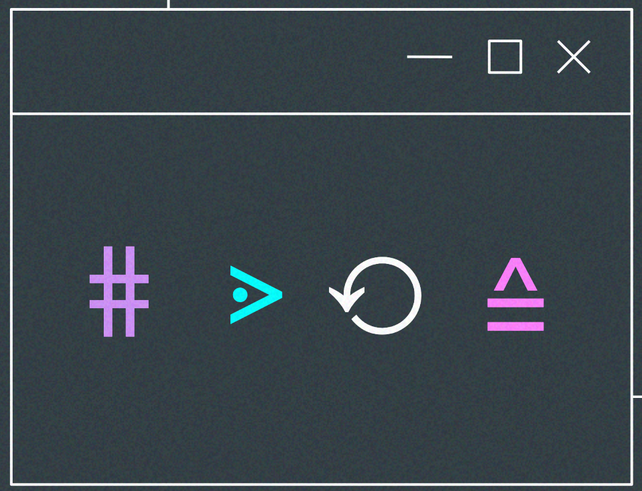
Network Traffic and Monitoring



Introduction to Network Traffic and monitoring

Network traffic monitoring is the process of analyzing, capturing, and reviewing network traffic for performance, security, and troubleshooting purposes. It involves tracking the data flowing across a network, such as the type of data, the source and destination addresses, and the volume of data being transmitted.

Understanding Network Traffic

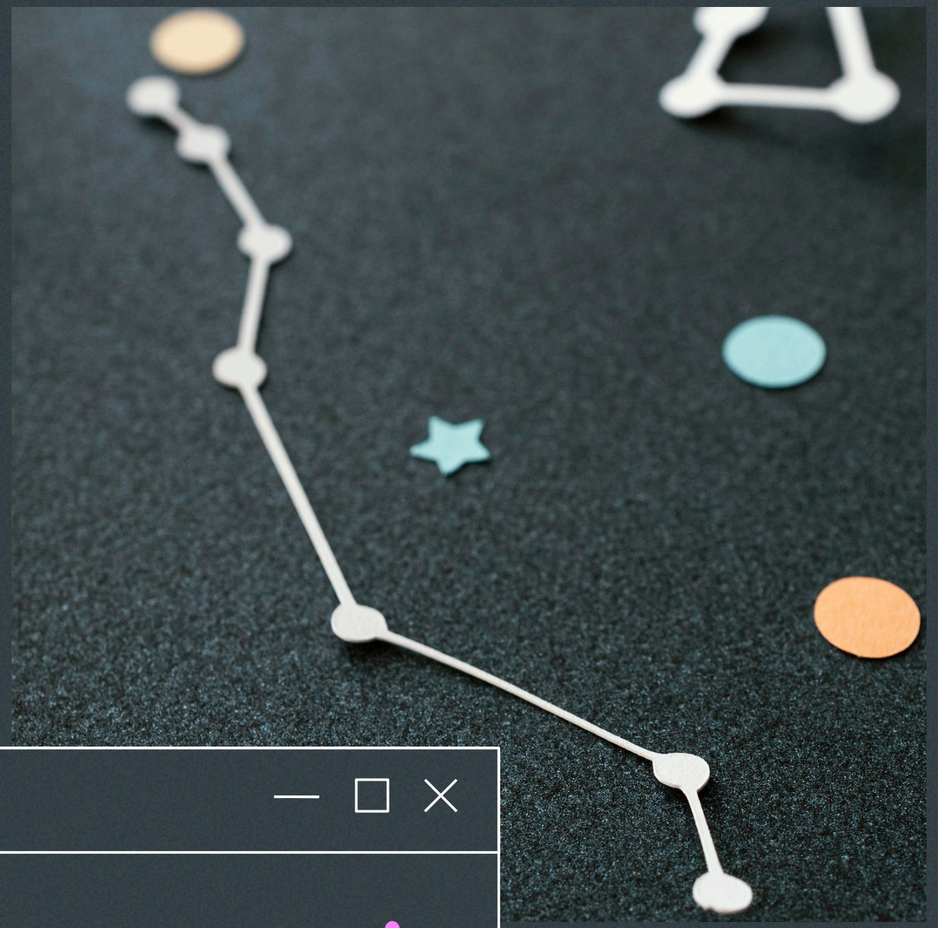
To effectively monitor network performance, it's essential to understand **network traffic** types. Different types of traffic, such as **streaming**, **browsing**, and **file transfers**, can impact performance differently, necessitating tailored monitoring strategies.

