**Project: Network Packet Sniffer with Alert System**

1. INTRODUCTION

This project, Network Packet Sniffer with Alert System, was developed as part of a cybersecurity internship. The tool captures live packets, logs traffic details, detects anomalies such as flooding or port scanning, and visualizes data for better understanding. It mimics the initial role of a SOC (Security Operations Center) analyst, who is responsible for real-time monitoring and detection of threats.

This project was developed as part of my cybersecurity internship to simulate a Security Operations Center (SOC) monitoring tool. Its purpose is to capture network packets in real-time, analyze their contents, and detect anomalies such as port scanning or flooding. It highlights essential SOC analyst skills, including traffic inspection, anomaly detection, and incident alerting.

1. ABSTRACT

The project implements a packet sniffer using Python and Scapy to capture packets in real time. Each packet’s metadata (timestamp, source IP, destination IP, protocol, and size) is stored in an SQLite database for structured logging. A simple anomaly detection algorithm checks whether an IP address exceeds a defined traffic threshold. If so, an alert is triggered to notify about potential malicious activity, such as port scans or denial-of-service attempts.  
Additionally, the tool generates traffic graphs using Matplotlib, allowing visualization of packet distribution across protocols (TCP, UDP, ICMP, etc.). This combines three essential SOC operations: monitoring, detection, and reporting.

1. OBJECTIVES

 To build a Python-based sniffer capable of capturing real-time network packets.

 To log traffic details for analysis and forensic purposes.

 To implement anomaly detection rules for detecting suspicious activities.

 To generate alerts when traffic thresholds are exceeded.

 To visualize captured data for better understanding of network behavior.

1. TOOLS USED

**Python** – Programming language for implementation.

**Scapy** – Packet sniffing and manipulation library.

**SQLite** – Database for structured log storage.

**Matplotlib** – Graph generation and visualization.

**SMTP** – For sending email alerts.

1. STEPS INVOLVED IN BUILDING THE PROJECT

 Installed Python and required dependencies (scapy, matplotlib).

 Configured Scapy to sniff packets from the network interface.

 Extracted details: source IP, destination IP, protocol, and size.

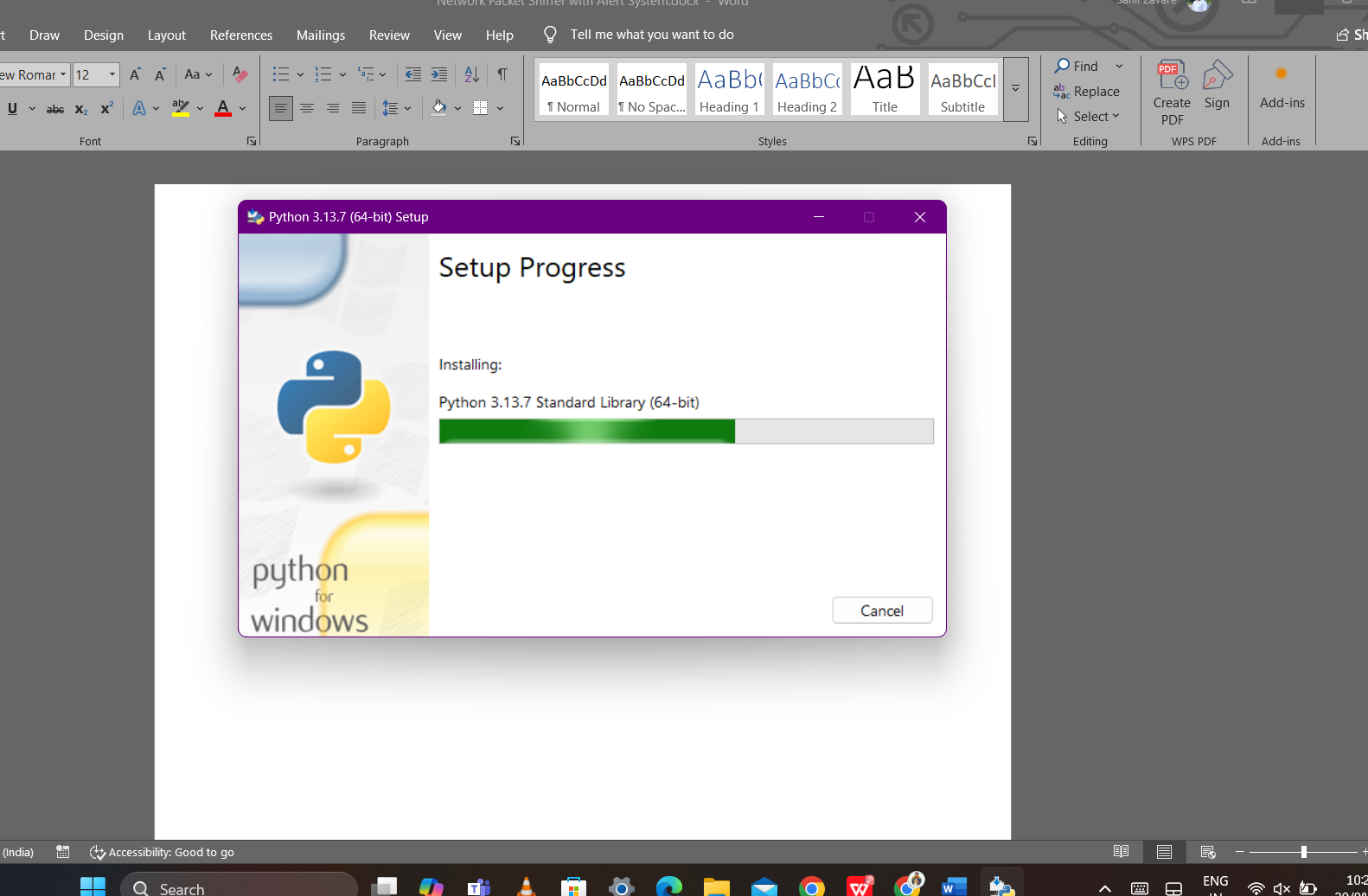
 Logged details into **SQLite database** (packets.db).

