



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Network Traffic Analysis Tool

Ankit Sharma

Department of Computer Science &
Application

Sharda School of Computing Science &
Engineering

Sharda University, Greater Noida, India

Barkha Nandwana

Department of Computer Science &
Application

Sharda School of Computing Science &
Engineering

Sharda University, Greater Noida, India

Abstract

Python implementation of a real-time network analyser is provided here. It shows traffic by protocol, Internet protocol (IP), IP address packets and shows top Ips depending on traffic. It also shows incoming and exiting traffic. As Internet-connected devices grow tremendously, traffic management and network traffic tracking's complexity has skyrocketed as well. Ensuring network security, bandwidth optimization, and anomaly detection depends on traffic analysis tools, which are absolutely indispensable. This project presents a Python real-time traffic analysis tool meant to track, show, and investigate real-time traffic data. It records packets in real time from the network interface and analyses important data including protocols, packet lengths, destination and origin Ips, one important element of the application is its simple graphical interface, which lets users monitor traffic statistics in real time and so makes it readily available to technical and non-technical users alike. Using simple comparative views through updatable charts, it divides traffic into arriving and exiting streams. For reporting or closer inspection, these can be exported in PNG form. It also notes atypical traffic patterns that can cause security concerns or effective yet ineffective bandwidth usage.

Keywords- introduction, network traffic, analysis, protocols, real-time data

1. Introduction

Networking involves forming and developing relationships with other individuals in order to communicate information, share data and take advantage of each other's contacts. In computer terminology, Networking means the interconnectivity of two or more computer devices like computers, servers and other devices so that they may share resources and data between them. Networking consists of physical or virtual interconnected devices through cables, wireless means or other modes of communication. One of the main aim of networking is to make communication between multiple devices easy so that sharing of resources like printers, file servers and internet access between devices possible. By networking the devices share data and information and files and thus make it easy for interaction and sharing of information. The networking is based on communication protocol, such as TCP/ IP protocol that defines the manner in which the data is

transferred between devices. Monitoring of network traffic helps in understanding the network behaviour, detecting possible attacks and ensuring maximum performance of the network. The traditional command-line offer extensive functionalities but without a good interface. The paper overcomes this shortcoming through a Python GUI application having the functionality of real time packet sniffing and traffic analysis.

1.1 Network Types

There are many types of networks in computer networks

- **PAN (Personal Area Network)**

A Pan is the smallest types of networks, typically connecting devices within a personal workspace, such as smartphone, tablet and laptop. Its features are that it utilizes wireless technologies like Bluetooth and Wi-Fi, and can be used to share data and resources between devices.

- **LAN (Local Area Network)**

A Lan give access to limited area, such as a small home, office or building. It uses Ethernet or Wi-Fi for connections, which enables them to connect to devices like printers.

- **MAN (Metropolitan Area Network)**

A man gives access to a larger area than a LAN, typically connecting devices within a city or metropolitan area. Its features are it uses technologies like fiber optics and high-speed data transmission to connect devices across a city.

- **WAN (Wide Area Network)**

A wan connects devices across a wide area, such as a country or even globally.

- **CAN (Campus Area Network)**

A can is a type of network that give connectivity within a specific geographical area, like a college campus or a large corporate facility.

- **VPN (Virtual Private Network)**

A vpn creates a secure private connection over any type of network which make sures that your network in secure or encrypted to any type of cyber threats or illegal access of your network.

- **SAN (Storage Area Network)**

A san gives high-speed data across to storage devices. Its features are that they are often used in data centers and other environments where large amounts of data need to be stored and accessed.

