NETWORK TRAFFIC ANALYSIS FOR CYBER THREAT DETECTION

By Aravind, Mahesh, Suman, Nimesh, Karthikeya

Guide: Dr. Pramoda Patro

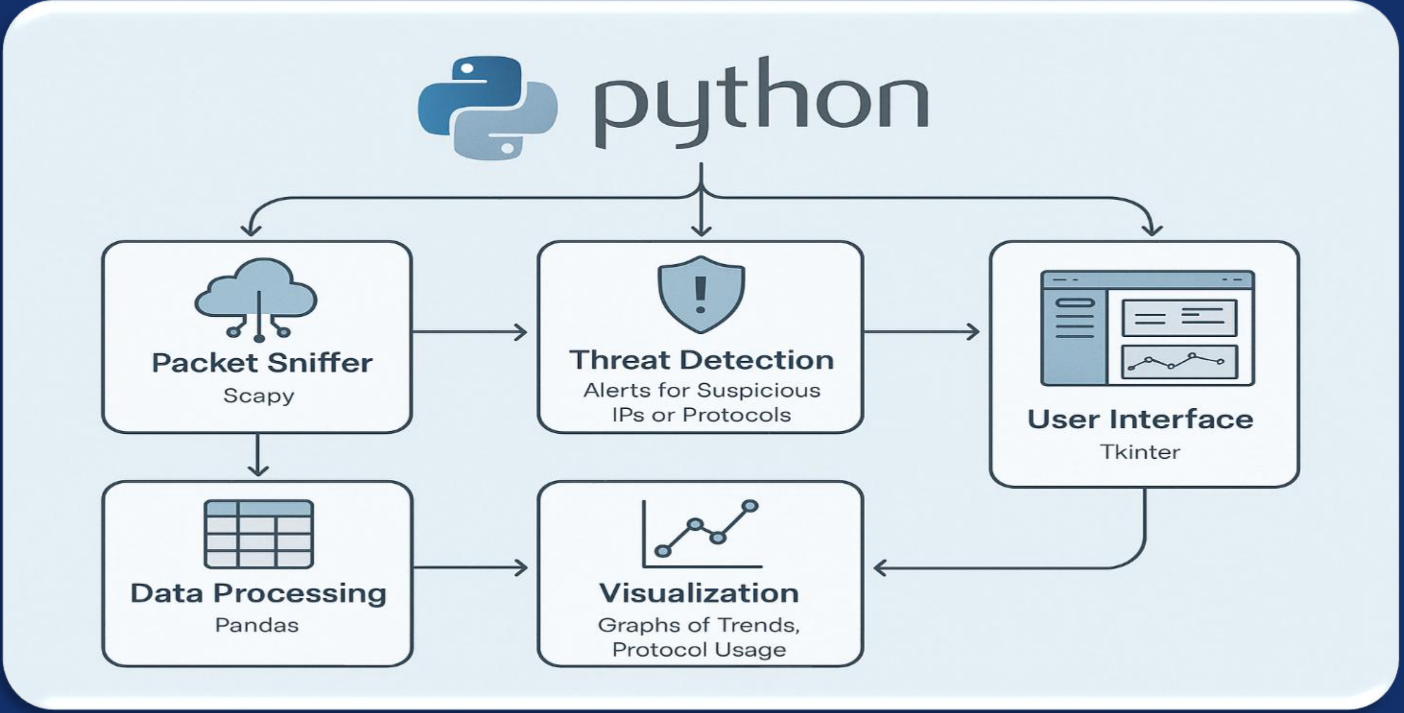
OBJECTIVES

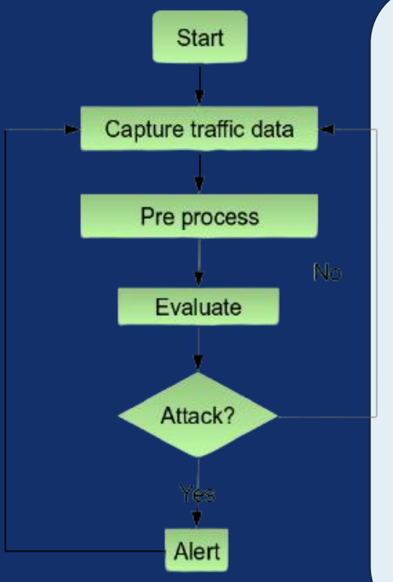
- To develop a real-time network traffic analyzer with an interactive GUI.
- To implement live packet sniffing and display relevant protocol and IP-level information.
- To analyze and categorize captured packets based on protocols such as TCP, UDP, and ICMP.
- To visualize network activity using charts and tables for better interpretation.
- To provide a foundation for future extensions such as automated threat detection or alerting mechanisms.
- This tool aims to assist users—both beginners and professionals—in understanding and managing their network environments more effectively.