 Applied threshold rule: >50 packets from the same IP = suspicious.

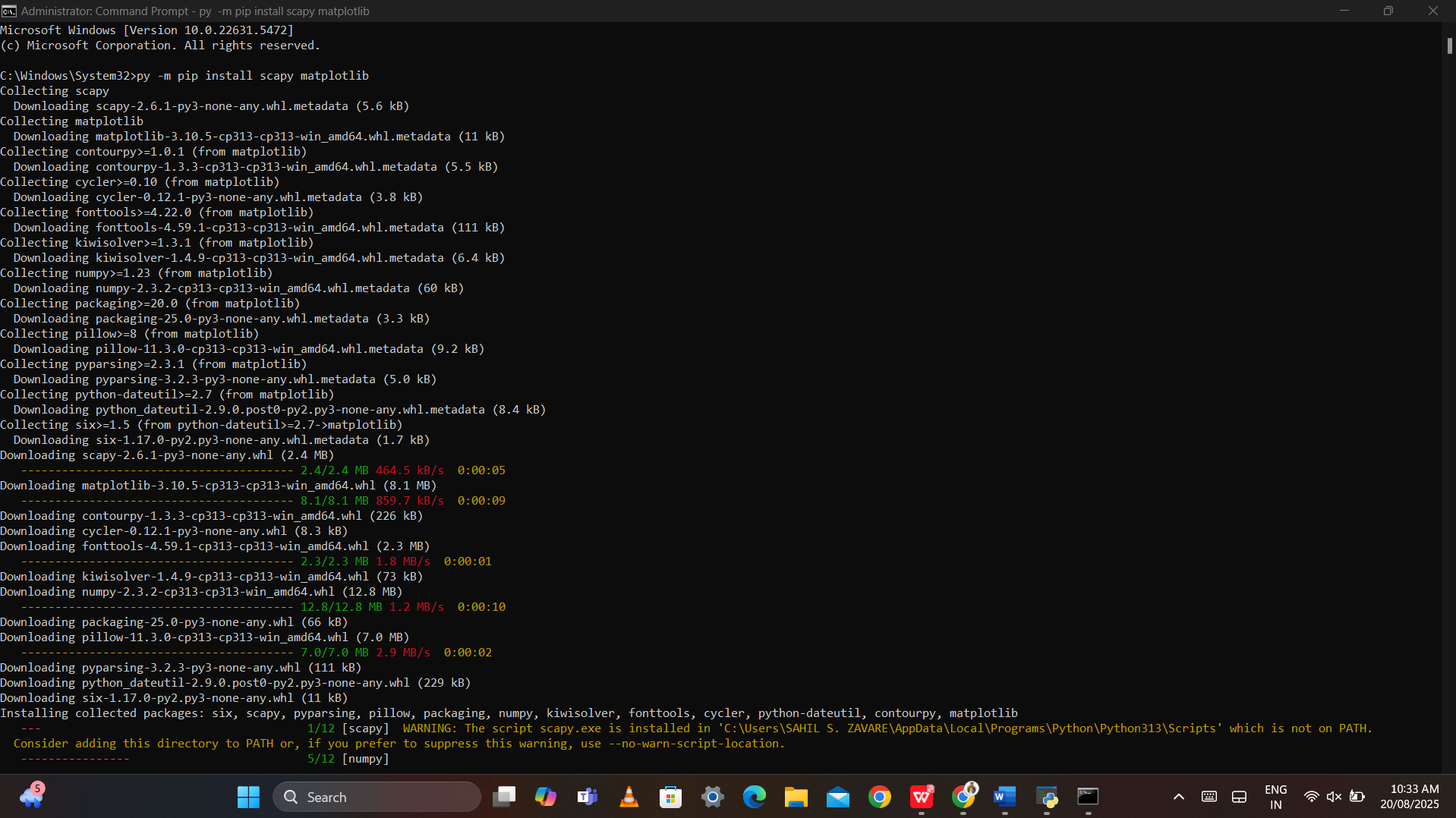
 Triggered alerts when rules were matched.

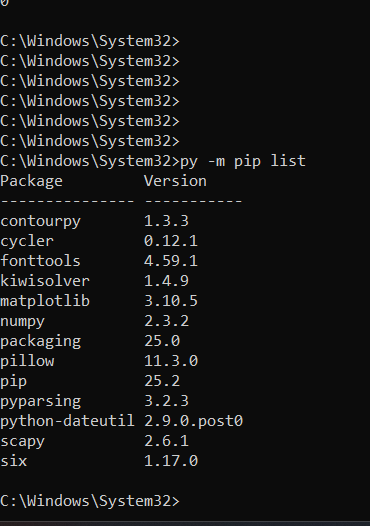
 Visualized results in bar charts (e.g., count of TCP, UDP, ICMP packets).