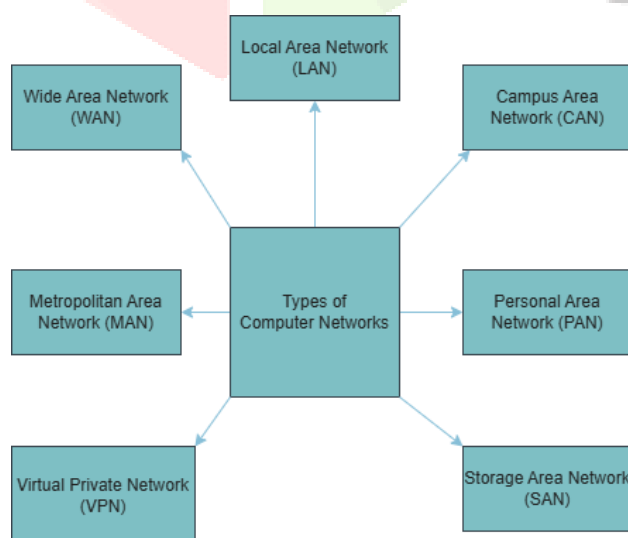


Fig.1 Types of Computer Networks

1.2 Types of Computer Network Protocols

A Computer network protocol is a set of instructions which defines that the data is formatted, transmitted, received and communicate between devices on a network. These rules and instructions ensure that devices can easily communicate between computer with any problems, regards of their hardware. Network protocols act as a common language, allowing devices with different architectures or designs to communicate. They specify how data is structured (e.g. headers, data packets), how it's sent (e.g. specific transmission methods), how its received and how to handle potential errors. These protocols are also important as without these protocols devices on a network would be able to understand each other, making communication impossible. Computer network protocols have different types such as-

1.3 Communication Protocols

These are some protocols communications.

- **Transmission Control Protocol/Internet Protocol (TCP/IP)**
This is the foundation of the internet, providing end-to-end data communication.
- **Hypertext Transfer Protocol (HTTP)**
It provides transformation of data into web content over the internet.
- **File Transfer Protocol (FTP)**
This is the protocols which enables file transfer between computers.
- **Simple Mail Transfer Protocol (SMTP)**
It handles the transmission of email.
- **Domain Name System (DNS)**
DNS transfer domain name (like www.google.com) into IP addresses.
- **User Datagram Protocol (UDP)**
UDP is less reliable but faster protocol for applications like video streaming and online gaming.

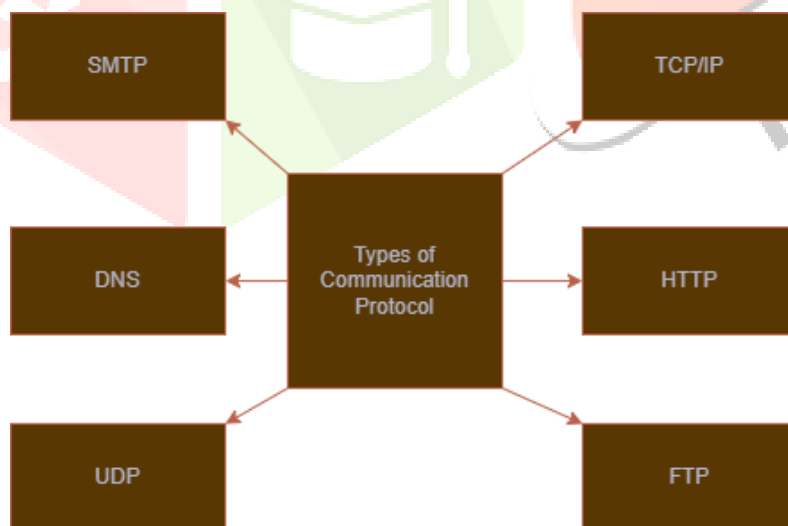


Fig.2 Types of Computer Protocols

1.4 Management Protocols

These protocols oversee and control network operations.

- **Internet Control Message Protocol (ICMP)**
It is used for find problems in the network connectivity.
- **Simple Network Management Protocol (SNMP)**
This protocol give access to network administrators to monitor and manage devices on a network.

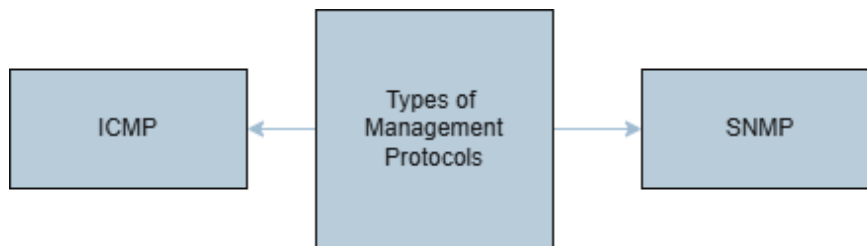


Fig3. Types of Management Protocols

1.5 Security Protocols

These protocols protect data and ensure secure communication.

