Journal of Information Systems Engineering and Management
2025, 10(49s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Network Traffic Analyzer

Ditixa Mehta[1], Aditi Nikam[2], Sumit Sharma[3], Vaibhav Walunj[4]
[1]*Assistant Professor, Computer Science and Engineering (Cyber Security), Thakur College of Engineering and Technology, Mumbai, India*
[2,3,4] *Student, Computer Science and Engineering (Cyber Security), Thakur College of Engineering and Technology, Mumbai, India*
Email: ditixa.mehta@tcetmumbai.in

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

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. This aims to provide understanding into their capabilities, advantages and disadvantages so that security professionals and network administrators may choose the appropriate solution for their specific requirements. This paper presents a comparative analysis of three renowned network traffic analyzer tools: Wireshark, tcpdump and NetFlow Analyzer, offers its own unique features and practicality. The introduction highlights the significance of network traffic analysis and states the objectives and value of comparing these tools. The features, functionalities and description of each tool and their working principles are covered in this document. Wireshark and tcpdump are packet sniffers, NetFlow Analyzer focuses on flow-based analysis and uses sensors to detect traffic. Based on the factors such as performance, robustness, accessibility, protocol support, a comparative analysis is carried out. The outcomes and discussions demonstrate the pros and cons of each network traffic analyzer tool. The conclusion finally sums up the findings and aims to guide on choosing the best tool based on specific network requirements and preferences.

Keywords: Network Traffic Analyzer, Netflow Analyzer, tcpdump, Wireshark, Packets, Protocols, Commands.

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. [4]

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. [10]

METHODOLOGY

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.

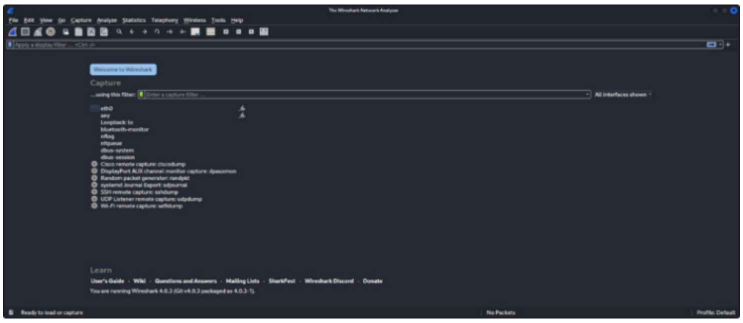

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.0.3 (Git v4.0.3 packaged as 4.0.3-1).
Ready to load or capture
No Packets
Profile: Default

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. [6]

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.

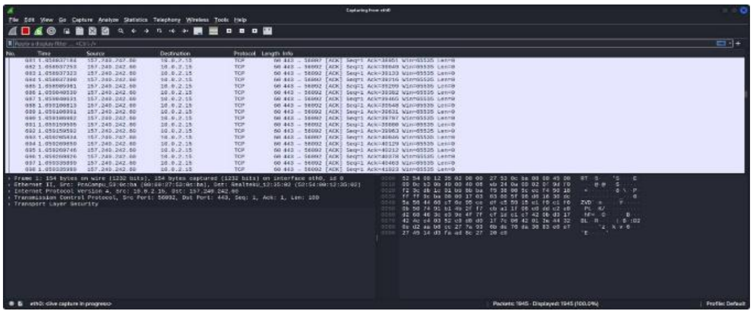

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No.
Time
Source
Destination
Protocol
Length
Info
Transport Layer Security
eth0: <live capture in progress>
Packets: 1945 · Displayed: 1945 (100.0%)
Profile: Default

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. [3]

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.