1. SCREENSHOTS ATTACHED
2. Python Installation

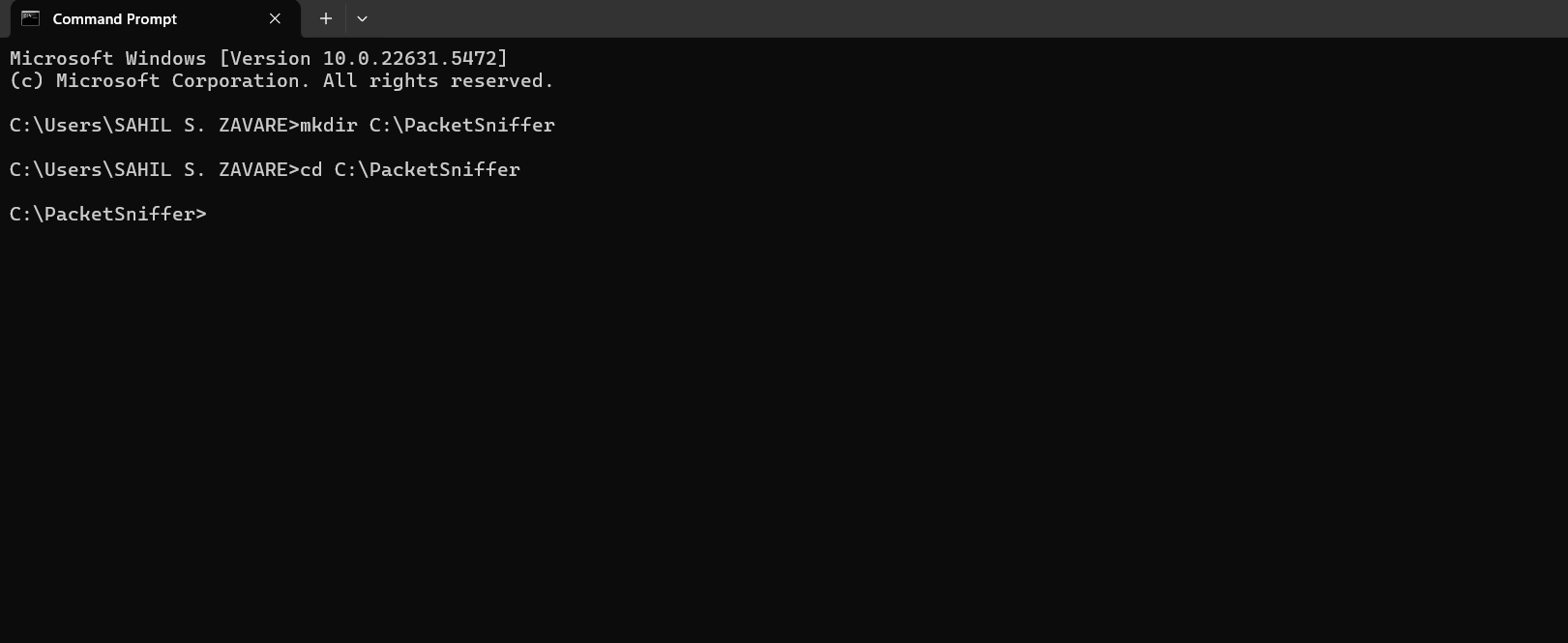


1. Configured Scapy to sniff packets from the network interface.