- **Hypertext Transfer Protocol Secure (HTTPS)**
This is the secure version of HTTP, using encryption to protect data.
- **Secure File Transfer Protocol (SFTP)**
This protocol is a protocol for providing secure file transfer.
- **Secure Sockets Layer/Transport Layer Security (SSL/TLS)**
This is a protocol which is used to create encrypted communication between a web server and a client.

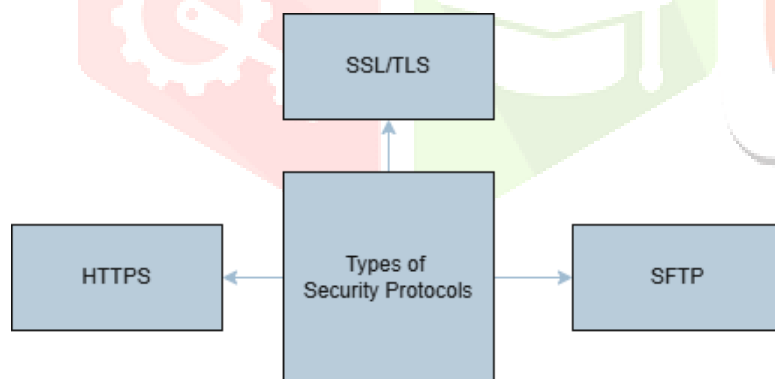


Fig 4. Types of Security Protocols

1.6 Computer Network Architecture

Computer network design and architecture ensures the planning and implementation of a network's physical and logical structure which includes hardware, software and protocols, to facilitate efficient data transmission and communication. It involves decision about network topology, device placement and communication protocols, all aimed to achieve specific business needs and performance goals. Key aspects of computer network design and architecture are

- **Network Components**

This refers to the physical and logical arrangement of network devices (computers, servers, routers, switches) and how they are interconnected. Common topologies include star, bus, ring, and mesh.

- **Hardware Components**

This includes network devices routers, switches, firewalls and servers along with cabling wireless technologies and other infrastructure.

- **Software Components**

This encompasses operating systems network protocols (e.g. TCP/IP, DNS) network management software and security protocols.

- **Communication Protocols**

These are the rules and standards that convert the data which is being transmitted and formatted across the network smoothly and makes sure there is a reliable communication between devices.

- **Security**

Network architecture must have security measures to protect against any kind of unauthorized access, data breaches and other kind of cyber threats.

- **Scalability and Reliability**

A well-designed network should be scalable to accommodate future growth and changed and reliable to ensure consistent and uninterrupted operation.

- **Performance**

Network architecture should optimize network performance for specific application and user need such as minimizing latency, maximizing bandwidth and ensuring efficient resource allocation.

- **Cost-Effectiveness**

Network design should consider the costs of hardware, software, implementation and ongoing maintenance, while achieving the desired performance and security requirements.

- **Network Management**

This involves monitoring the network's performance, troubleshooting issues, and maintaining the network's integrity and security.

- **Common Network Architecture**

- **Peer-to-Peer**

Each device can directly communicate with other devices on the network without a central server.

- **Client/Server**

A central server manages resources and provides services to client devices.

- **Distributed Network**

Data and processing power are distributed across multiple computers and servers, enabling scalability and fault tolerance.

- **Cloud Computing**

Services and resources are provided through the internet, offering flexibility and scalability.