Importance of Traffic Monitoring

Effective **traffic monitoring** is vital for identifying **bottlenecks** and ensuring optimal resource allocation. By continuously analyzing traffic patterns, organizations can make informed decisions to enhance performance and user satisfaction.

Key Monitoring Tools

Utilizing the right **monitoring tools** is essential for effective traffic analysis. Tools like **Wireshark**, **Nagios**, and **PRTG** provide insights into network performance, enabling IT teams to quickly identify and resolve issues.



What does this tool does?

This real-time network traffic monitoring tool captures and displays detailed packet information, logs data to a CSV file, and provides filtering options based on protocol, IP addresses, and ports. It features a user-friendly GUI for managing packet sniffing and viewing results, along with real-time traffic visualization using Matplotlib. This tool is valuable for network performance monitoring, security analysis, troubleshooting, education, and compliance, offering comprehensive insights into network behavior and facilitating quick response to issues.

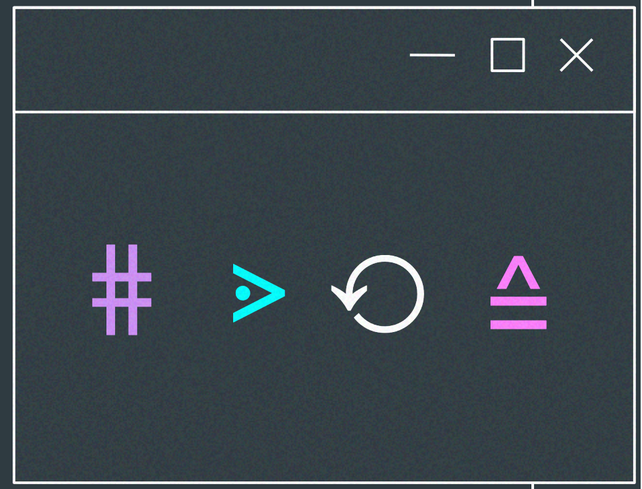
Functionalities

Network Monitoring: Helps network administrators detect suspicious activities, such as unusual traffic patterns or unauthorized access attempts, in real-time.

Network Performance Analysis: Allows monitoring of network traffic to identify bottlenecks, latency issues, and bandwidth utilization, aiding in network optimization.

Troubleshooting: Facilitates troubleshooting
by providing detailed information about network packets, making it easier to identify and resolve network issues.

Compliance and Auditing: Logs network traffic data which can be used for compliance with regulations and auditing purposes.



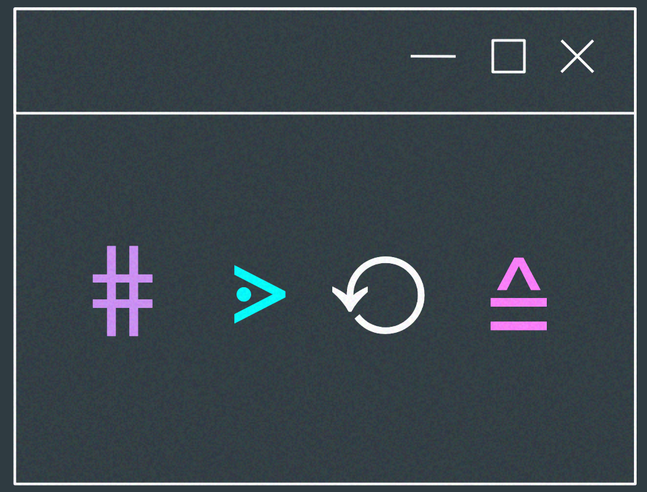
Features / Technical Implementation

- GUI Layout
- Packet capturing
- Logging
- Filtering
- Graphical representation

Flow Diagram

Packet Capturing -> Filtering -> Displaying -> Logging -> Visualizing

Components used



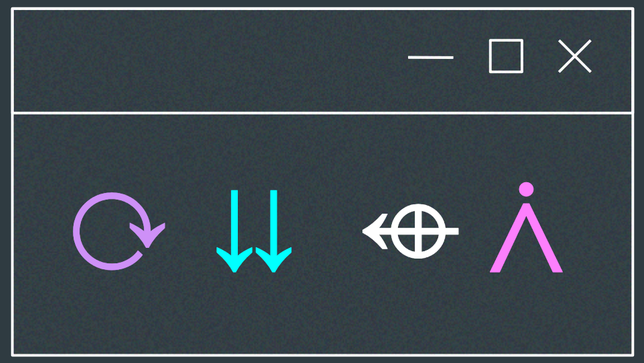
1. Tkinter
   Purpose: Used for creating the graphical user interface (GUI).