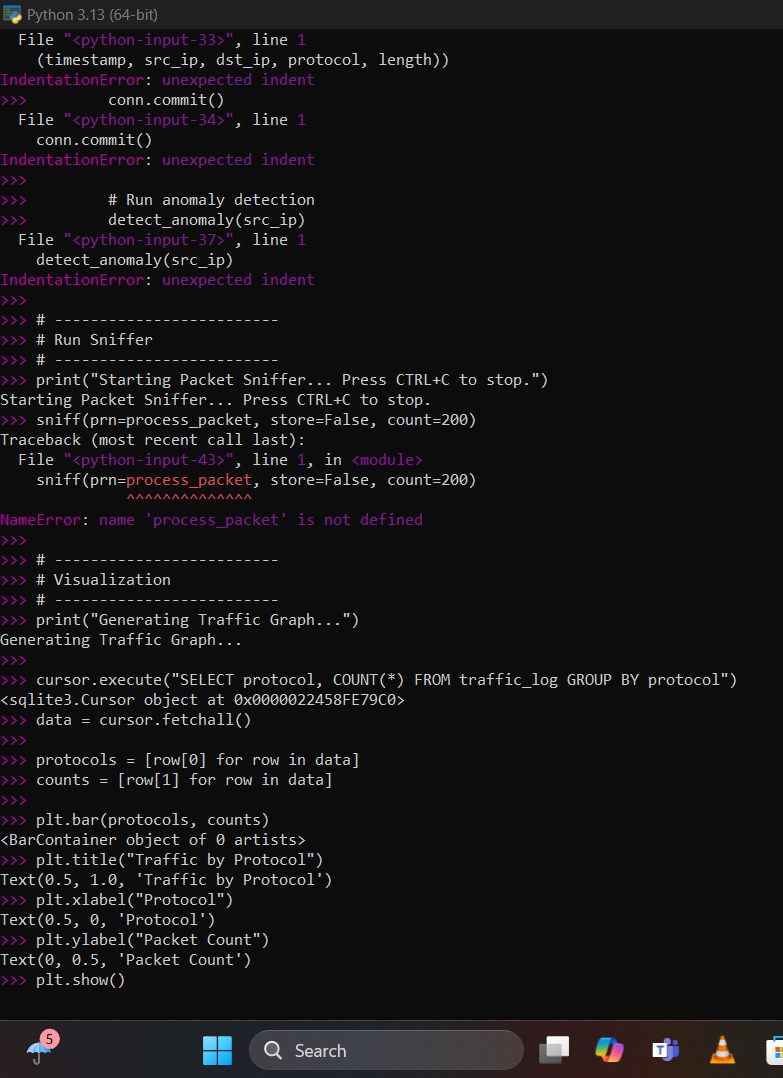




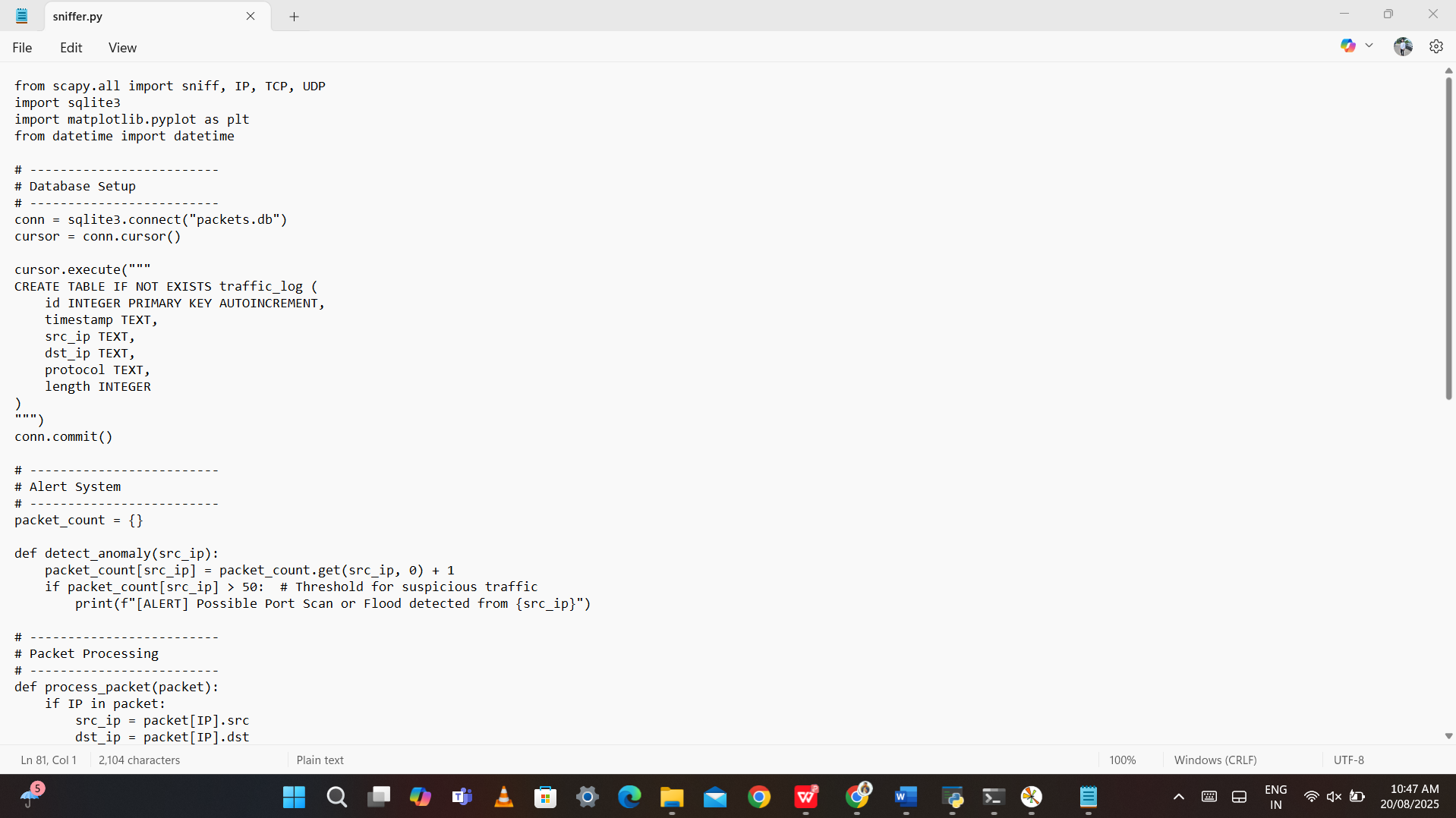
1. Created Project Folder

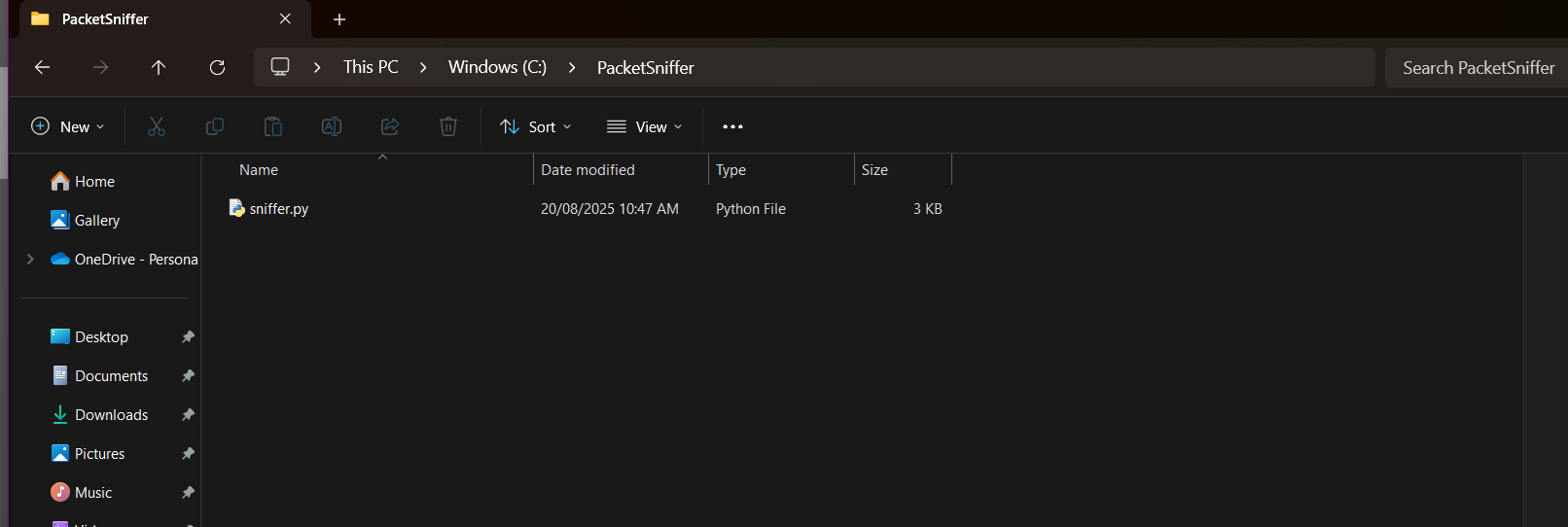


1. Writing code in python.

