Task-5

Capture and Analyze Network Traffic Using Wireshark

Title: Network Packet Capture & Protocol Analysis using Wireshark
Tool Used: Wireshark
Network: Wi-Fi on Windows Laptop

Objective

To capture live network traffic and analyze common protocols such as DNS, TCP, and ICMP by filtering and inspecting packet details in Wireshark.

Methodology (Steps Performed)

1. Installed **Wireshark** along with **Npcap** for network capture.
2. Started capturing packets on the active **Wi-Fi** interface.
3. Generated network traffic by browsing websites and interacting with online services.
4. Stopped the capture after sufficient traffic was collected.
5. Applied filters (dns, tcp, icmp) to analyze different protocol behaviors.
6. Examined packet details, including IP addresses, ports, queries, acknowledgments, and data payloads.
7. Exported the packet capture file (.pcapng) as required.

Protocols Identified & Analysis

Below are the key protocols extracted from the captured packets:

---

1. **DNS** – ***Domain Name System***

- **Purpose:** Converts domain names (e.g., google.com) to IP addresses.
- **Evidence from screenshot:**
    - Query: cloudnetworks.com (or similar domain name)
    - Protocol: DNS Query via **UDP Port 53**
    - Source IP: **192.168.31.1** → Local network
    - Destination IP: **cloudflare DNS / public DNS**

This confirms DNS resolution activity while browsing.

---

2. TCP – *Transmission Control Protocol*

- **Purpose:** Ensures reliable data delivery between server & client.
- **Observed details:**
    - Connection to HTTPS services: **Port 443**
    - Flags: ACK (Acknowledgment), showing ongoing stable communication
    - Source: Public IPv6 address
    - Seq/Ack numbers show packet exchange reliability

This traffic likely belongs to an encrypted HTTPS session (browsing, streaming, etc.).

3.UDP / ICMP / QUIC Data Traffic

- **Purpose:** Lightweight messaging (ICMP for connectivity, QUIC/UDP for fast encrypted web traffic)
- **Evidence:**
    - Payload data observed over **UDP**
    - When running pings or background app communications
    - Smaller size packets, low overhead

Modern browsers (Chrome, Edge) often use **QUIC (UDP-based)** instead of TCP for speed.

Technical Highlights Observed

Feature	What You Saw	Meaning
IPv6 traffic	Packets showing IPv6 addresses	Modern networking in action
DNS queries	Query names visible	Domain resolution process
TCP ACK flags	Reliable communications with servers	Successful encrypted traffic
Port numbers 53, 443	DNS, HTTPS	Common internet protocols
Payload Hex view	Data of ongoing session	Encrypted communication packet details

---

Conclusion

You successfully completed the network capture and analysis task.
You were able to:

✓ Capture real-time Wi-Fi traffic
✓ Identify and filter multiple protocols
✓ Inspect packet headers and payload
✓ Understand roles of DNS, TCP, and UDP/ICMP in everyday browsing