**Wireshark Packet Capture Analysis Report**

**1. Introduction**

The objective of this task was to capture live network traffic using Wireshark and analyze the packets to identify different protocols. This hands-on exercise provides insight into how data is segmented, addressed, and transmitted across a network using various protocols.

**2. Methodology**

1. Wireshark was started, and packet capture was initiated on the active network interface.
2. General internet browsing and network activity generated background traffic for capture.
3. The capture was stopped after a short duration.
4. The captured packets were analyzed, and three distinct protocols (DNS, TCP, and UDP) were identified for this report.

**3. Packet Analysis and Identified Protocols**

Here is a detailed analysis of one packet for each of the three core protocols identified in the capture.

**A. DNS (Domain Name System) - Packet #1**

* **Protocol:** DNS (over UDP)
* **Source Address:** 192.168.242.239 (Local Client)
* **Destination Address:** 192.168.242.94 (Local DNS Server)
* **Source Port:** 55302
* **Destination Port:** 53 (Standard DNS Port)
* **Brief Description:** This is a DNS query packet. The client is asking its DNS server for the IP address (A record) associated with the domain name teams.events.data.microsoft.com. This type of query is essential for converting human-readable website addresses into machine-readable IP addresses, allowing the connection to be established. DNS primarily uses the UDP protocol for these queries due to its low overhead and speed.
* **Purpose:** Domain Name Resolution.

**B. TCP (Transmission Control Protocol) - Packet #7**

* **Protocol:** TCP
* **Source Address:** 2600:1f18:24e6:b902:ad6c:a4a6:87fe:c14c (Remote Server)
* **Destination Address:** 2409:40e0:4f:6e05:a407:6679:a201:60b5 (Local Client)
* **Source Port:** 443 (HTTPS)
* **Destination Port:** 57348 (Local Client Port)
* **Brief Description:** This packet is part of a TCP connection, specifically a keep-alive or acknowledgment packet. The [ACK] flag is set, indicating it is acknowledging previously received data (Ack=806). The sequence number (Seq=1) and acknowledgment number are used to ensure reliable, in-order data delivery. This packet has a payload length of 0 (Len=0), meaning it carries no application data and is purely for maintaining the connection state, which is common in encrypted HTTPS sessions running over TCP.
* **Purpose:** Reliable, connection-oriented data delivery and session management.

**C. UDP (User Datagram Protocol) - Packet #2**

* **Protocol:** UDP
* **Source Address:** 2409:40e0:4f:6e05:e407:6679:e201:60b5 (Local Client)
* **Destination Address:** 2405:200:1606:1731::312c:b0c8 (Remote Server)
* **Source Port:** 56190
* **Destination Port:** 443 (HTTPS)
* **Brief Description:** This packet carries encrypted application data. The destination port 443 indicates this UDP packet is part of an **HTTPS** connection, likely using the QUIC protocol (which is the basis for HTTP/3). Unlike the TCP packet, this UDP packet contains a 35-byte payload of encrypted data. This demonstrates how modern web traffic is increasingly moving to UDP for reduced latency and improved performance, while still maintaining security through encryption at the application layer.
* **Purpose:** Fast, connectionless transport of encrypted web traffic (QUIC/HTTP/3).

**4. Summary of Findings**

The analysis of these packets reveals a modern network communication flow:

1. **DNS (UDP)** is used for the initial, fast resolution of a domain name (teams.events.data.microsoft.com).
2. **TCP** is observed managing a reliable, stateful connection to a web server, ensuring data integrity through acknowledgments, even for an encrypted HTTPS stream.
3. **UDP** is not only used for traditional lightweight tasks but is also employed for carrying high-performance, encrypted web traffic (QUIC), showcasing an evolution in protocol usage.

This exercise successfully demonstrated the practical use of Wireshark for capturing and analyzing network packets, reinforcing the distinct roles and characteristics of DNS, TCP, and UDP in real-world network communications.