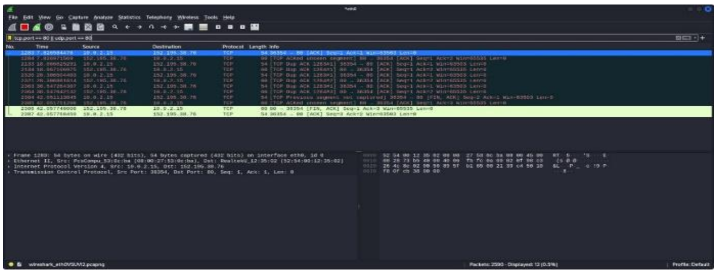
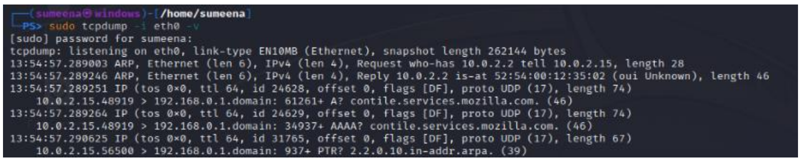

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80 || udp.port == 80
No. Time Source Destination Protocol Length Info
wireshark_eth0VSUVI2.pcapng
Packets: 2590 · Displayed: 12 (0.5%)
Profile: Default

Fig. 3. Wireshark Protocols

Tcpdump- TCPDUMP is a command line interface, it is used to capture and analyze network traffic which is running in this system. It does not have any UI interface, it is fully functionable via command interface. It is very easy to use, the main thing about tcpdump is the syntax which we use to give in the command and through the command, one can capture the ports and traffic. Tcpdump is usually pre-installed in Kali Linux. It is an effective tool used for troubleshooting and analyzing networks. This enables the users to capture and inspect the traffic that is flowing through a network interface in real-time. In Particular, it acts as a digital packet sniffer, used to view and transmit the packet over a network. This tool particularly proves in monitoring network activity, analyzing network protocols and diagnosing network problems.

Below are some of the basic commands that one can use to analyze traffic and packets.

The very first command is sudo tcpdump -i eth0 -v



```
┌──(sumeena㉿windows)-[/home/sumeena]
└─PS> sudo tcpdump -i eth0 -v
[sudo] password for sumeena:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:54:57.289003 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.2.2 tell 10.0.2.15, length 28
13:54:57.289246 ARP, Ethernet (len 6), IPv4 (len 4), Reply 10.0.2.2 is-at 52:54:00:12:35:02 (oui Unknown), length 46
13:54:57.289251 IP (tos 0x0, ttl 64, id 24628, offset 0, flags [DF], proto UDP (17), length 74)
    10.0.2.15.48919 > 192.168.0.1.domain: 61261+ A? contile.services.mozilla.com. (46)
13:54:57.289264 IP (tos 0x0, ttl 64, id 24629, offset 0, flags [DF], proto UDP (17), length 74)
    10.0.2.15.48919 > 192.168.0.1.domain: 34937+ AAAA? contile.services.mozilla.com. (46)
13:54:57.290625 IP (tos 0x0, ttl 64, id 31765, offset 0, flags [DF], proto UDP (17), length 67)
    10.0.2.15.56500 > 192.168.0.1.domain: 937+ PTR? 2.2.0.10.in-addr.arpa. (39)
```

Fig. 4. Tcpdump command line interface

One can start with the TCPDump tool in Kali Linux using the command, “sudo tcpdump -i eth0 -v”. So let's break into some instances, so that it can be easier to understand. The “sudo” command is used to execute the command by giving the root user privileges. Later the command “tcpdump” itself represents the start of a network packet capture. Here, “-i eth0” specifies, the network interface from which the traffic is to be captured is indicated. The “-v” option helps to activate verbose mode, which leads to more significant output regarding the captured packets and ports, including protocol and ports information and packet header details.

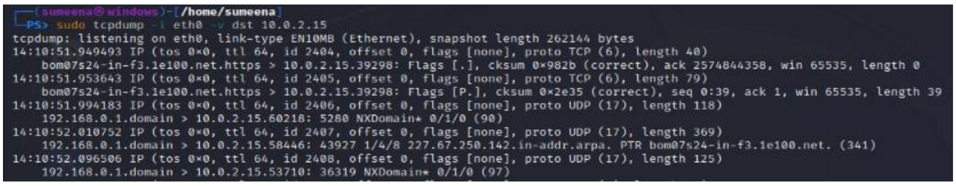
In short, this command captures network traffic efficiently on the designated ports, providing detailed output that proves valuable for thorough packet and traffic analysis.