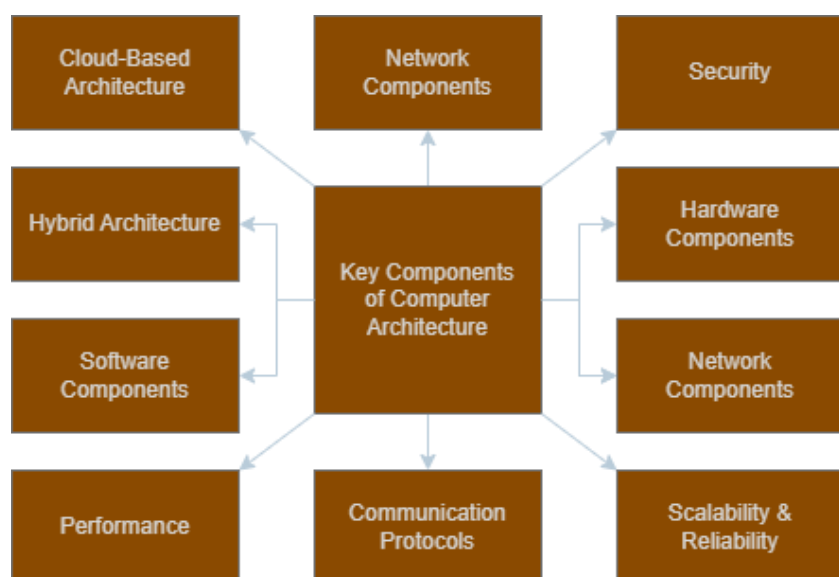


Fig 5. Types of Computer Network Architecture

1.7 Different Types of Computer Network Architecture

Computer network architecture can be broadly categorized into different types listed below

- **P2P Architecture**

P2P network is a network where different devices communicate between them as client and a server. Suitable for small networks, P2P offers simplicity and ease of setup but can be less secure and have performance limitations compared to client-server models. Examples- File Sharing applications, basic home networks.

- **Client-Server Architecture**

A Central server provides services (e.g. file storage, printing) to client devices. Offers centralized management, better security, performance and resource sharing, but can become a single point of failure if the server malfunctions. Examples- Most enterprise networks, web servers, database systems.

- **Hybrid Architecture**

Combines elements of P2P and client-server, allowing for both centralized and decentralized resource sharing. Provides flexibility and scalability, but can be more complex to manage. Example- Larger network where some services are managed centrally while others are peer-to-peer.

- **Cloud-Based Architecture**

Services and resources are hosted on the internet (the “cloud”) and accessed by users over the network. Offers scalability, flexibility and cost-effectiveness but relies on internet connectivity and can have security concerns. Example- Software-as-a-service (SaaS), cloud storage, online applications.

- **Software-Defined Networking (SDN)**

This architecture allows for centralized management and dynamic control of the network. Offers greater flexibility and programmability, enabling faster network configuration and adaption to changing demands. Examples- Large-Scale data centers, virtualized networks.

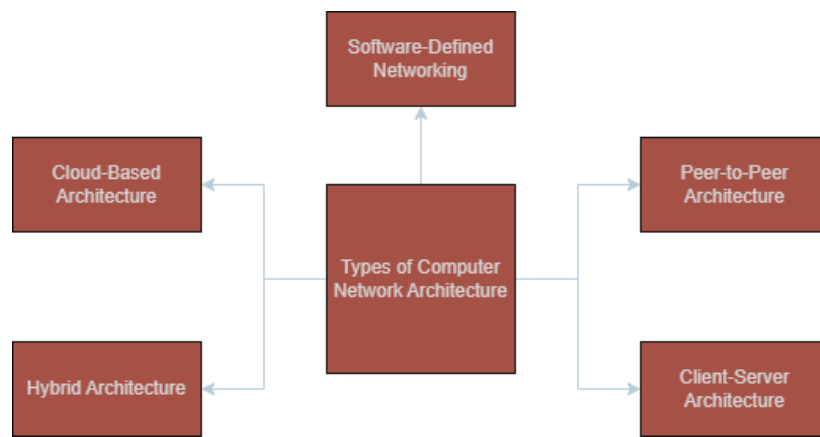


Fig 6. Types of Computer Network Architecture

2. Methodology

2.1 Implementation

To develop this tool, we used the Python programming language and worked within Jupyter Notebook, a browser-based Python IDE. As a first step, we installed essential Python libraries such as scapy, matplotlib, and scapy. We also installed Npcap, a packet capture software designed for Microsoft Windows. Npcap supports the open Pcap API and uses a custom Windows kernel driver, along with the built-in libpcap library for Windows. This setup enables the tool to capture raw network traffic on Windows systems, including traffic from wireless networks, wired Ethernet, localhost, and many VPNs — all through a simple and portable API.