2. Scapy
   Purpose: Used for packet sniffing and analysis.

3. CSV
   Purpose: Used for logging packet details to a CSV file.

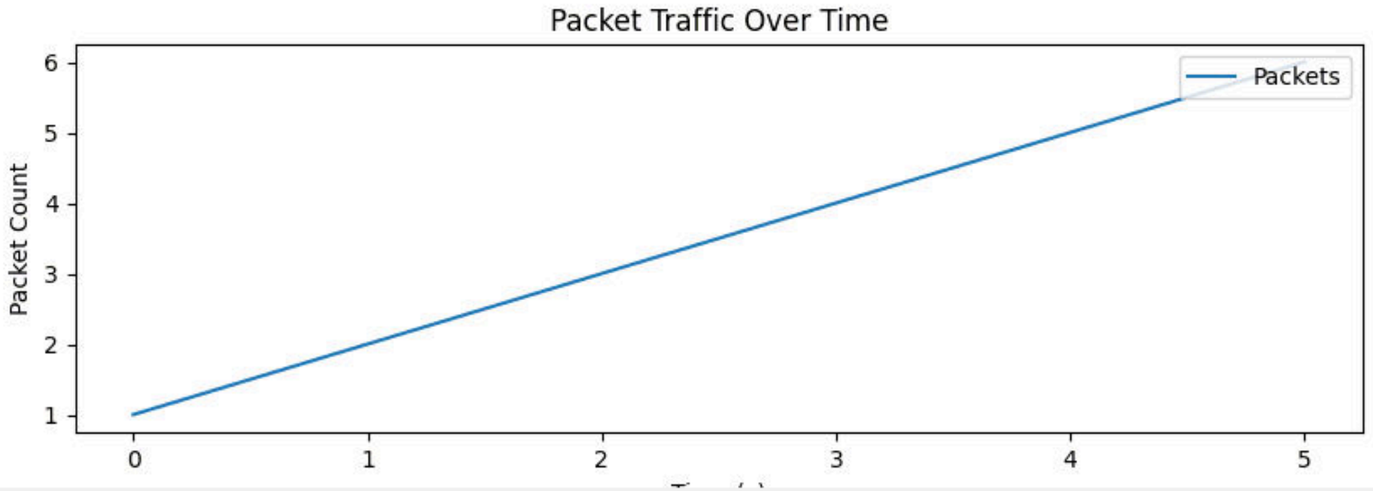
4. Datetime
   Purpose: Used for timestamping captured packets.

5. Matplotlib
   Purpose: Used for visualizing packet traffic data.



Real-time Network Traffic Monitor

```
Payload: Raw

[2024-07-28 18:58:41] TCP Packet: 172.16.211.96 ->
162.255.45.55 (Sport: 65042, Dport: 443, Flags: PA, TTL:
128)
Payload: Raw

[2024-07-28 18:58:41] TCP Packet: 162.255.45.55 ->
172.16.211.96 (Sport: 443, Dport: 65042, Flags: A, TTL: 59)
Payload: Padding

[2024-07-28 18:58:41] TCP Packet: 162.255.45.55 ->
172.16.211.96 (Sport: 443, Dport: 65042, Flags: A, TTL: 59)
Payload:

[2024-07-28 18:58:42] TCP Packet: 172.16.211.96 ->
162.255.45.55 (Sport: 65042, Dport: 443, Flags: PA, TTL:
128)
Payload: Raw

[2024-07-28 18:58:43] TCP Packet: 162.255.45.55 ->
172.16.211.96 (Sport: 443, Dport: 65042, Flags: A, TTL: 59)
Payload: Padding
```



Start Stop Restart

Protocol: All

Source IP:

