Project Report

Title: Basic Network Sniffer using Python

1. Introduction

This project is a **Basic Network Sniffer** developed using Python and the Scapy library. The main purpose of this project is to capture live network packets and analyze their important information such as source IP, destination IP, protocol type, and payload. This helps in understanding how data flows in a network.

2. Objectives

- To capture real-time network packets.
- To identify source and destination IP addresses.
- To detect different protocols such as TCP, UDP, and ICMP.
- To display packet payload and header information for analysis.

3. Tools and Technologies

- **Programming Language:** Python
- **Library Used:** Scapy
- **Platform:** Windows with VS Code
- **Environment:** Virtual Environment (venv)

4. Working of the Project

The program uses Scapy's sniff() function to capture packets from the network.
When a packet is received, the program checks if it contains an IP layer.
It then extracts information such as IP source, destination, TTL, flags, and packet length.
Based on the protocol (TCP, UDP, or ICMP), it displays port numbers and payload data.
All captured information is printed on the screen in real time.

5. Features

- Real-time packet capturing
- Displays IP and MAC addresses.
- Shows protocol type (TCP, UDP, ICMP)
- Shows payload data.

- Simple and easy to understand output.

6. Conclusion

This project successfully demonstrates how network packets can be captured and analyzed using Python. It is useful for learning network concepts and basic security monitoring. This project helped in understanding packet structure and protocol behavior in real-world networks.