Wireshark Network Analysis Report

Name: Abhinandan Porwal
Course: Computer Networks
Date: October 17, 2025

1. Overview

This report summarizes the network traffic captured during the Wireshark session. The analysis focuses on identifying the most active protocols, detecting any suspicious or unusual activity, and drawing key insights about network communication patterns.

2. Most Active Protocols

Protocol	Packet Count	Description
HTTP	210	Used for web browsing and application data transfer.
DNS	73	Resolves domain names to IP addresses.
ICMP	26	Used for network diagnostics (ping/traceroute).
TCP	405	Reliable data transmission; includes handshakes and data transfer.
ARP	31	Resolves MAC addresses to IP addresses within LAN.

3. Suspicious or Unusual Traffic

During the analysis, the following unusual patterns were observed:

1. Multiple ICMP Echo Requests: High frequency of ping requests from a single host could indicate network scanning activity.
2. Unknown External Connections: A few TCP packets were directed to external IP addresses not recognized in the network inventory.
3. Malformed Packets: Some packets showed inconsistencies in header lengths or flags, which may indicate errors or probing attempts.

(Screenshots of suspicious packets should be inserted here.)

4. Key Insights

1. Protocol Usage Trends: HTTP and DNS dominate the traffic, reflecting active web browsing and network name resolution.
2. Network Health: ARP and ICMP traffic indicates normal LAN operation and connectivity checks.
3. Potential Security Alerts: Unusual ICMP bursts and unexpected TCP connections highlight the need for monitoring.
4. Communication Patterns: Most internal communication occurs via TCP, indicating reliable data transfer within the network.

5. Deliverables

- Packet Capture Files: capture.pcap (original), filtered.pcap (filtered for analysis)
- Screenshots: Screenshots of notable traffic and anomalies
- Report: report.pdf (this document)