**EXPERIMENT NO 4**

**Name: Shaikh Zaid Muddaris Husain Roll no: 23DCO06 Batch: 3**

**AIM:Use Wireshark in Linux**

**1. Introduction:**

What is Wireshark? Wireshark is a tool used to capture and analyze network traffic. It helps you see what data is being sent over a network.

Why Use It? It’s useful for troubleshooting network issues, understanding network traffic, and learning about how networks operate.

**2. How Wireshark Works:**

Packet Capture: Wireshark captures packets of data that travel across a network. A packet is a small chunk of data sent from one computer to another.

Data Analysis: After capturing the packets, Wireshark allows you to inspect and analyze the data to see details like the source and destination of the packets, the data content, and protocols used.

**3. Key Features:**

Detailed View: Provides detailed information about each packet, including headers and payloads.

Filters: You can use filters to focus on specific types of traffic or particular network issues.

Protocol Support: Supports many different network protocols, so you can analyze a wide range of network communications.

**4. Common Uses:**

Troubleshooting: Helps identify and resolve network problems by showing where data is being lost or delayed.

Network Security: Useful for detecting suspicious activity or security breaches.

Learning Tool: Great for understanding how different network protocols work and how data travels across a network.

**5. Conclusion:**

Powerful Tool: Wireshark is a powerful and widely used tool for network analysis and troubleshooting.

Skill Development: Using Wireshark can enhance your understanding of network behavior and improve your ability to manage and secure networks.



