Network Traffic Analysis Report

Name: Pranshu Deep **Roll No.:** 2301MC59 **Course:** Computer Networks Lab **Assignment:** Wireshark Traffic Capture and Protocol Analysis **Date:** October 17, 2025

---

1. Objective

The objective of this analysis was to capture live network traffic using Wireshark while performing standard web browsing and network diagnostic activities. This report summarizes the findings from the captured data, focusing on the most active protocols, observed communication patterns, and key insights into the underlying network operations.

---

2. Most Active Protocols

The packet capture was performed while visiting websites (youtube.com, wikipedia.org) and running a ping command to 8.8.8.8. Analysis of the captured packets in capture_lab6.pcapng reveals that the traffic was dominated by standard web and network protocols.

The primary protocols observed were:

- **Transmission Control Protocol (TCP):** This was the most active transport layer protocol, responsible for the reliable delivery of web content. It carried the data for HTTP and TLS (HTTPS) sessions.
- **User Datagram Protocol (UDP):** This protocol was primarily used for Domain Name System (DNS) queries and also for QUIC traffic, a modern transport protocol used by Google services.
- **Transport Layer Security (TLS):** As most modern websites use HTTPS, the TLS protocol was highly active, encrypting the application data (like HTTP) between the client and web servers.
- **Domain Name System (DNS):** DNS traffic was observed at the beginning of web requests, used to translate human-readable domain names (e.g., www.wikipedia.org) into their corresponding IP addresses.
- **Internet Control Message Protocol (ICMP):** This protocol was generated exclusively by the ping 8.8.8.8 command to check for network connectivity.

---

3. Suspicious or Unusual Traffic

During the analysis, **no suspicious or malicious traffic was detected**. All captured packets were consistent with the actions performed (web browsing and pinging). The traffic consisted of standard protocols like DNS, TCP, TLS, and ICMP communicating with well-known public IP addresses (e.g., Google's DNS at 8.8.8.8, and the IP addresses for the websites visited). The presence of protocols like ARP and QUIC is also normal for a typical network environment.

---

4. Key Insights and Communication Patterns

The capture provided several key insights into the sequential and layered nature of network communication.

- **DNS Precedes Web Traffic:** The first step in accessing a website is a DNS lookup. The capture clearly shows that before any TCP connection was made to a web server, a DNS query was sent to a DNS server to resolve the website's name to an IP address. For instance, a query for www.wikipedia.org had to be resolved before the browser could connect to its server.
- **ICMP for Network Diagnostics:** The ping command demonstrated the function of ICMP. As seen in the icmp filter screenshot, the local machine (192.168.29.141) sent a series of ICMP "Echo (ping) request" packets to the destination (8.8.8.8), which responded with "Echo (ping) reply" packets. This confirms a live and reachable connection path between the two hosts.
- **The HTTP Request/Response Cycle:** The HTTP filter revealed the fundamental communication pattern for unencrypted web browsing. The client sent an HTTP GET request to the server (93.184.216.34 for example.com) to ask for the webpage content. The server then responded with the requested data.
- **Prevalence of Encryption (HTTPS/TLS):** While the filter for http successfully isolated traffic to example.com, very little other web traffic was seen using this filter. This is because most modern sites, including wikipedia.org, force connections over HTTPS. This encrypted traffic runs over TCP port 443 and is encapsulated within the TLS protocol, highlighting the modern web's focus on security. This was confirmed by the custom filter ip.src == 192.170.10.0 && (tcp.port == 80 || tcp.port == 443), which showed significant traffic on port 443 (HTTPS).

---

5. Conclusion

This Wireshark lab successfully demonstrated the ability to capture, filter, and analyze live network traffic. The exercise provided practical insight into the roles of essential protocols like DNS, TCP, ICMP, and HTTP. The key takeaway is that simple user actions, such as visiting a webpage, involve a complex and rapid sequence of underlying network communications that can be effectively observed and understood using network analysis tools.