Network Packet Capture Report

Date: 2025-06-02

Analyst: Jetan Bhargav N

Tool Used: Wireshark v4.x

Interface Used: Wi-Fi (802.11)

1. Objective

To capture live network packets using Wireshark and identify commonly used protocols and traffic types in a real-world network environment.

2. Methodology

- Wireshark was launched and packet capture was initiated on the primary wireless interface.
- Network activity was generated by browsing websites, pinging domains, and opening a few applications to stimulate varied traffic.
- The capture was run for approximately 5 minutes.
- After the capture, the session was saved in .pcap format for analysis.

3. Protocols Identified

Protocol	Port(s) Used	Description	Observed Usage
ARP	N/A	Resolves IP addresses to MAC	Initial communication on LAN
DNS	53 (UDP/TCP)	Domain name resolution	Detected for every site visited
HTTP	80 (TCP)	Unencrypted web traffic	Some sites still serve HTTP content
HTTPS	443 (TCP)	Encrypted web traffic	Majority of web browsing

TCP | Various | Reliable transport layer protocol | Backbone for most communications

UDP | Various | Lightweight transport protocol | Used in DNS, some streaming apps

ICMP | N/A | Ping/traceroute and diagnostics | Detected during ping google.com

TLSv1.2/1.3 | 443 (TCP) | Encryption layer for HTTPS | Seen in most HTTPS connections

4. Traffic Summary

- Total packets captured: ~2,300 - Average packet size: ~300 bytes - Top talkers (IP addresses):

- Local IP: 192.168.1.10 (Client)

- DNS Server: 192.168.1.1 (Router)

- External: 142.250.190.xxx (Google)

5. Observations

- Over 70% of the traffic was HTTPS, indicating secure communication is now the norm.

- DNS queries occurred consistently as new domains were accessed.

- ICMP packets verified network connectivity and were manually triggered.

- Minimal HTTP traffic was observed, likely from legacy services or redirects.

- ARP broadcasts occurred regularly, suggesting normal LAN behaviour.

Conclusion

The network traffic captured using Wireshark shows a typical modern network environment dominated by secure web traffic (HTTPS), regular DNS lookups, and system-level protocols like ARP and ICMP. This analysis demonstrates basic proficiency in using Wireshark for protocol inspection and traffic categorization.