27/12/24 Experiment - 17

a) Tool exploration - Wireshark.

Wireshark is a powerful and widely used network protocol analyzer. It allows you to capture and inspect data packets travelling over a network in real-time, making it a crucial tool for studying computer networks, troubleshooting network issues, and understanding protocols.

Key features:

1. packet capture : captures live network traffic from various interfaces (e.g. Ethernet, Wi-Fi).

2. Protocol Analysis: Supports hundreds of protocols (e.g, TCP, UDP, HTTP, FTP)

3. Filtering: offers powerful filters to isolate specific packets or traffic types.

4. Visualization: Displays packets details with hierarchial layers (ethernet, IP, TCP/UDP).

Use cases of Wireshark.

1. Network Troubleshotting:
   - Diagnosing slow network speeds.
   - Identifying bottlenecks or misconfigurations

2. Security Analysis:
   - Detecting malicious traffic or intrusions.

3. Protocol Study:

- understanding packets structures and communication flow.

Common Filters:

- http : show only HTTP traffic
- tcp.port == 80 : show traffic on TCP port 80
- ip.addr == 192.168.1.1: show packets to or from a specific IP address.
- udp : show only UDP traffic.