2.2 Npcap Introduction and working

Npcap is a library for capturing and transmitting packets for Windows, written by the Nmap Project. It's the follow-up software for the discontinued WinPcap library which gives a mechanism for Windows applications to interface with raw network traffic, as on Linux and macOS. Npcap gives a means for programs to capture, filter, and even inject packets on the network. Npcap functionality is that it captures and sends the packets independently of the host protocol like TCP/IP. This indicates that it's not capable of filtering or blocking the traffic generated by other programs on the same host: it simply "sniffs" the packets that travel on the wire.

Below are the screenshot of the tools output

In the below Fig 7 you can see the top Ips packets data which is sorted according to the highest data packet IP.

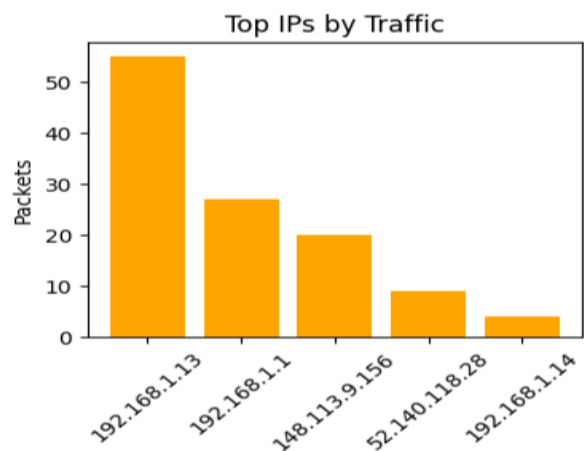


Fig 7. Top IPs by Traffic

In the below Fig 8 you can see the Traffic of different protocols in the wireless network.

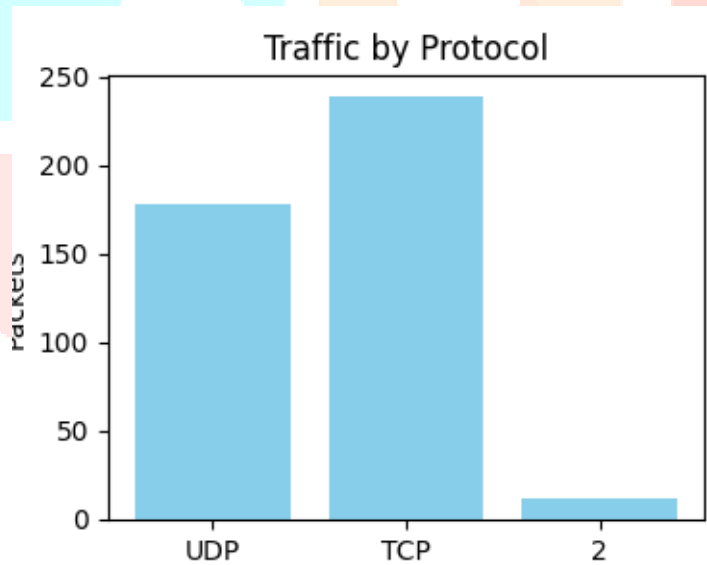


Fig 8. Traffic by Protocol

In the below Fig 9 you can see the incoming and outgoing traffic and their packet sizes.