INTRODUCTION

With the rapid growth of internet usage and connected devices, monitoring network traffic has become crucial for ensuring security, detecting intrusions, and optimizing performance. Network traffic analysis involves capturing and examining data packets that travel across a network to identify patterns, anomalies, and potential threats. This project, "Network Traffic Analyzer," is designed to provide a user-friendly and efficient tool for real-time packet sniffing and protocol analysis.

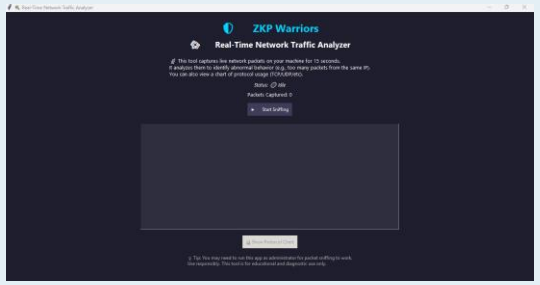
Built using Python, the application integrates libraries such as Scapy for packet capturing and analysis, Tkinter for graphical user interface (GUI) development, and Pandas for data handling and visualization. It enables users to monitor live network traffic, display protocol-wise statistics, analyze packet details, and detect unusual network behavior through visual insights.





RESULTS

The network traffic analyzer successfully captured and analyzed real-time packet data using Scapy, enabling deep packet inspection and protocol-level breakdowns. The graphical user interface, built with Tkinter, allowed intuitive visualization of traffic statistics, including IP addresses, ports, protocols, and packet size distributions. Integration with Pandas enabled efficient data logging and manipulation for detailed offline analysis. The tool effectively identified anomalies such as unusually high traffic or suspicious packets, contributing to potential threat detection. Overall, the system demonstrated reliability in monitoring network behavior, providing users with actionable insights for enhancing cybersecurity and optimizing network performance.



Real-Time Network Traffic Analyzer

ZKP Warriors

Real-Time Network Traffic Analyzer

This tool captures live network packets on your machine for 15 seconds.
It analyzes them to identify abnormal behavior (e.g., too many packets from the same IP).
You can also view a chart of protocol usage (TCP/UDP/etc).

