# CodeAlpha Internship Project Report

## Submitted by

**Name**: Rahul Jebin Raju
**Institution**: University College of Engineering, Muttom
**Internship Course**: Cyber Security
**Internship Organization**: CodeAlpha
**Internship Duration**: 5 June 2025 – 5 September 2025

---

## TASK 1: Basic Network Sniffer

### 1.1: Project Abstract

**This internship project aims to develop a real-time network traffic monitoring system, Traffic-Nexus V1, that captures, analyzes, and visualizes live network packets with geolocation mapping of IP addresses. The project provides a centralized dashboard for packet analysis, alerts on abnormal activity, and integrates open-source tools to ensure flexibility and transparency. It is designed for educational, forensic, and small enterprise use.**

---

### 1.2: Project Objectives

- **Capture and log live network packets.**
- **Geolocate source and destination IPs using MaxMind.**
- **Visualize network traffic on a global map.**
- **Provide protocol-based and time-based filtering.**
- **Enable threshold-based anomaly detection and alerts.**
- **Store data for real-time and historical analysis.**

---

### 1.3: Project Methodology

**1. Packet Capture**

**Used PyShark, a Python wrapper for TShark, to capture:**

- **Source & Destination IP**
- **Protocol (TCP/UDP)**

- **Date, Time, Packet Count**

**2. IP Geolocation**

- **Integrated MaxMind GeoLite2 database**
- **Resolved IPs to: City, Country, Latitude, Longitude**

**3. Database Design**

- **Used MySQL for structured storage**
- **Logged traffic data for filtering, analysis, and persistence**

**4. Dashboard Development**

- **Built with Streamlit for a fast, responsive interface**
- **Integrated Folium for map visualization**
- **Real-time traffic and historical data views included**

