Network Traffic Moniter

Mr. Atul Ramlal Saroj[1], Dr.UdayAswalekar[2]
[1] University of Mumbai

Abstract- *Network traffic analysis is crucial for overseeing and protecting modern network infrastructures or network connections as they help in monitoring, analyzing and troubleshooting network related activities.Enhancing air quality monitoring, raising public awareness, and enabling data-driven decision-making,While it's easy to use and offers many benefits, such as safeguarding your.The conclusion finally sums up the findings and aims to guide on choosing the best tool based on specific network requirements and preferences*

Keywords- Data-Driven Network Traffic Analyzer, Netflow Analyzer, tcpdump, Wireshark, Packets, Protocols, Commands.

I. INTRODUCTION

During this digital revolution, networks play a major role in communication, data exchange, and letting information flow smoothly across different channels. Nonetheless, security, effectiveness, and authenticity are not always easy to maintain on these networks. In addition, one needs advanced and modern network analyzer tools that will help them understand the intricacies of network operations.

These are software-based tools that are designed to capture, check, and analyze data packets that travel across the network. By examining these packets, they give us precise insights about network performance, potential threats, and overall robustness. There are various network analyzer tools each offering different services that one can use as per their convenience and requirement.

This research paper digs into the world of several network analyzer tools such as tcpdump, Wireshark and NetFlow Analyzer. Through the exploration of their working, features, and comparative analysis this paper can help network administrators and security professionals to make informed decisions regarding network monitoring and analysis strategies. In the next sections, the working of these tools will be thoroughly examined, with an emphasis on their operation, advantages, and disadvantages. This study aims to provide readers with information that they can utilize to optimize network speed, improve security, and lower risks associated with today's evolving network settings by dissecting tcpdump, Wireshark, and NetFlow Analyzer.

II. LITERATURE SURVEY

Different tools used for network analyzer

There are multiple tools online through which one can use the tool for traffic analysis, network packet gathering and many more. Below mentioned are some of the tools with their description and working along with the pictures:

Wireshark

Wireshark is a network protocol analyzer tool that helps in capturing packets and also tells the network traffic. It is a vital tool in the field of network analysis and diagnostics because of its many capabilities and intuitive interface. It’s the most often used packet sniffer compared to others. It enables users to record and interactively explore network traffic between connections. It may be downloaded for free and can be run on any operating system, such as Linux, macOS, and Windows. Hackers find this tool useful for them to capture the unencrypted traffic and, thus, gather more information about their targets. It is used by network engineers and security professionals to troubleshoot network issues, assess network performance, to find network intrusions and look into security occurences. By using this tool, we get to know how all devices, like laptops, mobile devices, switches, and routers, communicate in a network and about network communication protocols.

Fig. 1. Wireshark Interface

The functioning of wireshark is similar to that of tcpdump, which is also a network traffic analyzer. Wireshark can capture the packets either in real-time from the network interface or from a capture file that has been saved earlier. There are different network protocols which are supported by wireshark such as TCP/IP, UDP, HTTP, FTP, and others.

Wireshark offers a broader view of each packet's header and payload when the packets are collected. As it can decode the packets by using a particular protocol that is in use,

users can look into a detailed analysis, which includes different protocols, source and destination IP addresses, port numbers, and packet timing. Once packet starts flowing over the interface, Wireshark starts recording and analysing them. Wireshark has robust filtering features in which users can basically focus on particular packet kinds or discussions over the network. A range of standards, including protocols, source and destination IP addresses, port numbers, and packet contents, are suitable for applying filters.

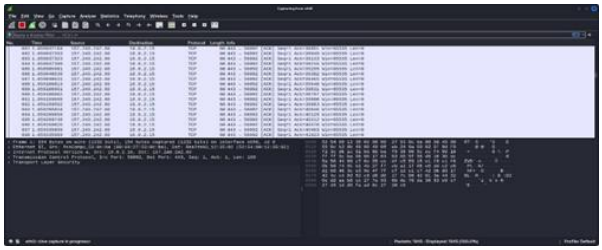
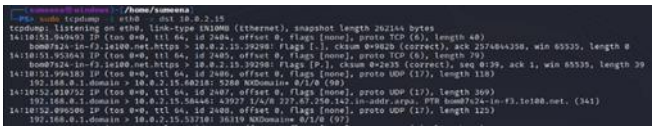