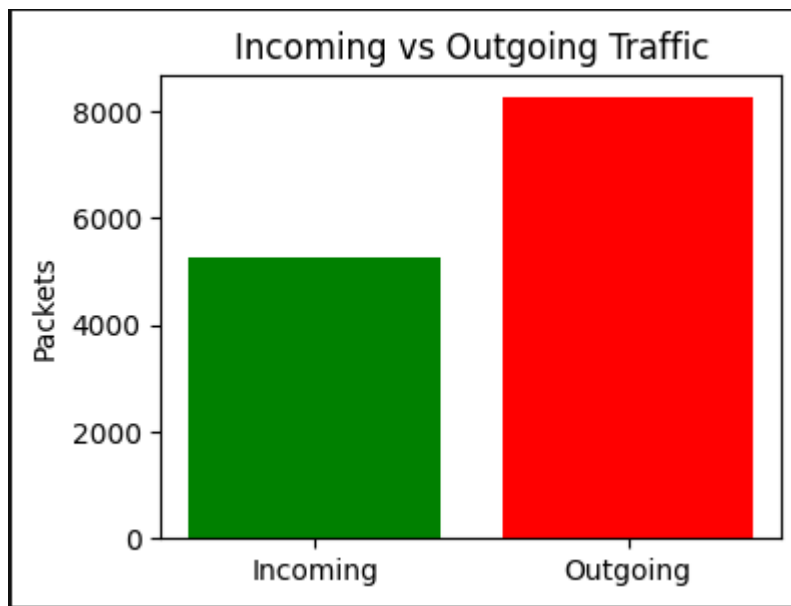


Fig 9. Incoming vs Outgoing Traffic

In the below Fig 10, you can see the list of IP address and their packets using below,

IP Address	Packets
192.168.1.13	161
192.168.1.14	85
192.168.1.1	71
148.113.9.156	26
23.57.251.49	24
204.79.197.203	22
199.232.22.217	16
34.107.204.85	9
172.64.145.151	7
34.36.213.229	6

Fig 10. IP address and its Packet uses

In the below Fig 11, you can see the whole tool GUI which shows that which interface is using in my case its Wi-Fi, it also shows total packets, top Ips by traffic Ip address list with its packets and incoming and outgoing traffic



Fig 11. Tool Screenshot

This application initializes a GUI with controls to start and stop packet capturing. Each packet is analyzed to identify its protocol and IP details, which are used to update counters. Real-time updates are displayed through three key charts-

- **Protocol Usage Chart**
Shows distribution of TCP, UDP, ICMP and other protocols
- **Top IP Addresses Chart**
Displays the most active source Ips.
- **Incoming vs Outgoing Chart**
Compares internal and external traffic flow.

This tool automatically logs all detected IP addresses with their respective packet counts in a CSV file. Users can click a button to export all charts.

3. Conclusion

This Network Traffic Analysis tool is a useful and simple way to track, examine and graphically represent real-time network activities. Through a range of measures including protocols, IP addresses and data flow direction, the application lets technical and non-technical users to view traffic data using simple and strong GUI. The system efficiently gathers and analyzes real-time packets of data by using libraries such as Scapy and Matplotlib as well as tool like Npcap. Apart from graphical analysis, the software maintains historical records in CSV files so one may review prior events. This tool not only simplifies difficult network analysis procedures but also helps to maximize bandwidth and provide better security monitoring. Its adaptability and completeness also make it a good tool for small businesses, personal or educational use. In addition to real-time monitoring the tool maintains comprehensive logs in CSV format.

