

# PRACTICAL NO. 5

## A. Use Wireshark to Sniff the Network

---

### Aim

To capture and analyze network packets using **Wireshark** in order to understand network traffic.

---

### Tools / Software Used

- Wireshark
  - Windows / Kali Linux
  - Active Network Connection
- 

### Theory

Wireshark is a network packet analyzer used to capture, inspect, and analyze network traffic in real time. It helps in identifying protocols, suspicious traffic, and data flow across the network.

---

### Steps / Procedure

1. Start the system.
  2. Open **Wireshark** application.
  3. Select the active **network interface** (Wi-Fi / Ethernet).
  4. Click on **Start Capturing Packets**.
  5. Generate network traffic by opening any website.
  6. Observe captured packets such as TCP, UDP, HTTP, DNS.
  7. Apply filters (e.g., `http`, `tcp`, `dns`) to analyze traffic.
  8. Stop packet capture after analysis.
- 

### Result

Network packets were successfully captured and analyzed using Wireshark.