Fig. 2. Wireshark Working Principle

Higher-level protocols like HTTP, FTP, and SMTP can be rebuilt by Wireshark in order to show or display the contents of web pages, files transferred, and email messages exchanged. Packet count, traffic distribution, and protocol usage are just a few of the statistics and visualization tools that Wireshark offers for analyzing network traffic trends. It can also help in creating charts and graphs to help individuals understand network dynamics more naturally.Wireshark is also used for network troubleshooting. By looking into issues like malicious activity, configured devices or network congestion by examining at collected packets.Wireshark includes a feature that lets users rebuild and view the whole interaction between two end points for the protocols that use TCP. This makes it easier to understand the transfer of data between client and server applications. Using Wireshark, users can save recorded packets or may further evaluate then in different types of format and it works with CSV, PCAP and PDML.



Tcpdump commands and analyzing it

Software: The AQI checking device's software has several functions. The device's functionality, including the collection, processing, and communication of sensor data, is managed by the firmware. Data visualization, setting, and interaction are made easier by user interface software. Based on sensor measurements, data analysis algorithms determine the AQI, and reporting systems produce reports or alarms. Remote AQI data management and monitoring are made possible by cloud-based software or smartphone apps.

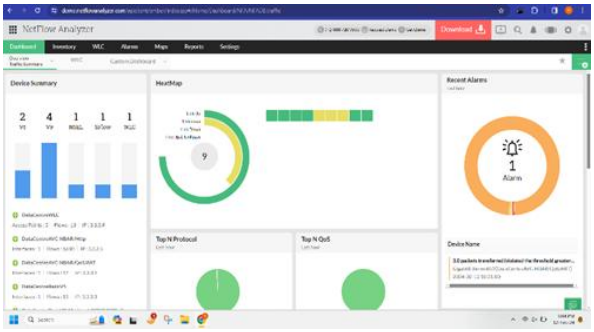
Calibration and Maintenance: These devices need to be calibrated and maintained on a regular basis to guarantee the accuracy of AQI readings. In order to account for sensor drift or imperfections, calibration entails comparing sensor measurements with reference equipment and applying the required corrections. Sensor cleaning, firmware upgrades, and routine device inspections are examples of maintenance duties.

Features of Net Flow Analyzer:

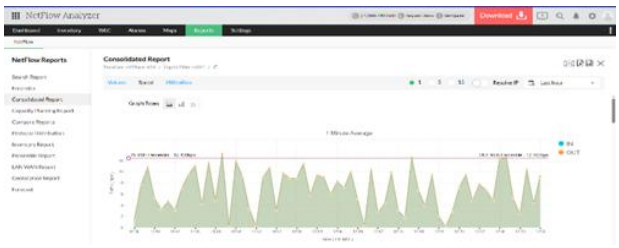
•Network Traffic Analysis (NTA): Evaluates network stability, performance degradation, device capabilities, and speed.
•Protocol and Application Monitoring: Categorizes and maps enterprise-specific applications according to user requirements.
•VoIP Monitoring: Tracks parameters such as jitter, latency, and packet loss to ensure high-quality voice communications.
•Traffic Shaping: It prioritises the traffic which helps to increase the performance of the user.
•NBAR Monitoring: It classifies the applications based on the dynamic ports available in the device.
•Bandwidth Management:
•Scans usage details, manages bandwidth cautiously, and gives alerts.
•Offers adaptive dashboards and enterprise bandwidth monitoring.
•Flow-based Monitoring: It uses J-Flow, sFlow, IPFIX, and NetFlow analysis.
•NetFlow Analyzer Reports: Specialised reports cover bandwidth, range planning, cost, and troubleshooting.
•Add-ons and Plug-ins: It includes Cisco IP SLA Monitoring, ManageEngine Network Configuration Manager, and IP Address Governance.
•Network Security and Forensics: Covers forensics, anomaly detection, deep packet inspection, and security reporting.
•Other Features: switchover setup, CISCO CBQoS validation, site-to-site monitoring, distributed monitoring, and WLAN Controller (WLC) Monitoring.

