Network Traffic Analysis Report

Date: 12 Aug 2025
Tool Used: Wireshark 4.2.3
Capture File: capture_analysis_12Aug2025.pcapng
Duration of Capture: 1 minute 12 seconds
Interface Monitored: Wi-Fi (Intel AX201)

1. Objective

The objective of this analysis was to capture live packets on the local network to identify basic protocols in use and verify network traffic flow during normal browsing activity.

2. Summary of Activity During Capture

- Accessed the websites:

- example.com
- wikipedia.org
- Performed ICMP ping tests to 8.8.8.8 (Google DNS).
- No intentional malicious activity was generated.

3. Protocol Overview

Protocol	Packet Count	% of TotalTraffic	Description
TCP	482	61%	Transport layer traffic for HTTP(S) and other applications.
DNS	36	4.5%	Domain name lookups for visited websites.
HTTP	22	2.8%	Unencrypted HTTP web requests.
HTTPS	230	29%	Encrypted web browsing (TLS over TCP).

ICMP	18	2.3%	Ping requests and replies to 8.8.8.8.

4. Key Packet

a) DNS Query

- **Time:** 12.435 s
- **Source:** 192.168.0.105
- **Destination:** 8.8.8.8
- **Info:** Standard query A www.wikipedia.org

b) HTTP Request

- **Time:** 20.302 s
- **Source:** 192.168.0.105
- **Destination:** 93.184.216.34 (example.com)
- **Info:** GET / HTTP/1.1

c) ICMP Echo Request/Reply

- **Time:** 45.981 s
- **Source:** 192.168.0.105 → 8.8.8.8
- **Info:** Echo (ping) request, seq=14

- **Reply:** 8.8.8.8 → 192.168.0.105, Echo reply, seq=14

5. Observations

- The majority of traffic was **TCP-based**, mostly encrypted HTTPS.
- Small volume of unencrypted HTTP traffic observed to example.com (likely for testing).
- DNS queries were sent primarily to 8.8.8.8, showing the system is using Google Public DNS.
- ICMP traffic confirms successful connectivity to an external host.

6. Conclusion

The captured traffic indicates normal, non-malicious activity typical of general web browsing and connectivity tests. HTTPS dominated the data flow, ensuring data confidentiality. Unencrypted HTTP requests, although minimal, could expose sensitive information if used with login forms.

7. Recommendations

- Use HTTPS whenever possible to protect confidentiality.
- Restrict unnecessary ICMP access in firewall rules to reduce exposure.
- Monitor DNS traffic for unusual domains to detect possible malware activity.