Basic Network Sniffer - Project Documentation

# 1. Introduction

This project is a Basic Network Sniffer built using Python. The program captures live network traffic, analyzes packets, and displays key information such as source and destination IP addresses, protocol type (TCP/UDP), ports, and partial payloads.

# 2. Objective

The main objective of this project is to understand how data flows through the network, learn the structure of network packets, and explore basic networking protocols using Python.

# 3. Tools and Libraries

1. Python 3.x  
2. scapy (for packet sniffing and analysis)  
3. Command-line/terminal to run the program

# 4. Implementation

The program uses scapy's sniff() function to capture packets in real time. Each captured packet is analyzed to extract the IP header information, protocol type, source/destination ports, and raw payload data. Results are printed in a formatted manner for easy understanding.

# 5. Code Explanation

The Python code consists of:  
- Importing scapy modules (sniff, IP, TCP, UDP, Raw)  
- Defining a callback function that processes each packet  
- Checking for IP layer and printing Source/Destination IP  
- Identifying protocol (TCP/UDP) and printing ports  
- Displaying the first 50 characters of payload (if available)  
- Running sniff() continuously until stopped by the user (Ctrl+C)

# 6. Sample Output

==================================================  
Source IP : 104.208.16.95  
Destination IP : 10.172.221.183  
Protocol Num : 6  
Protocol : TCP  
Source Port : 443  
Destination Port: 17179  
Payload (first 50 chars): GET /index.html HTTP/1.1  
==================================================

# 7. Learning Outcomes

- Learned how to capture live network packets using Python.  
- Understood the structure of IP, TCP, and UDP packets.  
- Gained insights into how data flows through a network.  
- Built a foundation for advanced topics like network security and intrusion detection.

# 8. Conclusion

This project successfully demonstrates a simple network sniffer built in Python. It provides a hands-on approach to understanding networking fundamentals and analyzing real-time traffic. Such tools are useful for network debugging, learning, and security analysis.