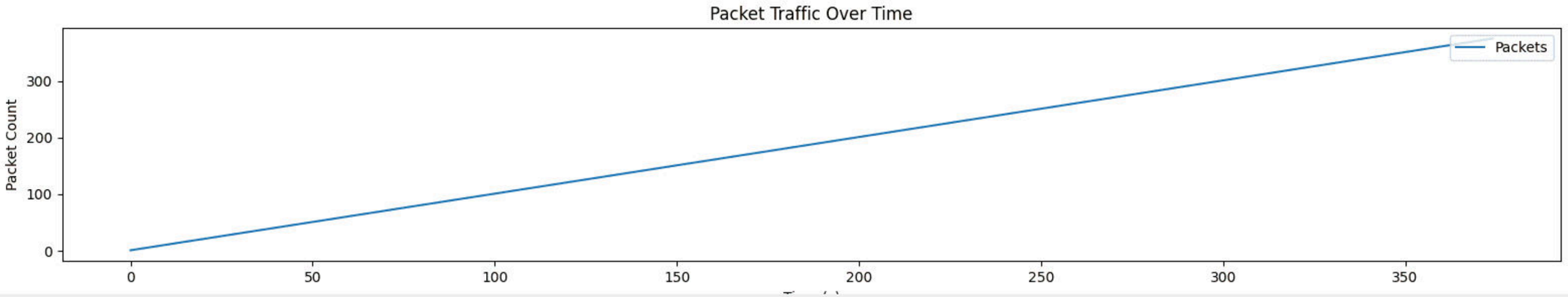
Destination IP:

Port:

Filter

```
172.16.211.96 (Sport: 443, Dport: 55212, Flags: PA, TTL: 64)
Payload: Raw

[2024-07-28 21:20:48] TCP Packet: 172.16.211.96 ->
20.192.44.78 (Sport: 55212, Dport: 443, Flags: A, TTL: 128)
Payload:

[2024-07-28 21:20:48] TCP Packet: 162.255.45.148 ->
172.16.211.96 (Sport: 443, Dport: 55258, Flags: PA, TTL: 56)
Payload: Raw

[2024-07-28 21:20:48] TCP Packet: 172.16.211.96 ->
162.255.45.148 (Sport: 55258, Dport: 443, Flags: A, TTL:
128)
Payload:

[2024-07-28 21:20:52] TCP Packet: 172.16.211.96 ->
20.192.44.78 (Sport: 55212, Dport: 443, Flags: PA, TTL: 128)
Payload: Raw

[2024-07-28 21:20:52] TCP Packet: 20.192.44.78 ->
172.16.211.96 (Sport: 443, Dport: 55212, Flags: A, TTL: 64)
Payload: Padding
```

```
[2024-07-28 21:19:25] TCP Packet: 162.255.45.148 ->
172.16.211.96 (Sport: 443, Dport: 55270, Flags: PA,
Payload: Raw
```



Start Stop Restart

Protocol: All

Source IP: 162.255.45.148

Destination IP: 172.16.211.96

Port:

Filter

Learning

- Network Protocols: Understanding TCP/IP stack and packet structure.
- Packet Sniffing: Using Scapy for real-time packet capture and analysis.
- GUI Development: Building a user-friendly interface with Tkinter.
- Data Visualization: Creating real-time graphs using Matplotlib.
- Data Logging: Writing packet details to CSV files.
- Multithreading: Handling concurrent processes for sniffing and GUI updates.
- Data Filtering: Implementing effective packet filtering mechanisms.
- Error Handling: Developing robust error handling and debugging strategies.

challenges

- Real-time Performance: Ensuring efficient handling of high traffic with minimal latency.
- GUI Responsiveness: Maintaining a responsive interface during real-time updates.
- Concurrency Issues: Coordinating sniffing and GUI threads to avoid race conditions.
- Data Accuracy: Preventing packet loss and ensuring data integrity.
- Complex Filtering: Implementing comprehensive filters without impacting performance.
- Visualization Scalability: Keeping visualizations clear with large datasets.
- Error Management: Handling unexpected packet formats and file I/O errors.
- User Experience: Designing an intuitive and user-friendly interface.
- Security: Ensuring sensitive data is protected and access is controlled.

Thank you

By,
Akilan S S[2261003]
B Sai Sandyaa[2261010]
M Kaushik[2261030]