---

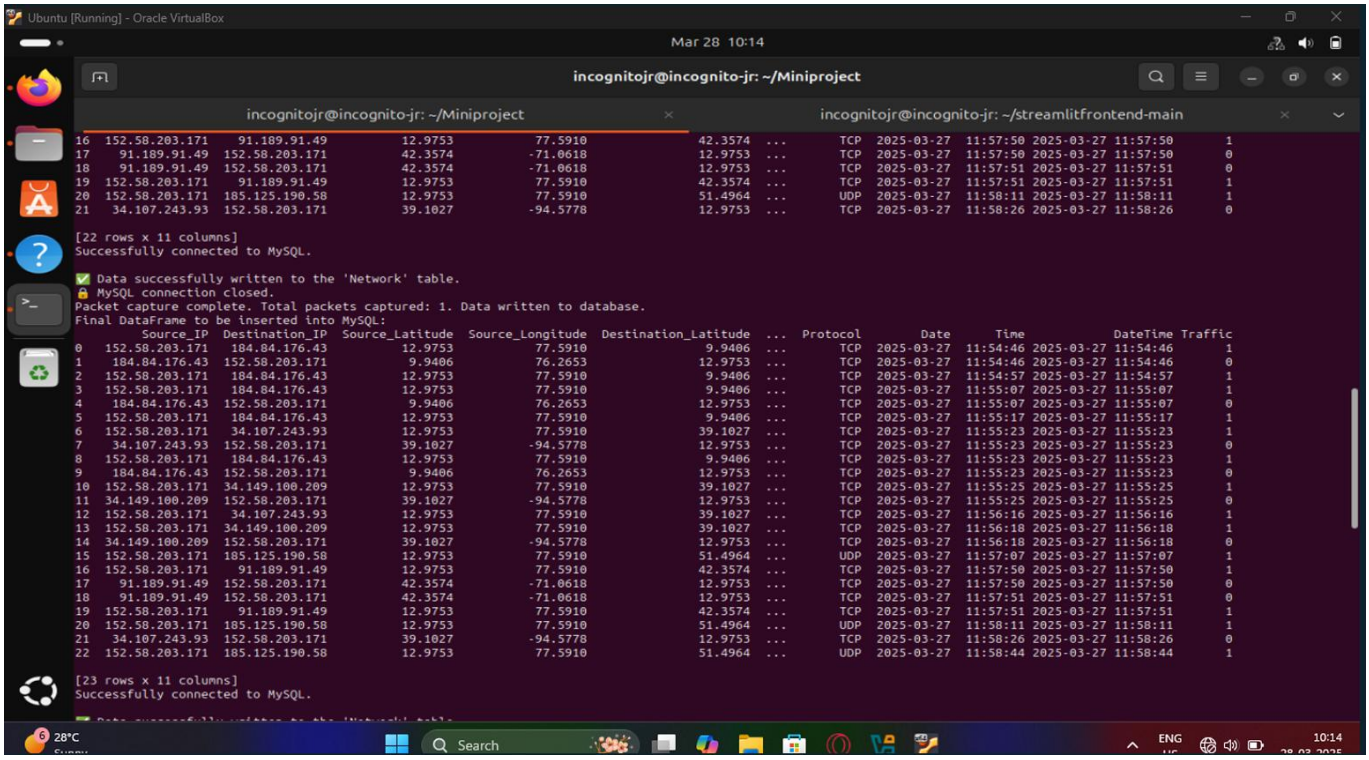
## 1.4: Technologies Used

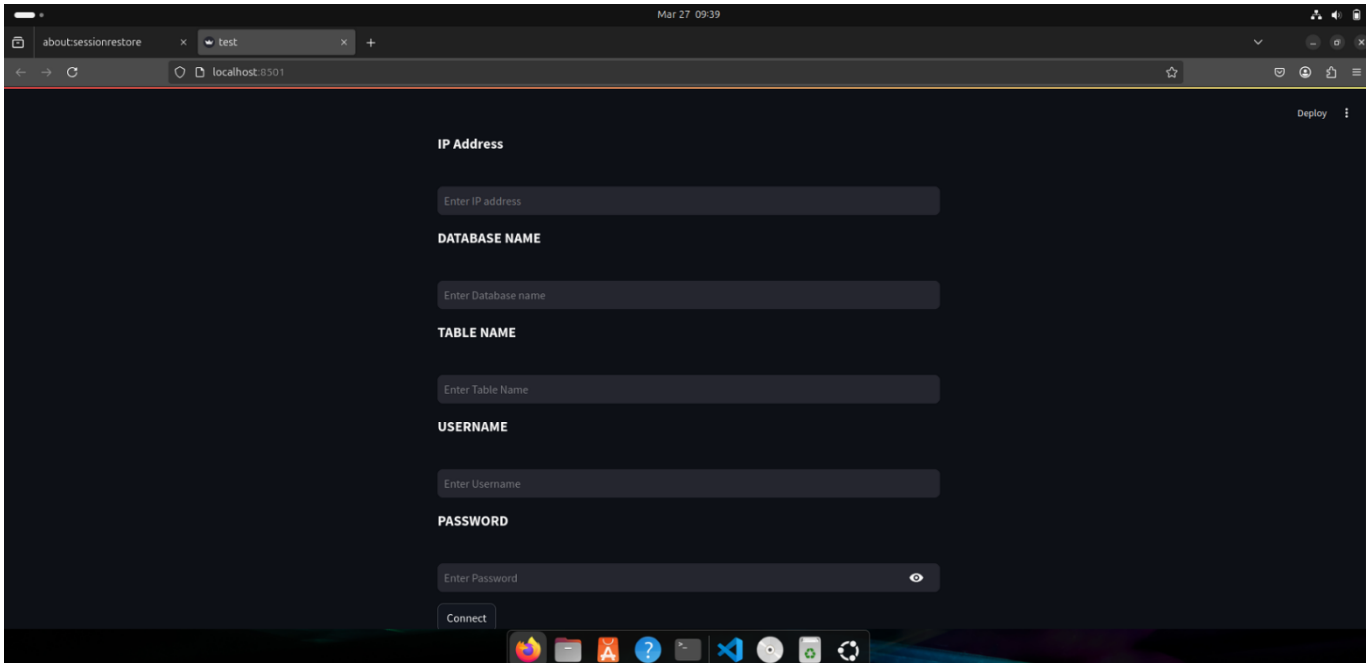
| Component | Tool/Technology |
|---|---|
| Packet Capture | PyShark (TShark) |
| IP Geolocation | MaxMind GeoLite2 |
| Data Visualization | Streamlit, Folium |
| Data Handling | Pandas, MySQL |
| Development Language | Python |

