Task 5: Capture and Analyze Network Traffic Using Wireshark

Objective:
Capture live network packets and identify basic protocols and traffic types using Wireshark.

Tool Used:
Wireshark (Version: [Insert version])

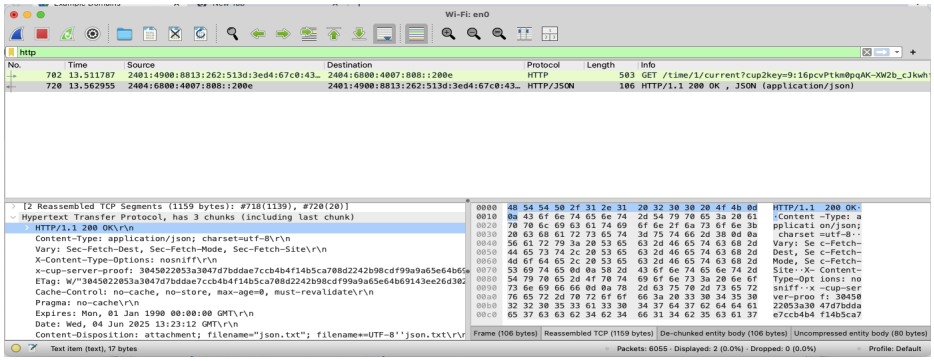
Steps Performed:

1. **Installed Wireshark** on the system.
2. **Selected active network interface** (Wi-Fi) for live packet capture.
3. Generated traffic by:
    - **Browsing a website** (https://example.com)
    - **Pinging** 8.8.8.8 (Google DNS)
    - **Sending email**
4. Stopped capture after approximately **1 minute**.
5. Applied protocol filters in Wireshark (http, dns, tcp, udp, tls, icmp, mdns, etc.)
6. Identified 3+ distinct protocols from the captured traffic.
7. Exported capture file as: task5_traffic_analysis.pcap

Protocols Identified:-

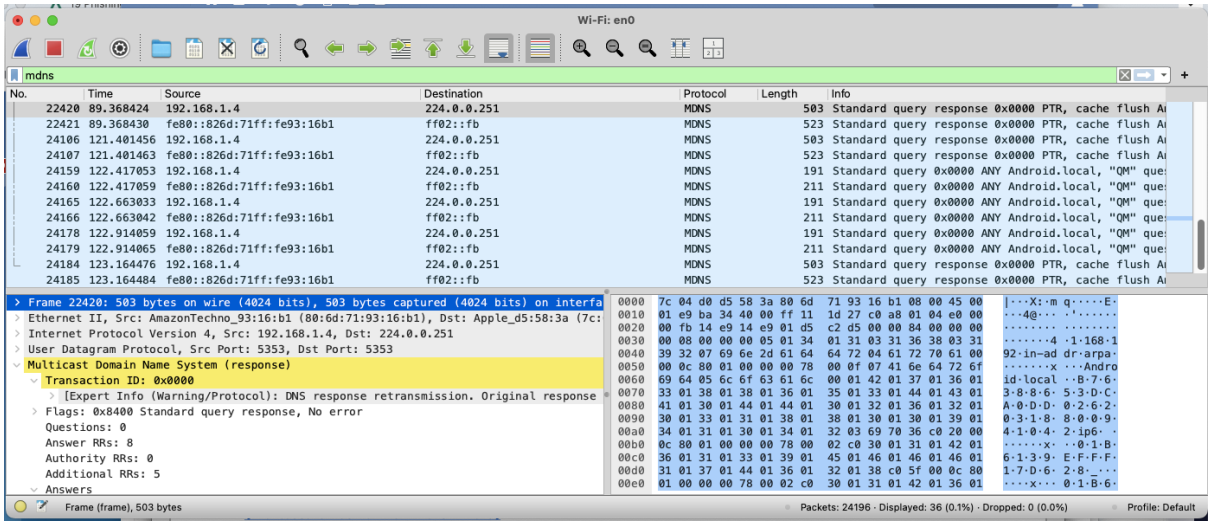
Different Protocols Sample Packet Captured are:-

1. **HTTP (HyperText Transfer Protocol):**
    - The Hyper Text Transport Protocol is a text-based request-response client-server protocol.
    - Sample HTTP Packet captured:
        - **Source port:** 80
        - **Destination port:** 49414
        - **Method:** GET
        - **Response Code:** 200 OK
        - **Screenshot:**



