Task 3 – Networking Analysis Report

Tool Used - Wireshark

Objective

To understand basic networking concepts and observe live network traffic using Wireshark.

What I Did

- Opened Wireshark and selected the **wlo1 (Wi-Fi)** interface.
- Started live packet capture.
- Visited websites like **google.com** and **example.com**.
- Used filters like **dns**, **tcp**, and **http** to analyze traffic.
- Observed how data flows between my system and the internet.

Observations

1.IP Address

- IP address is like a **home address** for devices on a network.
- It helps computers identify where data should go.

2. MAC Address

- MAC address is a **unique identity** of a network device.
- It does not change like an IP address.

3. DNS

- DNS helps convert a **website name** into an **IP address**.
- In Wireshark, I saw DNS queries when I opened websites.

4. TCP Three-Way Handshake

- TCP uses a **three-step process** to start communication:
    - **SYN** – request to connect
    - **SYN-ACK** – response from server
    - **ACK** – confirmation

- This makes TCP reliable.

5. TCP vs UDP

- **TCP** is reliable and ensures data is delivered correctly.
- **UDP** is faster but does not check delivery.

6. HTTP vs HTTPS

- **HTTP** data can be seen in plain text.
- **HTTPS** data is encrypted and secure.
- HTTPS protects user information.

7. Packet Sniffing

- Packet sniffing means **capturing and analyzing network packets**.
- Wireshark is used for packet sniffing.

Conclusion

Wireshark helped me understand how network communication works.
I learned how data travels, how DNS works, and why encrypted traffic is important.
This task improved my basic knowledge of networking for cybersecurity.