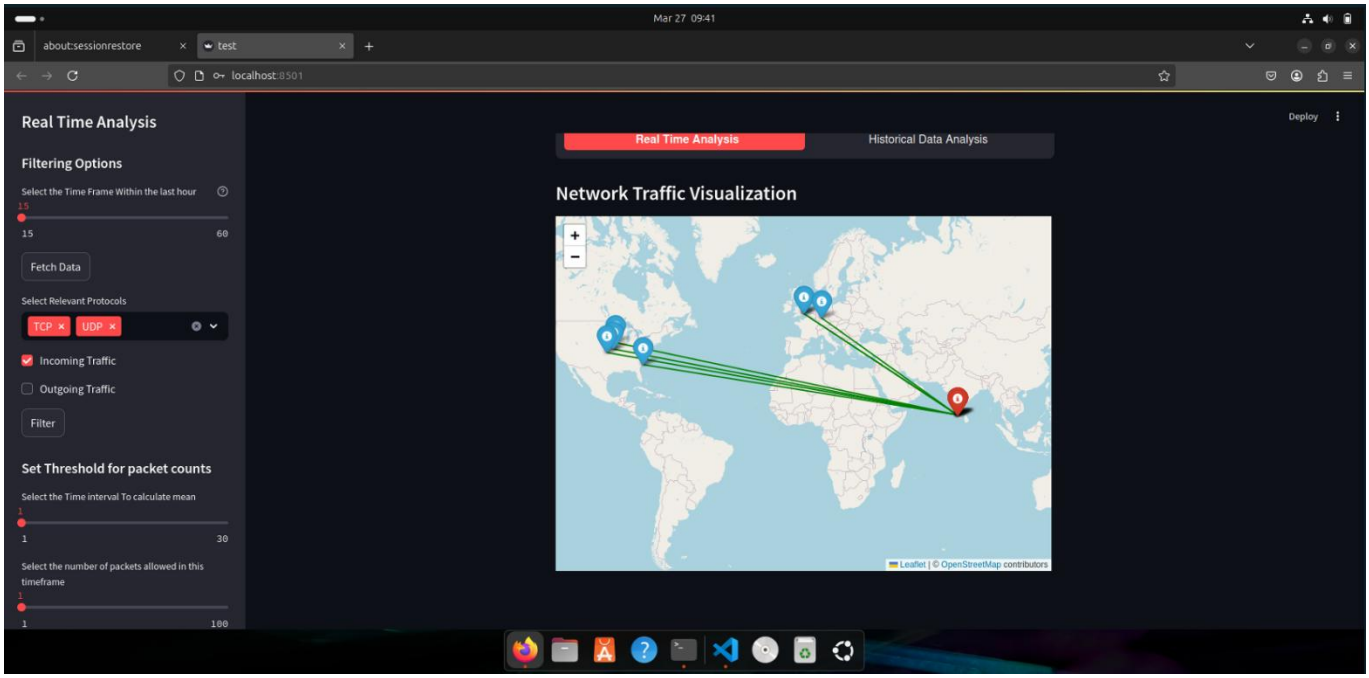
---

## 1.5: Implementation Screenshots

| Field | Type |
|---|---|
| id | int |
| Source_IP | varchar(45) |
| Destination_IP | varchar(45) |
| Source_Latitude | float |
| Source_Longitude | float |
| Destination_Latitude | float |
| Destination_Longitude | float |
| Protocol | varchar(10) |
| Date | date |
| Time | time |
| DateTime | datetime |
| Traffic | int |




Mar 27 09:39
about:sessionrestore
test
localhost:8501
Deploy
IP Address
Enter IP address
DATABASE NAME
Enter Database name
TABLE NAME
Enter Table Name
USERNAME
Enter Username
PASSWORD
Enter Password
Connect


Mar 27 09:41
about:sessionrestore
test
localhost:8501
Deploy
Real Time Analysis
Filtering Options
Select the Time Frame Within the last hour
15
15
60
Fetch Data
Select Relevant Protocols
TCP
UDP
Incoming Traffic
Outgoing Traffic
Filter
Set Threshold for packet counts
Select the Time interval To calculate mean
1
1
30
Select the number of packets allowed in this timeframe
1
1
100
Real Time Analysis
Historical Data Analysis
Network Traffic Visualization
Leaflet | © OpenStreetMap contributors


---

## 1.6: Results & Output

- **Successfully captured real-time traffic on a LAN.**
- **Mapped geolocation of both source and destination IPs.**
- **Displayed alerts based on user-defined packet thresholds.**
- **Enabled protocol- and date-based filtering for forensic analysis.**
- **Allowed data export and visual monitoring via Streamlit UI.**

---

## 1.7: Key Features

- ✅ **Live packet capture with logging**
- 🌍 **World map plotting of IP origins**
- 🔎 **Filters by protocol & time**
- 🚨 **Threshold-based traffic alerts**
- 📁 **Persistent database storage**
- 🖥️ **Clean and professional user interface**

---

## 1.8: Challenges Faced

- **Configuring TShark permissions for live capture.**
- **Handling IPs with unknown geolocation.**

- **Managing real-time data without affecting dashboard speed.**
- **Syncing database and UI in real-time.**

---

## 1.9: Learnings & Takeaways

- **Improved proficiency in network protocols and packet analysis.**
- **Gained hands-on experience with Python networking libraries.**
- **Learned to integrate multiple tools (PyShark, MaxMind, MySQL).**
- **Developed and deployed an end-to-end cybersecurity tool with real-world applications.**

---

## 1.10: Applications

- 🛡️ **Cybersecurity Education & Demonstration**
- 🕵️‍♂️ **Threat Intelligence Mapping**
- 🕵️‍♀️ **Digital Forensics**
- 🏢 **Lightweight Network Monitoring for SMBs**

---

## 1.11 Future Enhancements

- **Add AI-based anomaly detection.**
- **Dockerize the app for easy deployment.**
- **Support multi-node packet aggregation.**
- **Enable user authentication and report generation.**

---

## 1.12: Demo & Code

- 🔗 **YouTube Demo:** https://youtu.be/O2gbEhh7nX8?si=LKlInbitnBxNVFpN
- 💻 **GitHub Repositories:** https://github.com/IncognitoJR-007/CodeAlpha-CyberSecurity-Project
- 🧠 **Try it here:** https://traffic-nexus.streamlit.app/

## 1.13: Conclusion

**Traffic-Nexus V1 is a lightweight and effective solution for real-time network monitoring and visualization. It helps identify suspicious traffic patterns using intuitive visual tools and can be used in cybersecurity labs, educational settings, and small enterprises. This internship provided the opportunity to apply theoretical cybersecurity knowledge into a working prototype, laying a foundation for more advanced tools in future.**