To conclude, Netflow Analyzer is an excellent network analyzer tool that can be used as a web app. It also allows the user to use this tool as a mobile application so that it can be accessible at any time and for anyone. It has 3 editions, namely Standard for 500 interfaces at 8595$, Professional for 10 interfaces at 595$, and Enterprise for 10 interfaces at 1045$. It also has a free edition with only two interfaces. Also, it generates an entire report of your network

analysis that includes your bandwidth utilisation, capacity planning, billing, troubleshooting, etc. Because of these reasons, it is widely used in companies as it reduces their costs and the process becomes automated.



The above image depicts the web based dashboard of the Netflow Analyzer that includes the Device Summary, Alerts, HeatMap and the applications used in the last one hour. The dashboard can also be customised as per users' requirement



The above image shows the consolidated report of the entire network traffic, which includes bandwidth utilisation, volume, and speed, in the form of a graph. Also, it allows us to get different reports as per our convenience and requirements, which can be visible on the left of the image.Developing a biometric authentication system involves several crucial stages. Initially, defining authentication requirements is essential, aligning capabilities with data privacy regulations. Threat modelling identifies and mitigates potential risks, ensuring the system's integrity and confidentiality. After assessing requirements and threats, appropriate biometric technology is selected, considering factors like accuracy and user acceptance. Database design focuses on encryption to safeguard biometric data, while enrollment processes secure its collection and storage. Integration efforts seamlessly embed biometric authentication into existing systems, enhancing user experience. User training is vitalthroughout the development lifecycle, ensuring compliance with regulatory frameworks. Adherence to these principles ensures the system's efficacy, security, and regulatory compliance in biometric authentication.Define authentication requirements aligned with data privacy regulations.Conduct threat modelling to identify and mitigate potential risks.Select appropriate biometric technology based on factors like accuracy and user acceptance.

Design database structure with encryption mechanisms to safeguard biometric data.

Implement enrollment processes for secure collection and storage of biometric information. - Integrate biometric authentication seamlessly into existing systems or applications. - Provide user training throughout the development lifecycle to ensure compliance with regulatory frameworks

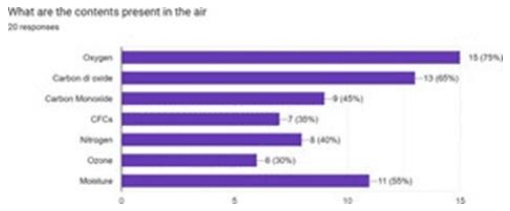
Facial recognition has gained significant attention due to its non-intrusive nature, accuracy, and ease of use. Li and Jain (2018) presented an in-depth analysis of facial recognition algorithms, discussing the evolution from basic feature-based techniques to modern machine learning-based approaches, such as deep convolutional neural networks (CNNs). Their findings show that deep learning has significantly improved recognition accuracy in varying conditions, making facial recognition increasingly viable for authentication systems.

However, studies like those conducted by Buolamwini and Gebru (2018) reveal bias issues within facial recognition systems, especially in identifying individuals from diverse demographic backgrounds. These findings highlight the importance of creating systems that are tested on diverse datasets to ensure fair and unbiased recognition. The high computational demands of facial recognition were also noted by Wang et al. (2019), suggesting that optimizing these systems is crucial for deploying them in real-time applications, particularly for large-scale, multi-user systems.

RSA encryption is a well-established method of asymmetric cryptography that remains widely used for secure data exchange. Rivest, Shamir, and Adleman (1978) originally introduced RSA encryption, which relies on a pair of public and private keys to ensure secure data access. The system’s robustness agains attacks has made it a preferred method for sensitive data encryption, especially in applications where data confidentiality is paramount.

Recent studies by Sahai and Waters (2020) indicate that RSA encryption, when combined with biometric systems, can provide an additional layer of security by requiring both the biometric verification and an RSA private key for access. This two-factor approach has been particularly effective in protecting sensitive information, as shown in studies of multi-factor authentication systems in online banking (Zhu and Huang, 2021). However, RSA encryption is computationally

intensive, which poses a challenge for systems requiring rapid authentication, especially in combination with facial recognition.