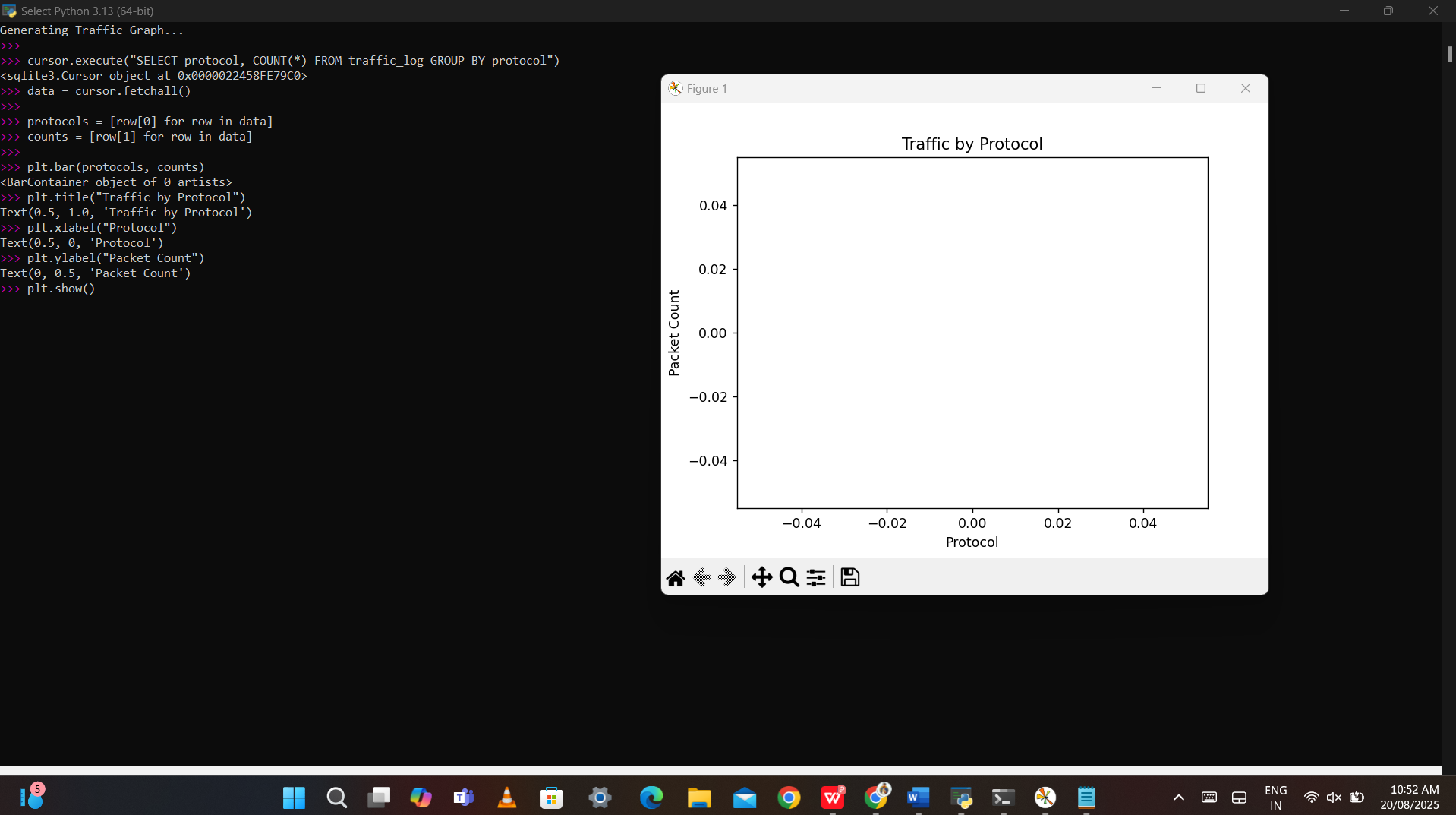


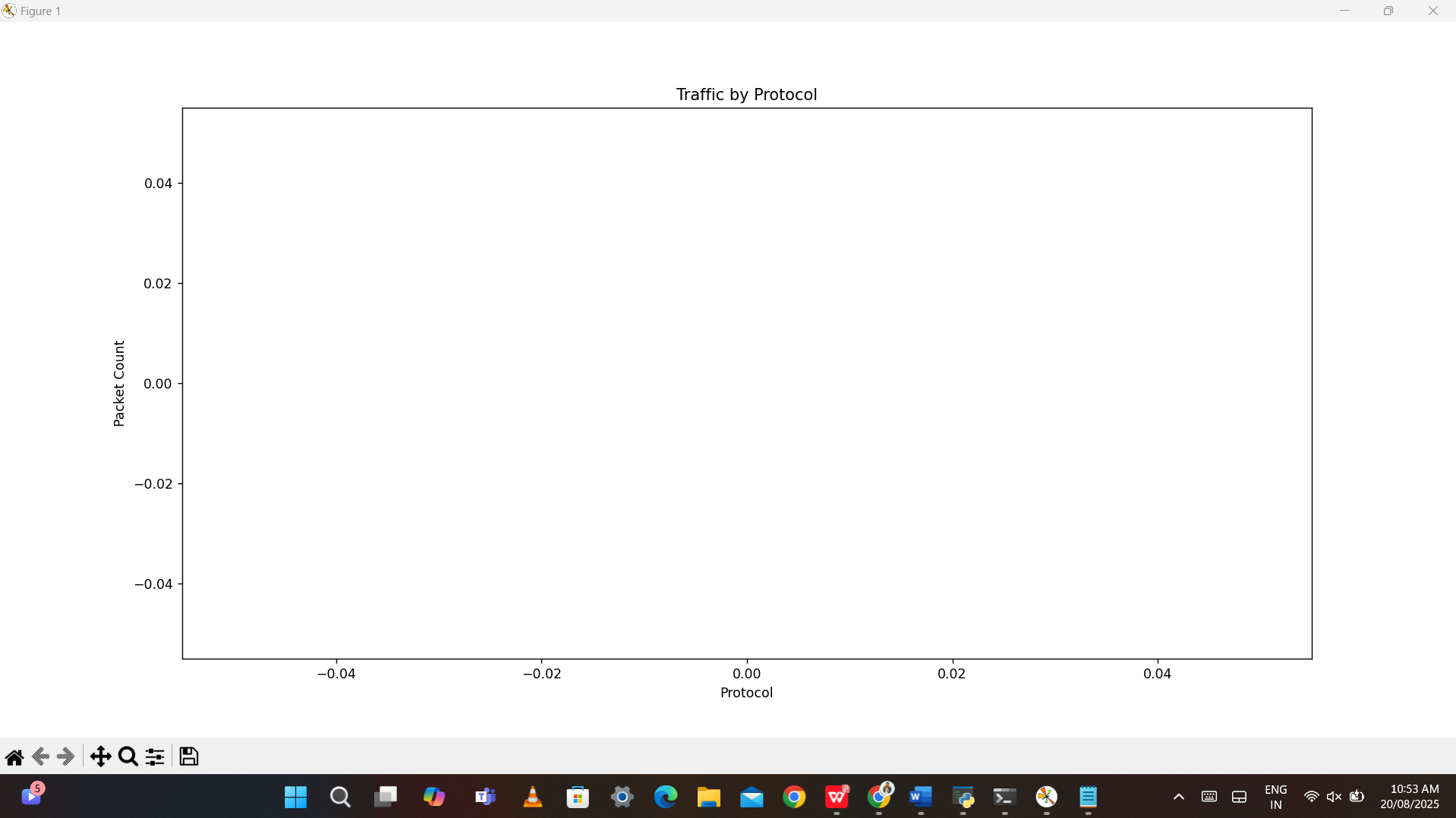
1. Pasted python project code to sniffer.py and save to the file name packet sniffer.



