

Network Traffic Analysis Report — Task 5

Prepared By : Arti kumari

Date: 20 Nov 2025

Tool Used: Wireshark

Target: Active Network Interface (Wi-Fi)

1. Objective

The purpose of this task was to capture and analyze live network traffic using Wireshark, identify basic protocols, and understand how data flows between the system and external servers.

2. Methodology

- Installed and launched **Wireshark**.
 - Selected the **Wi-Fi interface** for capturing packets.
 - Performed browsing activity (visited a website) and executed a **ping command** to generate traffic.
 - Captured packets for ~1 minute.
 - Applied filters (dns, tcp, http) to analyze specific protocols.
 - Saved results in .pcap format.
-

3. Scan Summary

- **Total Capture Duration:** 1 minute •
File Saved As: task5_capture.pcap
 - **Protocols Identified:**
 - **DNS** → Domain resolution queries and responses.
 - **TCP** → Reliable connection for data transfer.
 - **ICMP** → Ping request and replies for connectivity testing.
 - **HTTP/HTTPS** → Web browsing traffic.
-

4. Observations

- **DNS Queries:** My system sent queries to resolve domain names (e.g., <https://aihumanize.io/>) to IP addresses.
- **TCP Sessions:** TCP connections were established for communication with web servers.

- **ICMP Packets:** Detected ping packets, confirming network connectivity testing.
 - **HTTP/HTTPS Traffic:** Showed browsing activity, but HTTPS packets were encrypted.
-

5. Conclusion

The Wireshark capture successfully recorded live traffic on my PC. The analysis confirmed the presence of **multiple protocols (DNS, TCP, ICMP, HTTP/HTTPS)**.

This exercise helped me understand how everyday actions like browsing or pinging a server generate identifiable network packets.