Comparative analysis

TABLE I. Comparative Analysis between Wireshark, tcpdump and Netflow Analyzer

Features	Wireshark	Tcpdump	NetFlow Analyzer
Type	GUI	CLI	Varies Applications
Platform	Cross-platform (Windows, macOS, Linux)	Cross-platform (Windows, macOS, Linux)	Varies
Filtering	Offers powerful filtering capabilities	Supports Filtering based on command	Provides filtering based on attributes
Data Capture	Live and Offline	Live Only	Flow records (aggregated network traffic data)
Ease of Use	User Friendly due to GUI	Familiarity with CLI command	User Friendly due to GUI
Real Time Analysis	Yes	Yes	Limited
Security	Used for security Analysis	Basic Security Monitoring	Insight into threats and network traffic patterns
Cost	Free	Free	Free or commercial

III. RESULT AND DISCUSSION

Through this study, we aimed to do a comparative study of network traffic analyzers, which included Wireshark, tcpdump, and Netflow Analyzer tools and highlighted unique functionalities and applications. With a user-friendly graphical interface, Wireshark is a robust packet analyzer that offers wide protocol study and real-time traffic inspection. TCPdump, though not having a good GUI, offers simple packet capture and filtering features that are useful for command-line users and for short analytical tasks.real-time notifications, and possible additions of more weather parameters. The information gathered will be crucial in improving and honing the project, directing choices about preserving its advantages and tackling its shortcomings. The survey's user preferences will be used to prioritize features, making sure the weather station closely matches customer requirements and expectations.from participants, including comments on the system's overall usability, perceived accuracy of weather data, and user experience. Responses on usability are expected to vary, with users showing interest in accessibilityTheNetflowAnalyser is best for large-scale network systems as it provides understanding about traffic patterns and usage of bandwidth. In order to meet the requirements of network analysis, factors like performance and ease of use should be taken into consideration while selecting an analyzer

IV. CONCLUSION

In conclusion, this paper dive into the realm of network traffic analysis, highlighting the crucial importance in securing and managing the network. Through the exploration of different tools like, Wireshark, Tcpdump, NetFlow analyzer, the paper has gained valuable knowledge with respect to the significance of the tools., its functionalities, strength and limitations.The user-friendly interfaces of the AQI checker, both on the device and through mobile or web applications, enable authorities and individuals to readily access vital information about air quality. It provides users with immediate notifications, historical data access, and real-time data visualization, empowering them to make well-informed decisions to safeguard their health and wellbeing. An important instrument for raising public awareness of air quality, directing public health responses, influencing environmental policy, and encouraging research on air quality-related topics is the AQI testing device. Its effective creation and implementation support the overarching objective of reducing air pollution and improving the standard of living for people everywhereBased on the research, we had found that each tools have its own advantages and disadvantages. While researching, we conclude with some key-aspects, Wireshark and Tcpdump are good in packet level analysis and when while concluding for the ease of use, the Tcpdump lags behind

the Wireshark and NetFlow analyzer, the reason is pretty clear, because of the CLI interface in Tcpdump. The Network Traffic Analyzer plays an effective role in rapidly growing network infrastructure and cybersecurity threats.This research proves a valuable resource for each one finding the guide for selection and implementation of appropriate network traffic analyzer tools, helping different organizations to manage and secure their network in face of modern challenges.

V. ACKNOWLEDGMENT

I, Atul Saroj would like to express our gratitude to Vidyavardhi's College of Engineering and Technology for providing us with the opportunity to work and construct this research paper. We'd also like to thank Dr.UdayAswalekar.,who provided us with unconditional support, knowledge and guidance and continuously worked to motivate and encourage us to publish this paper..

REFERENCES

[1] Y. Zhou, Q. Zhou, Q. Kong, and W. Cai, "Wireless temperature amp; humidity monitor and control system," in 2012 2nd InternationalConference on Consumer
[2] S. Gangopadhyay and M. K. Mondal, "A wireless framework for environmental monitoring and instant response alert," in 2016 Internationale Conference on
[3] Microelectronics, Computing and Communications(MicroCom), Jan 2016, pp. 1–6.
[4] Y. Zhou, Q. Zhou, Q. Kong, and W. Cai, "Wireless temperature amp; humidity monitor and control system," in 2012 2nd InternationalConference on Consumer