Two major points to note here are the source and the destination IP addresses. The Ip address which is seen on the left side represents the source IP address (src), whereas the IP address present on the right represents the destination IP address.

It can nicely be understood by the example below:

10.8.3.14 > 192.178.0.4

So here, the source IP address is 10.8.3.14 and the destination IP address is 192.178.0.4.



```
┌──(sumeena㉿windows)-[/home/sumeena]
└─PS> sudo tcpdump -i eth0 -v dst 10.0.2.15
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
14:10:51.949493 IP (tos 0×0, ttl 64, id 2404, offset 0, flags [none], proto TCP (6), length 40)
    bom07s24-in-f3.1e100.net.https > 10.0.2.15.39298: Flags [.], cksum 0×982b (correct), ack 2574844358, win 65535, length 0
14:10:51.953643 IP (tos 0×0, ttl 64, id 2405, offset 0, flags [none], proto TCP (6), length 79)
    bom07s24-in-f3.1e100.net.https > 10.0.2.15.39298: Flags [P.], cksum 0×2e35 (correct), seq 0:39, ack 1, win 65535, length 39
14:10:51.994183 IP (tos 0×0, ttl 64, id 2406, offset 0, flags [none], proto UDP (17), length 118)
    192.168.0.1.domain > 10.0.2.15.60218: 5280 NXDomain* 0/1/0 (90)
14:10:52.010752 IP (tos 0×0, ttl 64, id 2407, offset 0, flags [none], proto UDP (17), length 369)
    192.168.0.1.domain > 10.0.2.15.58446: 43927 1/4/8 227.67.250.142.in-addr.arpa. PTR bom07s24-in-f3.1e100.net. (341)
14:10:52.096506 IP (tos 0×0, ttl 64, id 2408, offset 0, flags [none], proto UDP (17), length 125)
    192.168.0.1.domain > 10.0.2.15.53710: 36319 NXDomain* 0/1/0 (97)
```

Fig. 5. Tcpdump commands and analyzing it

So, after knowing the basic command and its description, let's understand some of the commands used for filtration.

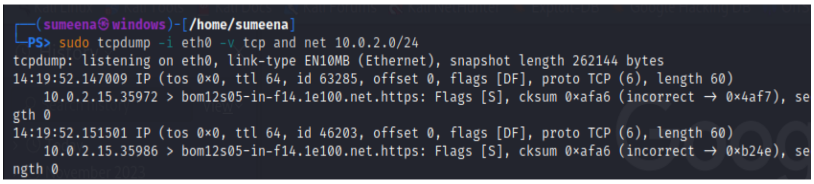
`sudo tcpdump -i eth0 -v dst ip_address`

The command here is used to filter to get the desired output. As from the above image, it can be clearly seen that the output generated here has the same destination IP address as mentioned in the command. Here, dst means Destination, similar things can be done for getting the source IP address, while exchanging the dst to src for analysis.

When we execute the above command.

Tcpdump -i eth0 -v host #ip_address

It could help to yield output with complete details regarding the traffic associated with the designated host IP address present on the eth0 network interface. The output contains exclusive information about each packet, such as the source and destination IP address, port numbers, packet size and timestamps. Examining and analyzing this can help pertaining to a particular host.



```
┌──(sumeena㉿windows)-[/home/sumeena]
└─PS> sudo tcpdump -i eth0 -v tcp and net 10.0.2.0/24
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
14:19:52.147009 IP (tos 0×0, ttl 64, id 63285, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.2.15.35972 > bom12s05-in-f14.1e100.net.https: Flags [S], cksum 0×afa6 (incorrect → 0×4af7), se
gth 0
14:19:52.151501 IP (tos 0×0, ttl 64, id 46203, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.2.15.35986 > bom12s05-in-f14.1e100.net.https: Flags [S], cksum 0×afa6 (incorrect → 0×b24e), se
ngth 0
```