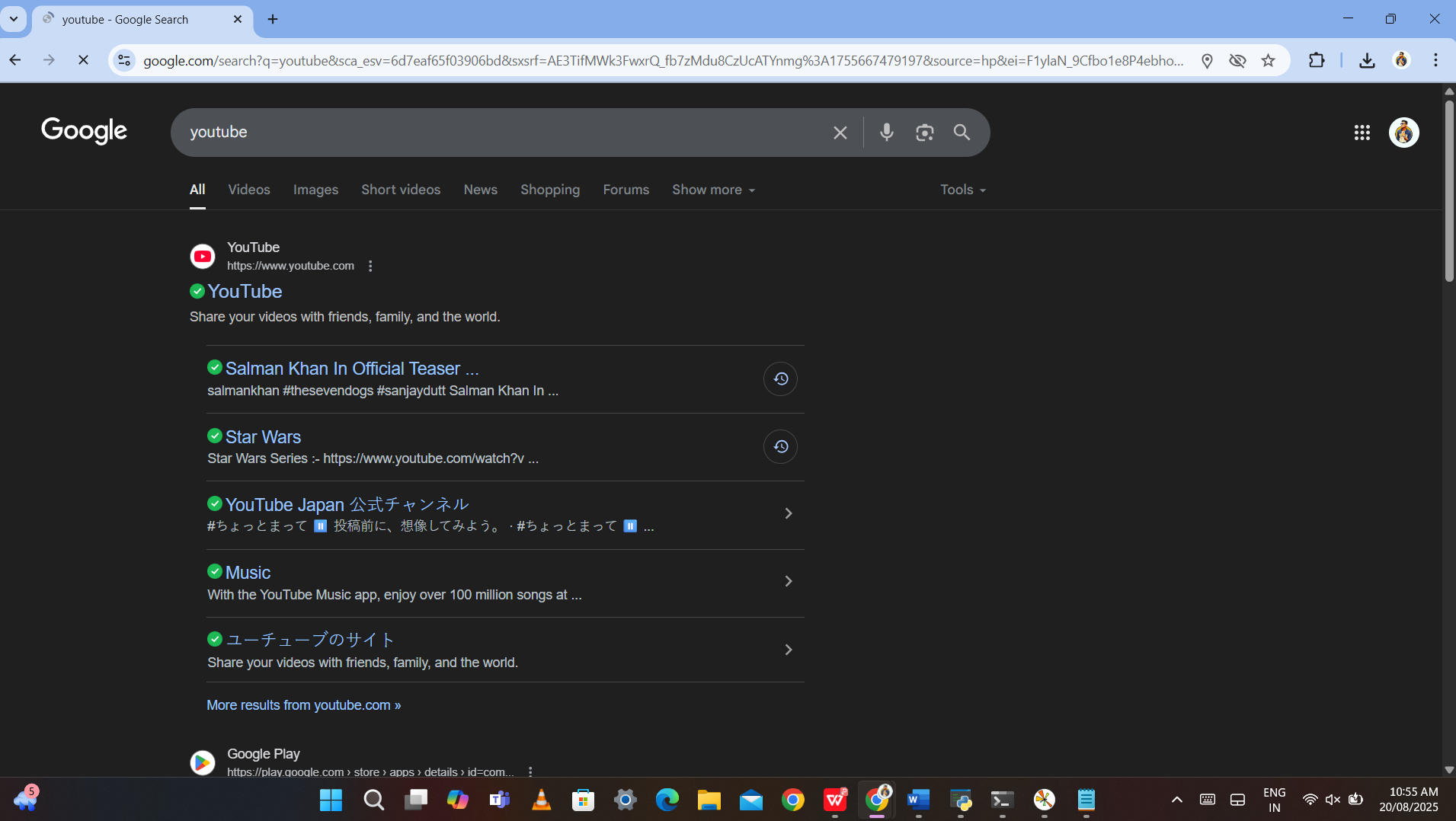


1. Running the Project on python.

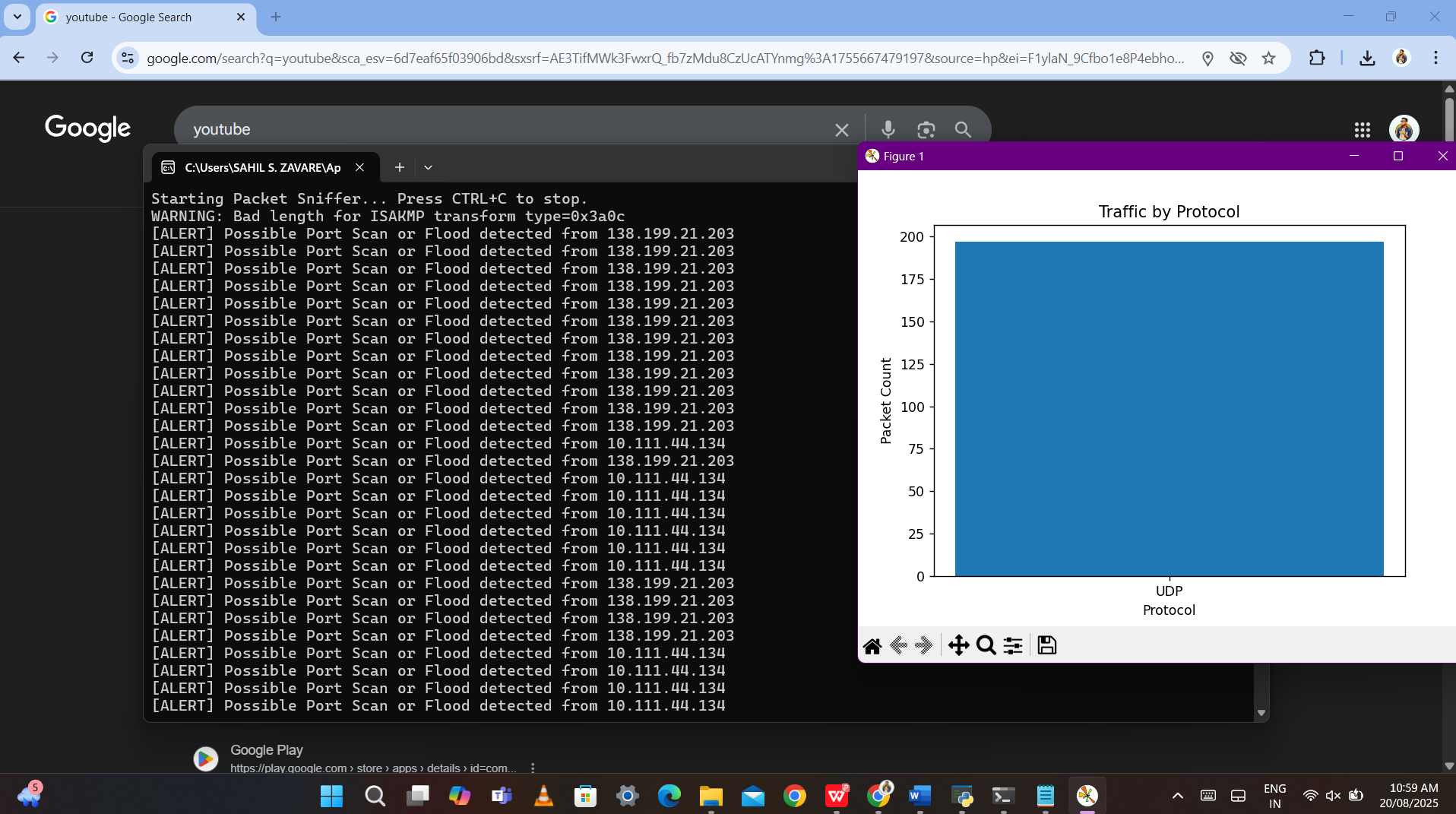