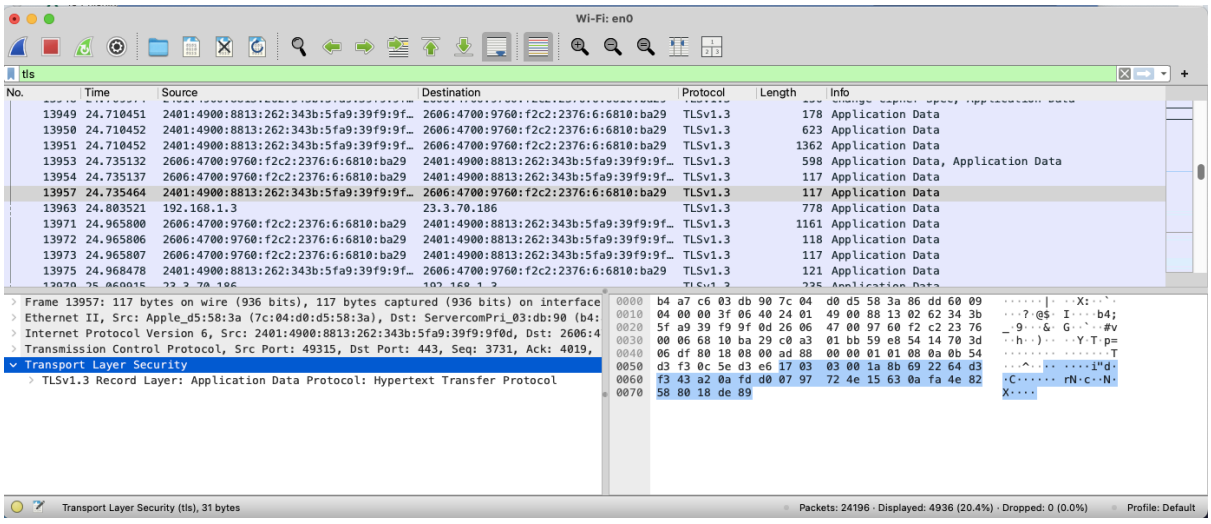
2. MDNS(Multicast DNS [mDNS] :

- mDNS is a protocol that facilitates zero-configuration networking, enabling devices on a local network to discover and resolve hostnames without needing a central DNS server.
- mDNS utilizes the User Datagram Protocol (UDP) and specifically port 5353 for communication.
- Sample MDNS packet captured Screenshot:



3. TLSv1.3 (Transport Layer Security v1.3):

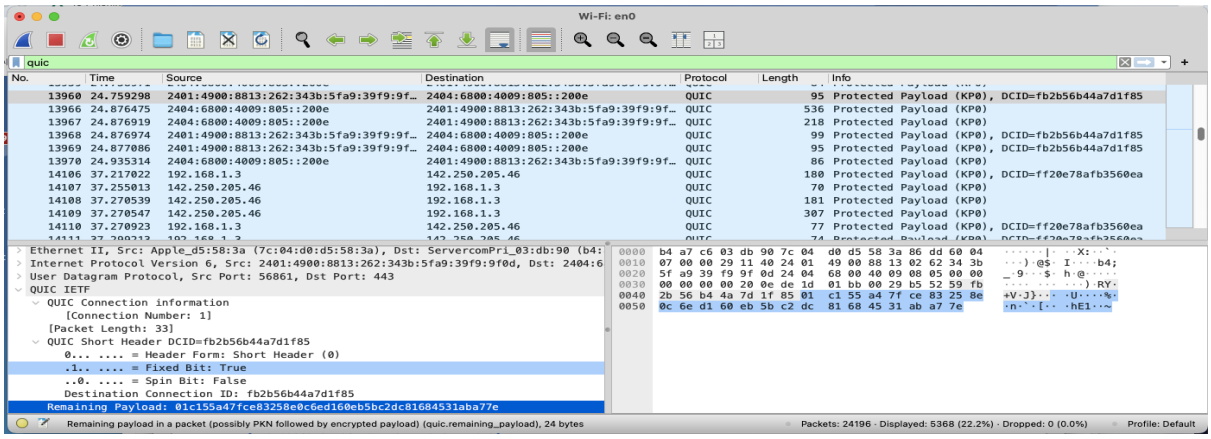
- TLS 1.3 is a secure communication protocol used to encrypt internet traffic between a client and a server. Packet inspection refers to the process of analyzing network packets to identify specific patterns or characteristics. When it comes to TLS 1.3 packet inspection, it can be challenging due to its encryption and lack of predictable packet structure.
- Sample TLS packet captured Screenshot:



4. QUIC (Quick UDP Internet Connections):

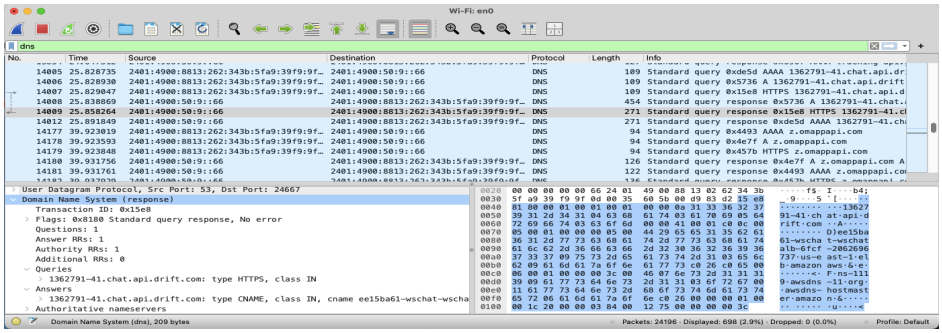
- QUIC is based on UDP: QUIC uses UDP as its transport protocol, but it adds features like connection multiplexing and flow control.
- Encrypted at the transport layer: QUIC mandates encryption for all connections, unlike TCP where it's optional.
- TLS handshake: QUIC uses a TLS handshake to establish a secure connection and encryption.
- HTTP/3 uses QUIC: HTTP/3 is built on top of QUIC.

- QUIC packet inspection refers to the process of analyzing and understanding the contents of packets transmitted over the QUIC (Quick UDP Internet Connections) protocol. QUIC is a transport-layer protocol designed to provide security, reliability, and efficiency for internet communications.
- It involves examining the packet headers, payloads, and other metadata to gain insights into the communication patterns, protocol errors, and potential security vulnerabilities.
- Sample QUIC packet captured Screenshot:



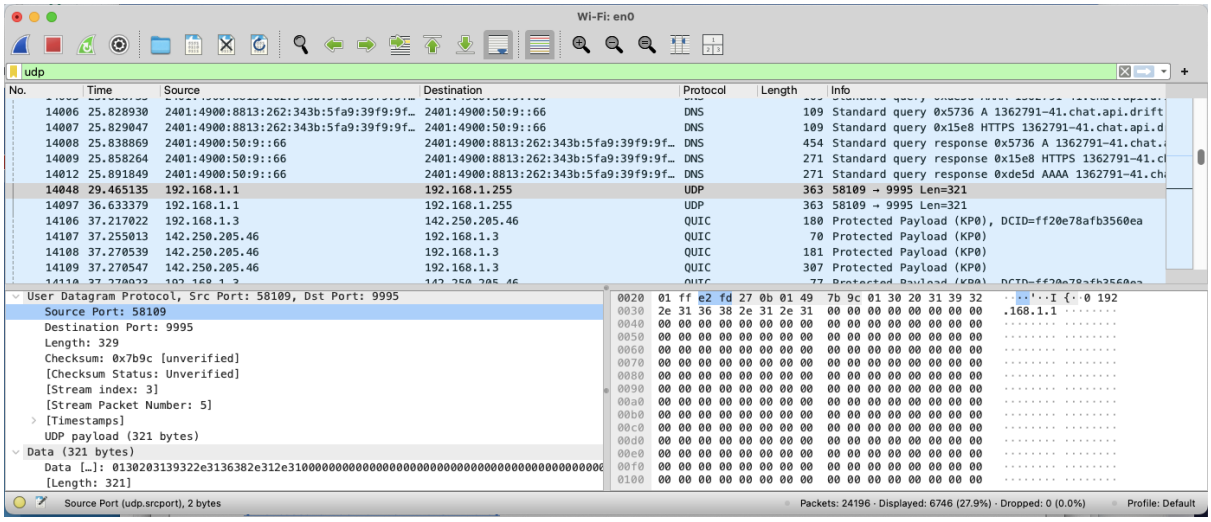
5. DNS (Domain Name System):

- DNS is a fundamental protocol on the internet, enabling users to access websites using human-friendly domain names rather than IP addresses.
- DNS typically uses UDP (User Datagram Protocol) for queries, but can also use TCP (Transmission Control Protocol) for certain types of queries.
- Wireshark's DNS dissector is fully functional and can help in various analyses, including security investigations and performance monitoring.
- Understanding DNS is crucial for network security, as malicious actors can exploit DNS for various attacks, such as domain hijacking or DNS poisoning.
- Sample DNS packet captured Screenshot:



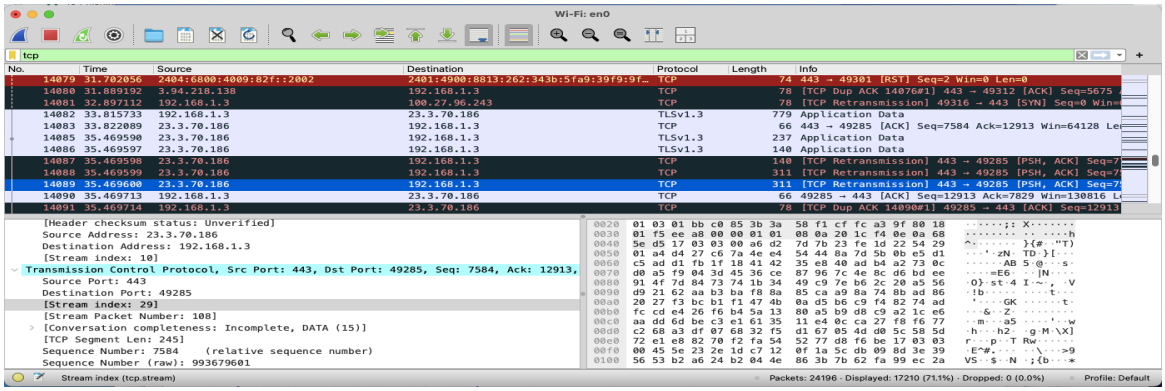
6. UDP (User Datagram Protocol):

- UDP is a connectionless protocol used for applications like DNS and streaming where speed is prioritized over guaranteed delivery.
- Sample UDP packet captured Screenshot:



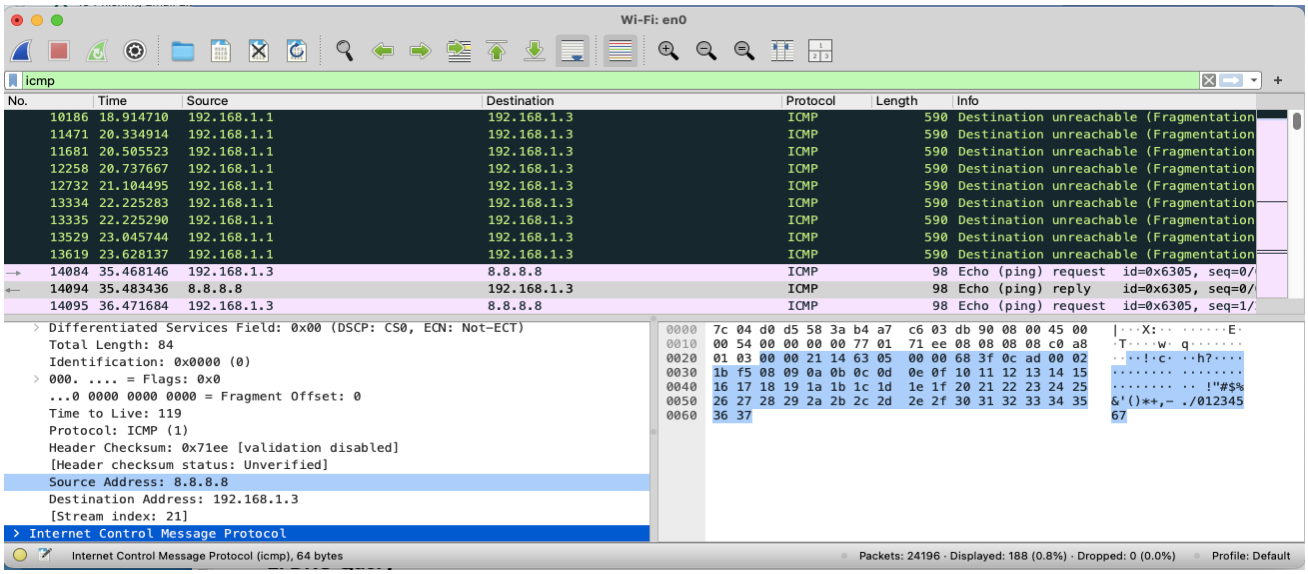
7. TCP(Transmission Control Protocol):

- Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.
- Sample TCP packet captured Screenshot:



8. **ICMP(Internet Control Message Protocol):**

- ICMP is a protocol used for error-reporting and diagnostic functions, including ping and traceroute.
- Understanding ICMP protocol in Wireshark is essential for network administrators and engineers to identify and resolve connectivity issues. This knowledge helps to optimize network performance and troubleshoot problems.
- Sample ICMP packet analysis:
  - **Type:** Echo Request (ping to 8.8.8.8)
  - **Reply:** Echo Reply received
  - **Source Address :** 8.8.8.8
  - **Destination Address :** 192.168.1.3
  - **Screenshot -**



4. Protocol : ICMP

Deliverable:

- **Packet Capture File (.pcap):** task5_traffic_analysis.pcap
- [You would normally attach/upload this file]

🧠 **Summary:**

The network traffic captured shows standard protocol usage:

- **HTTP** and **DNS** for website browsing
- **TCP** underlying all connections
- Optional **ICMP** from ping activity
  No suspicious or malicious activity was observed in the brief capture window. The exercise demonstrates baseline protocol behavior during normal network use.