Network Traffic Analysis Report

1. Introduction

This report presents the analysis of network traffic captured using Wireshark. The goal of this task was to capture live network packets, filter them by protocol, and identify the key types of traffic and communication patterns. The findings are based on the analysis of a sample capture session performed on an active network interface.

2. Objective

The primary objective was to capture and analyze live network traffic, identify at least three different protocols, and provide details about their purpose, common use cases, and the role they play in network communication.

3. Tools Used

- Wireshark (latest version)
- Active internet connection
- Windows/Linux environment

4. Protocols Identified and Analysis

4.1 HTTP (Hypertext Transfer Protocol)

HTTP is an application-layer protocol used for transmitting hypermedia documents, such as HTML. It is the foundation of data communication for the World Wide Web. In the capture, HTTP packets were observed when accessing websites, which included request and response messages. This protocol operates over TCP, typically using port 80, and does not encrypt its contents, making it less secure compared to HTTPS. HTTP is essential for loading webpages, transferring resources, and enabling interaction between web browsers and servers.

4.2 DNS (Domain Name System)

DNS is a protocol that translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network. It is a critical component of the internet infrastructure. In the capture, DNS queries and responses were recorded when websites were accessed, mapping domain names to their respective IP addresses. DNS commonly operates over UDP on port 53 but can also use TCP for larger queries and zone transfers. Without DNS, users would have to remember numerical IP addresses for every site they want to visit.

4.3 TCP (Transmission Control Protocol)

TCP is a transport-layer protocol that provides reliable, ordered, and error-checked delivery of data between applications. It is connection-oriented, meaning that a connection must be established before data can be transferred. In the capture, TCP packets were seen as the underlying transport for protocols like HTTP and HTTPS. TCP ensures that all packets

arrive in the correct order and retransmits lost packets if necessary. It operates alongside IP, forming the TCP/IP model that underpins the internet.

5. Summary

The capture and analysis exercise provided practical insight into how different network protocols operate together to enable seamless communication over the internet. HTTP was observed for web content transfer, DNS for resolving domain names, and TCP for ensuring reliable packet delivery. Understanding these protocols is fundamental for network analysis, troubleshooting, and cybersecurity tasks.