Network Traffic Analysis Report

Date: October 17, 2025
Course: Computer Networks Lab
Assignment: Wireshark Traffic Capture and Protocol Analysis

Capture Overview

A snapshot of the network capture reveals the distribution of protocols. An analysis of the 1,244 packets shows the following key metrics:

- **Total Packets Captured:** 1,244
- **Dominant Protocol:** UDP (47.4% of traffic)
- **Primary Traffic Type:** IPv4 (80.2% of packets)

Most Active Protocols by Packet Count

The chart below illustrates the proportion of total traffic represented by each major protocol. The data clearly shows that UDP-based traffic (including DNS and QUIC) is the most significant component of the capture.

Protocol Breakdown:

- **DNS:** 22.5%
- **QUIC:** 10.1%
- **TCP:** 19.9%
- **HTTP:** 8.8%
- **Other UDP:** 14.8%
- **Other Protocols:** 23.9%

Protocol Breakdown

Each protocol plays a unique role in network communication. The following is a summary of the function for each major protocol identified within this specific network capture.

Domain Name System (DNS)

DNS accounted for 22.5% of all packets. This traffic was generated when the browser needed to translate human-readable domain names (like wikipedia.org) into machine-readable IP addresses. Because DNS lookups need to be fast, they use the connectionless UDP protocol.

User Datagram Protocol (UDP) & QUIC

UDP was the most active transport protocol at 47.4%. While a large part of this was DNS, 10.1% was from QUIC. QUIC is a modern transport protocol from Google that runs over UDP and is the foundation for HTTP/3. It's designed to be faster and more efficient than TCP.

Transmission Control Protocol (TCP)

TCP made up 19.9% of the packets and is the workhorse for reliable data transfer. Its role was to establish stable connections using its "three-way handshake" before any web data could be exchanged. It ensures that all parts of a webpage arrive in the correct order without errors.

Hypertext Transfer Protocol (HTTP) & TLS

HTTP (8.8%) is the protocol for fetching web pages. In this capture, most of the web traffic was encrypted using TLS (Transport Layer Security), which runs on top of TCP. Even though secure sites were browsed, some initial redirection from HTTP might have occurred, which is why HTTP packets are visible.

Internet Control Message Protocol (ICMP)

ICMP is used for network diagnostics. This traffic was generated exclusively by the ping 8.8.8.8 command. These packets appear as "Echo (ping) request" sent from the machine and "Echo (ping) reply" coming back from the server.

Security Analysis

A review of the captured packets was conducted to identify anomalies or potential threats.

All Clear: No Suspicious Traffic Detected

All captured network communications were directly attributable to the explicit actions performed during the lab exercise (web browsing and ping commands). Source and destination IP addresses were consistent with expected services like Google's DNS and known websites. No unsolicited connections, unusual port usage, or anomalous packet flags were observed, indicating the network activity was normal and benign.

Key Learnings

The analysis provided several practical insights into the fundamental principles of network communication.

1. **Protocol Sequencing:** A simple action like visiting a website is a multi-step process. The capture clearly showed the sequence: DNS resolves the name, TCP establishes a connection, and HTTP/TLS transfers the data.
2. **The Right Tool for the Job:** UDP is used for fast, connectionless tasks like DNS. TCP is used for reliable, connection-oriented transfers like loading a webpage, ensuring all data arrives correctly.
3. **Making the Abstract Visible:** Wireshark makes abstract networking concepts tangible. It deconstructs traffic, revealing the headers, flags, and data that control communication, turning theory into practice.
4. **The Power of Filtering:** Manually inspecting thousands of packets is impossible. Display filters are essential for isolating specific conversations and conducting a focused, efficient investigation.