4. Reference

1. Tian Qin, Guang Cheng, Yuyang Zhou, Zihan Chen, Xing Luan. "SNAKE: A Sustainable and Multi-functional Traffic Analysis System utilizing Specialized Large-Scale Models with a Mixture of Experts Architecture." arXiv preprint arXiv:2503.13808, 2025.([arXiv](#))
2. Gurjot Singh, Alim Dhanani, Diogo Barradas. "RevealNet: Distributed Traffic Correlation for Attack Attribution on Programmable Networks." arXiv preprint arXiv:2505.00618, 2025.([arXiv](#))
3. Borys Lypa, Ivan Horyn, Natalia Zagorodna, Dmytro Tymoshchuk, Taras Lechachenko. "Comparison of feature extraction tools for network traffic data." arXiv preprint arXiv:2501.13004, 2025.([arXiv](#))
4. Jinming Xing, Guoheng Sun, Hui Sun, Linchao Pan, Shakir Mahmood, Xuanhao Luo, Muhammad Shahzad. "NetSight: Graph Attention Based Traffic Forecasting in Computer Networks." arXiv preprint arXiv:2505.07034, 2025.([arXiv](#))
5. Javeriah Saleem, Rafiqul Islam, Zahidul Islam. "Darknet Traffic Analysis: A Systematic Literature Review." arXiv preprint arXiv:2311.16276, 2023.([arXiv](#))
6. Weibao Zhang, Joan P. Lazaro. "A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques." International Journal of Emerging Technologies and Advanced Applications, vol. 1, no. 4, pp. 8–16, 2024.([ijetaa.com](#))
7. "Building a Network Traffic Analyzer for Security Monitoring." Indian Journal of Engineering Research Networking and Development, vol. 1, no. 5, 2024.([ijernd.com](#))
8. "IoT Traffic Analyzer Tool with Automated and Holistic Feature Extraction Capability." Sensors, vol. 23, no. 11, 2023.([MDPI](#))
9. "Developing a Traffic Analysis Suite for Modified Packet Capture File." In Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN 2023), pp. 448–461, 2024.([SpringerLink](#))
10. "A Scalable Framework for Real-Time Network Security Traffic Analysis and Attack Detection Using Machine and Deep Learning." Journal of Cybersecurity and Privacy, vol. 3, no. 2, 2023.([MDPI](#))
11. Akshatha, Dr. Shrinivasan V. "Artificial Intelligence Based Network Traffic Analysis To Handle Large-scale And High Speed Traffic." International Journal of Engineering Research & Technology (IJERT), vol. 11, issue 6, 2023.([IJERT](#))
12. Thaksen Parvat, Siddhi Kolwankar, Neel Lopes, Prathamesh Sawant, Shreya Parchurkar. "Network Traffic Analysis Using Machine Learning." Indian Journal of Computer Science, vol. 9, no. 3, 2024.([indianjournalofcapitalmarkets.com](#))
13. Himanshu Gandhi, Vinay Ribeiro. "Packet Batching for Reducing System Resource Consumption for Botnet Detection using Network Traffic Analysis." In Proceedings of COMSNETS 2022.([ScienceGate](#))
14. Vasaki Ponnusamy, Aun Yichiet, NZ Jhanjhi, Mamoon Humayun, Maram Fahhad Almufareh. "IoT Wireless Intrusion Detection and Network Traffic Analysis." Computer Systems Science and Engineering, vol. 40, no. 3, pp. 865–879, 2022.([ScienceGate](#))

15. Chonghua Wang, Hao Zhou, Zhiqiang Hao, Shu Hu, Jun Li. "Network traffic analysis over clustering-based collective anomaly detection." *Computer Networks*, vol. 202, 2022. ([ScienceGate](#))
16. "User Behavior Traffic Analysis Using a Simplified Memory-Prediction Framework." *Computers, Materials & Continua*, vol. 72, no. 1, 2022. ([ScienceGate](#))
17. "Deep Learning Approaches for Network Traffic Classification: A Survey." *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, 2022.
18. "Anomaly Detection in Network Traffic Using Unsupervised Machine Learning Techniques." *Journal of Network and Computer Applications*, vol. 190, 2022.
19. "Real-Time Network Traffic Analysis Using Apache Kafka and Spark Streaming." *Future Generation Computer Systems*, vol. 135, 2022.
20. "A Comparative Study of Network Traffic Analysis Tools for Cybersecurity." *Journal of Information Security and Applications*, vol. 65, 2022.
21. "Machine Learning-Based Intrusion Detection Systems: A Comprehensive Review." *Computers & Security*, vol. 113, 2022.
22. "Network Traffic Analysis Using Deep Packet Inspection and Machine Learning." *IEEE Access*, vol. 10, 2022.
23. "A Survey on Encrypted Traffic Classification." *ACM Computing Surveys*, vol. 55, no. 1, 2023.
24. "Graph-Based Network Traffic Analysis for Anomaly Detection." *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, 2022. ([ijetaa.com](#))
25. "Time-Series Analysis of Network Traffic for Predictive Maintenance." *Journal of Network and Systems Management*, vol. 30, no. 3, 2022.
26. "Application of Reinforcement Learning in Network Traffic Management." *Computer Networks*, vol. 210, 2022.
27. "Blockchain-Based Secure Network Traffic Analysis Framework." *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, 2022.
28. "Edge Computing for Real-Time Network Traffic Analysis." *IEEE Internet of Things Journal*, vol. 9, no. 5, 2022.
29. "Privacy-Preserving Network Traffic Analysis Using Federated Learning." *IEEE Transactions on Information Forensics and Security*, vol. 17, no. 1, 2022.
30. "Automated Network Traffic Analysis Using Natural Language Processing Techniques." *Journal of Cybersecurity*, vol. 8, no. 1, 2022.