Network Traffic Analysis Report

---

1. Report Overview

This report presents the analysis of live network traffic captured using Wireshark. The purpose of this analysis is to understand basic networking behavior, identify commonly used protocols, and evaluate the security posture of network communication by distinguishing between encrypted and unencrypted traffic.

---

2. Objective

The objectives of this task are as follows:

- To capture live network traffic in a controlled environment.
- To analyze common network protocols used in day-to-day communication.
- To observe TCP connection establishment mechanisms.
- To identify plain-text and encrypted traffic.
- To develop foundational packet analysis skills relevant to SOC operations.

---

3. Environment Details

- **Operating System:** Kali Linux (Virtual Machine)
- **Tool Used:** Wireshark
- **Capture File Format:** PCAPNG
- **Network Interface:** Wi-Fi / Ethernet
- **Capture Type:** Live network traffic

---

4. Packet Capture Details

- **Capture File Name:** task3_network_capture.pcapng
- **Capture Duration:** 183.4 secs
- **Total Packets Captured:** 6068
- **Capture Date:** 19/01/2026

5. Protocols Observed

The following protocols were identified during the packet analysis:

- **TCP (Transmission Control Protocol):** Reliable, connection-oriented communication
- **UDP (User Datagram Protocol):** Fast, connectionless communication
- **DNS (Domain Name System):** Resolves domain names to IP addresses
- **HTTP:** Unencrypted web communication
- **HTTPS (TLS):** Encrypted and secure web communication

---

6. TCP Three-Way Handshake Analysis

Display Filter Used:
tcp.flags.syn == 1

Observation:

The TCP connection establishment was observed using the standard three-way handshake process:

1. SYN packet sent from client to server
2. SYN-ACK packet sent from server to client
3. ACK packet sent from client to server

Conclusion:
The TCP three-way handshake confirms reliable and successful connection establishment between communicating systems.

---

7. DNS Traffic Analysis

Display Filter Used:
dns

Observation:

- DNS queries were observed requesting IP addresses for domain names
- DNS responses returned resolved IP addresses
- DNS communication primarily used UDP port 53

Conclusion:
DNS plays a critical role in network communication by enabling domain name resolution.

8. HTTP vs HTTPS Traffic Analysis

HTTP Filter:
http

HTTPS Filter:
tls

Observation:

- HTTP traffic transmitted data in plain text, making it readable
- HTTPS traffic was encrypted using TLS and not readable

Security Impact:
Plain-text HTTP traffic is vulnerable to interception, whereas HTTPS protects data confidentiality and integrity through encryption.

---

9. Plain-Text vs Encrypted Traffic Comparison

Traffic Type	Data Visibility	Security Risk
HTTP	Readable	High
HTTPS	Encrypted	Low

---

10. Security Findings

- Unencrypted protocols increase exposure to network-based attacks
- Packet sniffing can reveal sensitive information over plain-text protocols
- Encrypted communication significantly reduces security risks
- Network traffic analysis is essential for identifying insecure communication patterns

---

11. Limitations

- Analysis is limited to captured traffic only
- Encrypted payloads cannot be inspected without decryption keys
- No malicious traffic was intentionally generated during capture

---

12. Conclusion

This task provided practical exposure to network traffic analysis using Wireshark. It strengthened foundational cybersecurity skills such as packet inspection, protocol identification, and basic security assessment, which are essential for entry-level SOC and Blue Team roles.

13. Learning Outcome

- Hands-on experience in PCAP analysis
- Improved understanding of networking protocols
- Ability to distinguish between secure and insecure communication
- Increased readiness for SOC analyst responsibilities

---

14. Analyst Details

Name: Parijat Das
Role: Cybersecurity Intern