Basic Network Sniffer - Project Documentation

This project is part of the SourceHub IT Academy Internship. The goal is to build a Basic Network Sniffer in Python to capture, analyze, and log network packets. The project helps understand how data moves across a network using raw sockets and packet decoding techniques.

Project Features

* Captures raw Ethernet packets using Python's socket module

* Extracts and prints source/destination IP addresses and protocol types

* Filters and displays only IPv4 packets

* Logs all captured data to 'packet_log.txt' with timestamps

* Easy to extend with deeper TCP/UDP parsing

How to Run

1. Use a Linux system or enable WSL (Windows Subsystem for Linux)

2. Open the terminal and navigate to the project folder

3. Run the script with administrator privileges:

```
sudo python3 Basic_Network_Sniffer.py
```

4. Observe the output in the terminal

5. Review packet_log.txt for a saved copy of the results

Sample Output

```
[19:44:02] IPv4 Packet: 192.168.1.4 -> 8.8.8.8, Protocol: 6
[19:44:03] IPv4 Packet: 192.168.1.4 -> 8.8.4.4, Protocol: 17
[19:44:04] IPv4 Packet: 192.168.1.4 -> 1.1.1.1, Protocol: 1
```

Technologies & Tools Used

* Python 3

* Socket module

* Struct module

* Linux/WSL (required for raw sockets)

* VS Code for development

Created By

Vishv Pruthi