Network Traffic Analysis Report

Task 5 – Internship Project

Name: Bhatt Jaymeenbhai Shaileshbhai

Date: 4 June 2025

Tool: Wireshark

---

1. Objective

To capture live network traffic and identify at least three protocols using Wireshark.

---

2. Environment

- Operating System: Windows 10

- Tool: Wireshark v4.x

- Network: Wi-Fi (Home Network)

---

3. Actions Performed

- Wireshark installed with NPcap.

- Active Wi-Fi interface selected.

- Traffic generated by visiting google.com and pinging external servers.

- Captured for ~1 minute.

---

4. Protocols Identified

A. DNS (Domain Name System)

- Port: 53 (UDP)

- Used to resolve `google.com` to an IP address.

- Example Packet:

- Query: `A google.com`

- Response: `142.250.195.46`

B. HTTP (HyperText Transfer Protocol)

- Port: 80 (TCP)

- Captured unencrypted HTTP requests.

- Shows headers and resource paths.

C. TCP (Transmission Control Protocol)

- Used for reliable data transport.

- Seen in combination with HTTP and DNS.

- Example: SYN, ACK, and FIN flags observed in handshake and termination.

---

5. Observations

- IP addresses involved: `192.168.29.41` (Local), `8.8.8.8` (Google DNS)

- Ping requests seen as ICMP Echo Request and Reply.

- Packet size varied by protocol.

---

6. Conclusion

Successfully identified multiple protocols in live traffic. Understood how packet headers reveal protocol behavior. Gained confidence in basic packet analysis.

---

7. Attachments

- `network\_capture.pcap`: Raw packet data