Network Traffic Analysis Report

Generated from Wireshark Capture Analysis

October 17, 2025

Abstract

This report presents an analysis of a network traffic capture performed using Wireshark. The objective is to identify the primary network protocols in use, examine the contents of representative packets, and interpret the overall communication patterns observed within the capture. The analysis covers key protocols including TCP/TLS, UDP/QUIC, DNS, and ICMP, providing insights into typical secure web browsing and network diagnostic activities.

1 Introduction and Objective

The goal of this analysis is to deconstruct a captured network session to understand the underlying operations of modern internet communication. By inspecting packet-level data, we can observe the sequence of events for common user activities, such as visiting a secure website or checking network connectivity. This exercise serves to practically demonstrate the roles and interactions of fundamental network protocols. The analysis is based on a capture containing 24,876 packets.

2 Protocol Hierarchy Analysis

An initial overview of the captured traffic was obtained from the Wireshark Protocol Hierarchy statistics. This provides a quantitative breakdown of all protocols detected in the capture, revealing which protocols are most active. The distribution is summarized in Table 1.

Table 1: Protocol Hierarchy Statistics

Protocol	Percent Packets	Packets
Transmission Control Protocol (TCP)	**71.7%**	**17,841**
Transport Layer Security (TLS)	46.7%	11,614
Hypertext Transfer Protocol (HTTP)	0.1%	36
User Datagram Protocol (UDP)	**25.4%**	**6,327**
QUIC IETF	22.1%	5,494
Domain Name System (DNS)	1.2%	294
Internet Control Message Protocol (ICMP)	**0.1%**	**18**

Key Insights from Statistics

- **Dominance of Secure Web Traffic:** The capture is overwhelmingly dominated by TCP traffic at 71.7%. Within this, TLS accounts for 46.7% of all packets, indicating that the vast majority of the communication is encrypted HTTPS traffic for secure web browsing.

- **Presence of Modern Protocols:** UDP constitutes a significant portion of the traffic (25.4%), with the QUIC protocol being the largest contributor (22.1%). QUIC is a modern transport protocol developed by Google, often used for its own services (like YouTube, Google Search) to reduce connection latency. Its strong presence points to interaction with such modern web services.
- **Essential Network Services:** DNS and ICMP traffic are present but in much smaller volumes. DNS (1.2%) is used for domain name resolution, a necessary precursor to web browsing. The very low volume of ICMP traffic (0.1%) suggests it was used for isolated network diagnostics, such as a 'ping' command.

3 Detailed Packet Examination

To understand the function of these protocols, individual packets were filtered and examined. The following sections describe the findings for each major protocol.

3.1 ICMP (Internet Control Message Protocol)

ICMP traffic was isolated to observe network diagnostics. The capture shows ICMP Echo (ping) requests originating from the local IP address `10.21.16.170` and directed to Google's public DNS server at `8.8.8.8`. This is a standard method for verifying internet connectivity and network latency. Each request packet is 74 bytes long.

3.2 DNS (Domain Name System)

DNS traffic is responsible for translating human-readable domain names into machine-readable IP addresses. The capture shows the local host `10.21.16.170` sending DNS queries for various domains, including `prod.do.dsp.mp.microsoft.com`. This traffic uses UDP as its transport protocol and is a fundamental step that must occur before a TCP connection to a web server can be established.

3.3 TCP/TLS (Secure Web Traffic)

Filtering by `tcp.port == 443` isolates the encrypted web traffic. The capture clearly shows the TLS handshake sequence between the client (`10.21.16.170`) and a web server. This includes the "Client Hello," "Server Hello," and "Certificate" messages, which are part of the process to negotiate a secure, encrypted session. Once the handshake is complete, the application data is exchanged, but its contents are encrypted by TLS and not visible in the capture.

3.4 Summary of Examined Packets

A summary of representative packets is provided in Table 2.

Table 2: Representative Packet Details

Protocol	Source IP	Destination IP	Length	Info
ICMP	10.21.16.170	8.8.8.8	74 bytes	Echo (ping) request
HTTP (TLS)	10.21.16.170	40.44.185.185	66 bytes	TCP Handshake [ACK]
DNS	10.21.16.170	172.16.1.80	252 bytes	Standard query response

4 Conclusion

The analysis of the Wireshark capture successfully identified the protocols and communication patterns of a typical internet user session. The data shows a network environment heavily reliant on secure protocols like TLS and QUIC for web browsing, confirming the modern web's shift to an "encrypted-by-default" model. The roles of foundational services like DNS for name resolution and ICMP for diagnostics were also clearly observed. No suspicious or malicious activity was detected; all traffic corresponds to standard, expected network behavior.