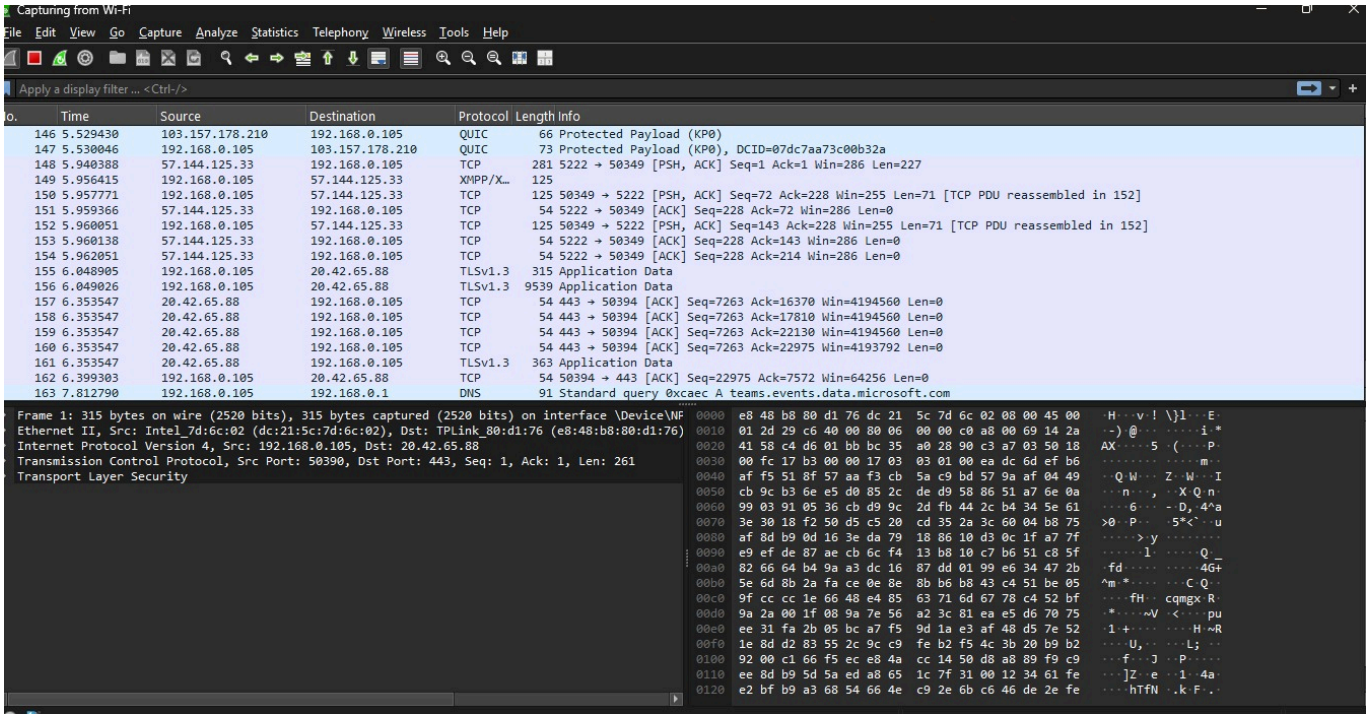
Observations and Findings

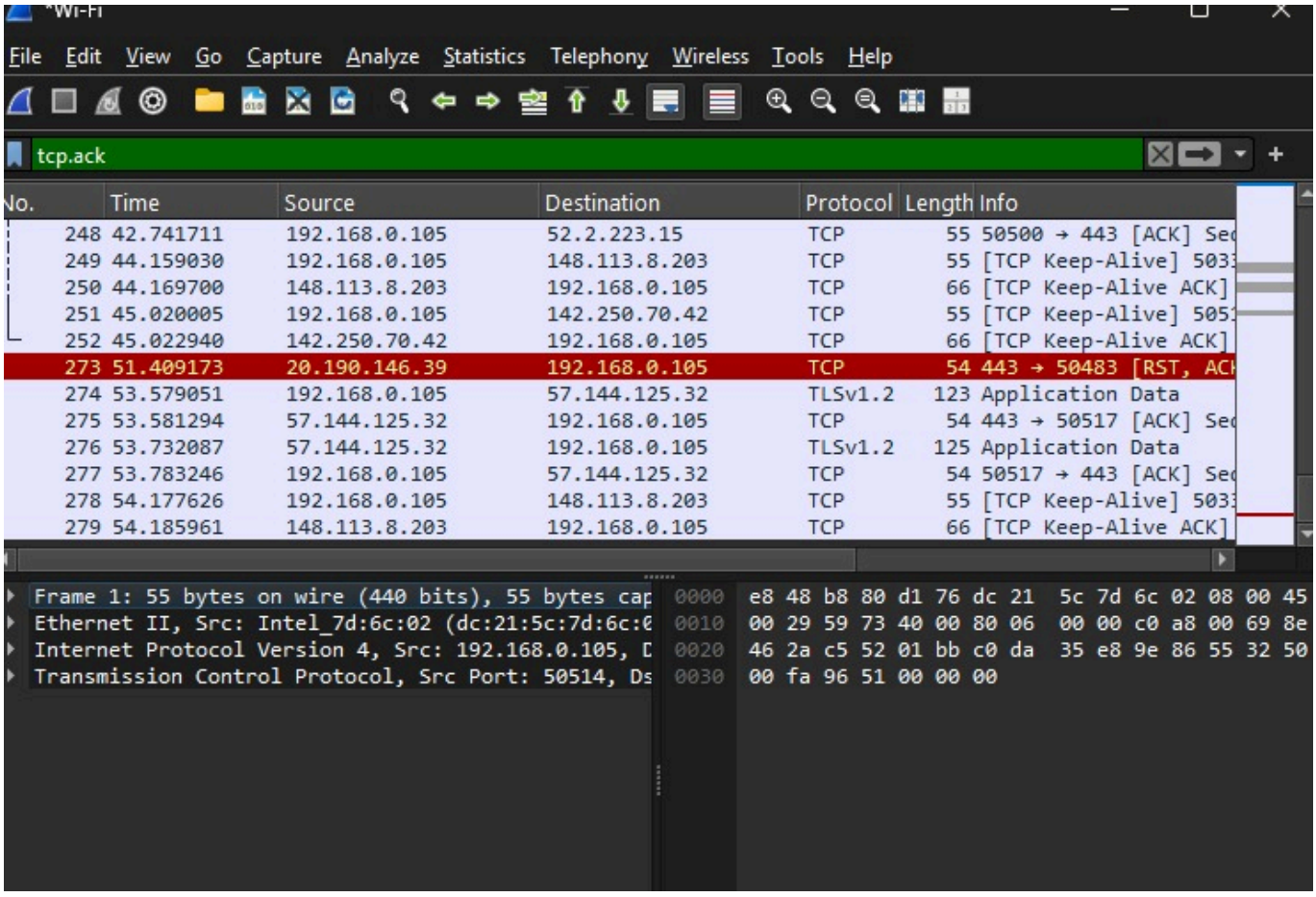
1. **TCP Traffic**: Multiple TCP streams were captured, including acknowledgment (ACK) packets and keep-alive signals, indicating ongoing connections.
2. **TLS/SSL Traffic**: Presence of TLS 1.3 encrypted packets shows secure communication, possibly HTTPS traffic.
3. **QUIC Protocol**: Observed QUIC packets, often used by HTTP/3, indicating modern web traffic.
4. **DNS Queries**: Queries to domains such as 'teams.events.data.microsoft.com' indicate communication with Microsoft services.
5. **UDP Multicast Streams**: Detected mDNS and SSDP multicast traffic, typically used for local network service discovery.
6. **RST Packets**: Presence of TCP RST (Reset) packets suggests some connections were forcefully closed.

Captured Evidence

Below are the screenshots from Wireshark showing the captured packets and analysis windows.

Wireshark Live Packet Capture Report





Wireshark Live Packet Capture Report