Network Traffic Analysis Report

1. Introduction

This report provides a simple analysis overview using a synthetic network capture file. The purpose is to demonstrate understanding of basic network traffic concepts, including TCP handshake, DNS, and encrypted vs plaintext traffic.

2. Tools Used

• Wireshark (or equivalent tools like tcpdump, Microsoft Network Monitor)

3. Overview of Packet Capture

A minimal synthetic PCAP file was generated containing a valid global header and one empty packet entry. This allows basic demonstration of packet structure even if real traffic could not be captured.

4. Key Networking Observations

• A PCAP file always begins with a global header describing format and link type.

• Each packet entry contains a timestamp, captured length, actual length, and packet data. In this synthetic capture, the packet contains 0 bytes of data.

5. Concept Explanations

- ### TCP Handshake
  The TCP three-way handshake is used to establish a reliable connection: SYN → SYN-ACK → ACK.

- ### DNS (Domain Name System)
  DNS converts user-friendly domain names (e.g., google.com) into IP addresses that machines understand.

- ### Plaintext vs Encrypted Traffic
  HTTP and some legacy protocols transmit data in readable plaintext. HTTPS, using TLS encryption, protects data so that intercepted packets cannot reveal actual content.

6. Conclusion

Even with a synthetic capture file, fundamental concepts of network traffic analysis can be understood, including packet structure, protocols, and security considerations.