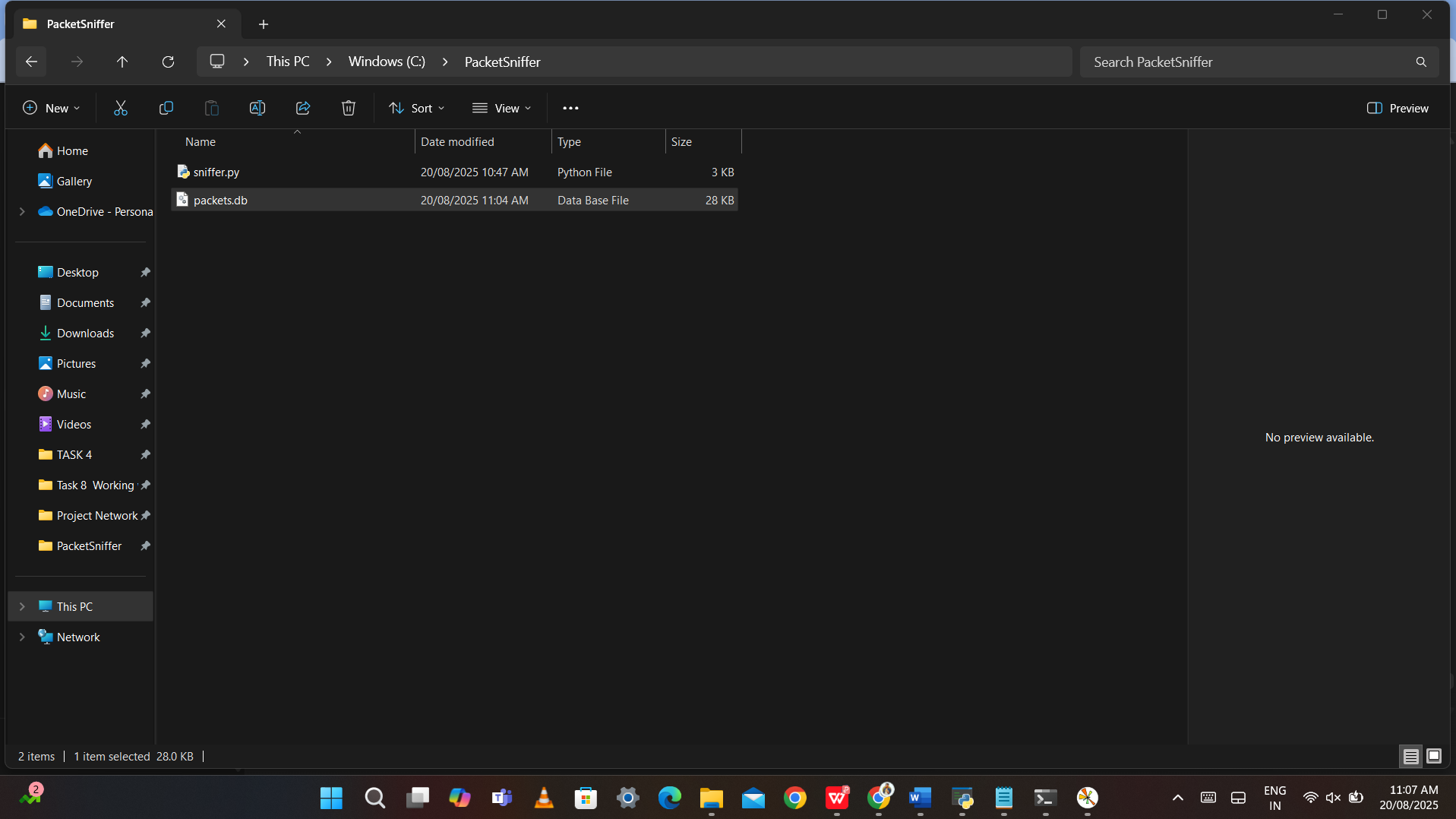
1. Generating network traffic.