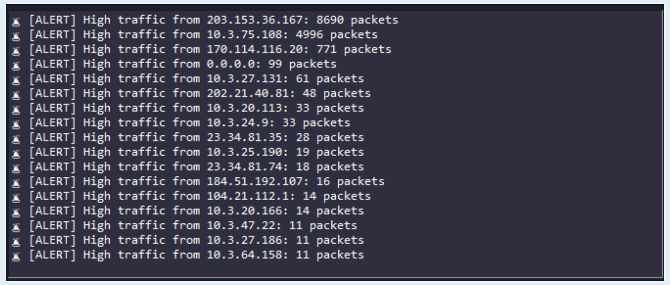
Status: Idle

Packets Captured: 0

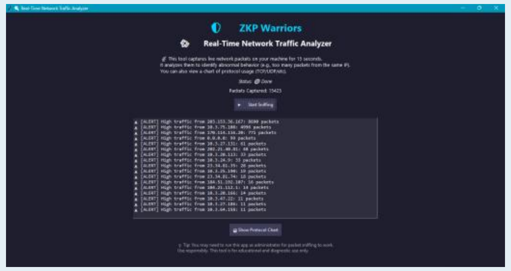
▶ Start Sniffing

Show Protocol Chart

Tip: You may need to run this app as administrator for packet sniffing to work.
Use responsibly. This tool is for educational and diagnostic use only.



```
[ALERT] High traffic from 203.153.36.167: 8690 packets
[ALERT] High traffic from 10.3.75.108: 4996 packets
[ALERT] High traffic from 170.114.116.20: 771 packets
[ALERT] High traffic from 0.0.0.0: 99 packets
[ALERT] High traffic from 10.3.27.131: 61 packets
[ALERT] High traffic from 202.21.40.81: 48 packets
[ALERT] High traffic from 10.3.20.113: 33 packets
[ALERT] High traffic from 10.3.24.9: 33 packets
[ALERT] High traffic from 23.34.81.35: 28 packets
[ALERT] High traffic from 10.3.25.190: 19 packets
[ALERT] High traffic from 23.34.81.74: 18 packets
[ALERT] High traffic from 184.51.192.107: 16 packets
[ALERT] High traffic from 104.21.112.1: 14 packets
[ALERT] High traffic from 10.3.20.166: 14 packets
[ALERT] High traffic from 10.3.47.22: 11 packets
[ALERT] High traffic from 10.3.27.186: 11 packets
[ALERT] High traffic from 10.3.64.158: 11 packets
```



Real-Time Network Traffic Analyzer

ZKP Warriors

Real-Time Network Traffic Analyzer

This tool captures live network packets on your machine for 15 seconds.
It analyzes them to identify abnormal behavior (e.g., too many packets from the same IP).
You can also view a chart of protocol usage (TCP/UDP/etc).

Status: Done

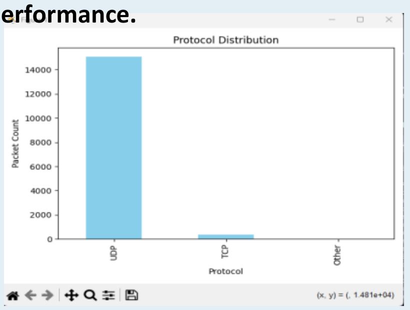
Packets Captured: 15425

▶ Start Sniffing

```
[ALERT] High traffic from 203.153.36.167: 8690 packets
[ALERT] High traffic from 10.3.75.108: 4996 packets
[ALERT] High traffic from 170.114.116.20: 771 packets
[ALERT] High traffic from 0.0.0.0: 99 packets
[ALERT] High traffic from 10.3.27.131: 61 packets
[ALERT] High traffic from 202.21.40.81: 48 packets
[ALERT] High traffic from 10.3.20.113: 33 packets
[ALERT] High traffic from 10.3.24.9: 33 packets
[ALERT] High traffic from 23.34.81.35: 28 packets
[ALERT] High traffic from 10.3.25.190: 19 packets
[ALERT] High traffic from 23.34.81.74: 18 packets
[ALERT] High traffic from 184.51.192.107: 16 packets
[ALERT] High traffic from 104.21.112.1: 14 packets
[ALERT] High traffic from 10.3.20.166: 14 packets
[ALERT] High traffic from 10.3.47.22: 11 packets
[ALERT] High traffic from 10.3.27.186: 11 packets
[ALERT] High traffic from 10.3.64.158: 11 packets
```

Show Protocol Chart

Tip: You may need to run this app as administrator for packet sniffing to work.
Use responsibly. This tool is for educational and diagnostic use only.



CONCLUSION

The Network Traffic Analyzer project demonstrates the effective use of Python, Scapy, Tkinter, and Pandas to create a practical tool for real-time network traffic monitoring and analysis. This system enables users to capture and inspect live packets, analyze protocol usage, and visualize traffic patterns, helping in identifying abnormal or suspicious network behavior.

Key findings

From the traffic analysis highlighted that TCP remains the most commonly used protocol in typical network environments, followed by UDP and ICMP. Visual representations such as protocol distribution charts and IP-based summaries proved valuable in understanding traffic flow and detecting anomalies, such as repeated access attempts or scanning behavior..

Overall, this project successfully integrates theoretical knowledge with hands-on implementation. With further development—such as integrating automated threat detection or cloud-based logging—it can evolve into a more robust tool for academic, personal, or small-scale enterprise use.

REFERENCES

Alsaqer, M. A., & Alghamdi, S. A. (2020). Real-time network traffic analysis using machine learning techniques: A survey. *Computers, Materials & Continua*, *66*(3), 2283–2301.

Garg, S., & Nia, M. M. (2018). Scapy-based packet sniffing and analysis for cybersecurity. *International Journal of Computer Science and Information Security (IJCSIS)*, *16*(5), 138–144.