1. Results after successfully running the code.

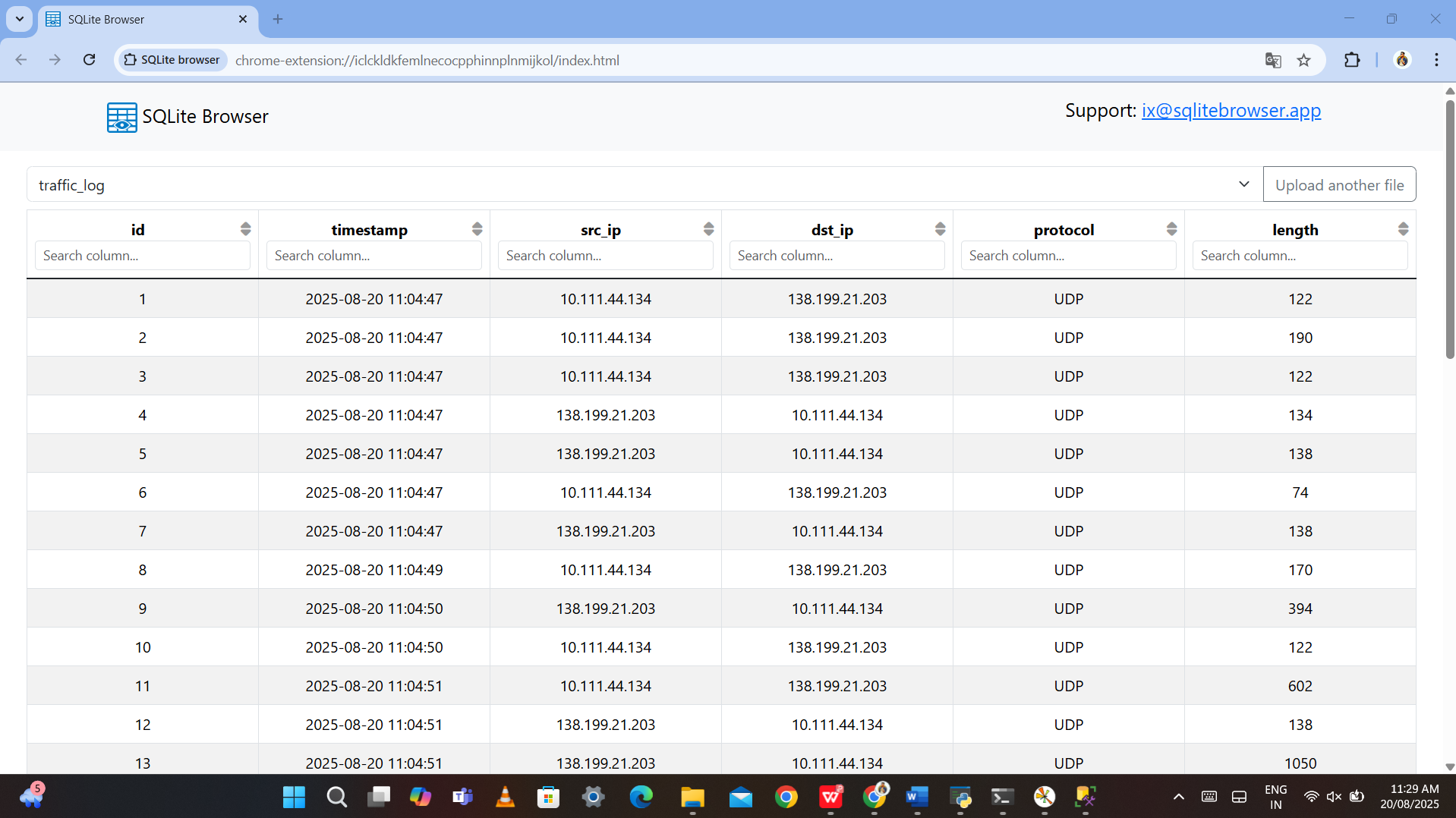


Also the packets.db file is saved in the packet sniffer file after running the code.



1. RESULTS

 **Logs**: Database entries show timestamps, IPs, protocol, and size.



 **Alerts**: [ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 10.111.44.134

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

[ALERT] Possible Port Scan or Flood detected from 138.199.21.203

 **Visualization**: Graph showing packet counts by protocol.