Fig. 6. Tcpdump commands

In the above command, we have used a different approach to fitarate, here we had to use the operator like "and" and "not" to narrow down the output based on specific criteria. By using the operators in the command line, we can get the desired output. Like from the above command from picture, the resulting output consists of packets that have both TCP ports and a network address of the IP address. This has become successful by combining both the conditions of tcp and net using the "and" operators. This technique improves the efficiency of the output produced by TCPDump.

To save tcpdump file in wireshark-

Tcpdump -w /root/Desktop/traffic.pcap -i eth- -v 'tcap and net 192.168.1.0'

The provided command is used in tcpdump, to capture the network traffic and to save it to a file in the PCAP (Packet Capture) format. When executed this command will capture TCP packets from the network specified by applying the filter and save them into the specified files format.

Netflow Analyzer- NetFlow Analyzer is a traffic interpreter tool that helps us to check the network bandwidth performance instantaneously. Originally designed as a bandwidth monitoring tool, it has been used to improve trillions of networks worldwide by providing an extensive view of their traffic patterns and network bandwidth. It is an all-purpose network traffic monitor that collects, checks, and creates reports data regarding the uses and receivers of your network bandwidth. It is an authentic partner that improves network traffic analysis, network flow monitoring, and network forensics across over a billion interfaces worldwide. Through net flow analyzer the user can gain complete insight into high network traffic, application performance, devices, interfaces, IPs, wireless network, WAN links, SSIDs, and access points, as well as we can track the bandwidth utilisation. AVC, NBAR, CBQoS, and IP SLA are just a few of the Cisco technologies that NetFlow Analyzer supports. [5]

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. [7] [9]

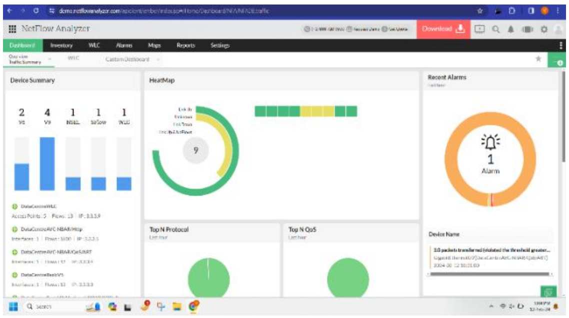


Fig. 7. Netflow Analyzer Interface

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.

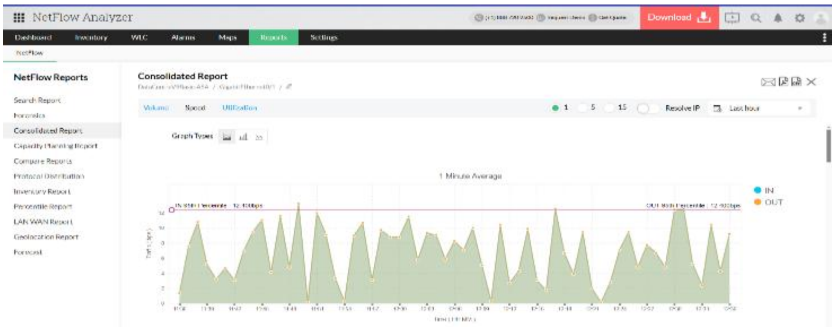


Fig. 8. Netflow Analyzer generated report

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. [1]

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. The Netflow Analyser 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. [2] [8]

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

Table 1. Comparative Analysis between Wireshark, tcpdump and Netflow Analyzer

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.

Based 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.

REFRENCES

[1] Akhunzada, A., Ahmed, M. A., & Minhas, A. (2015). Network traffic analysis and prediction using machine learning. Procedia Computer Science, 56, 246–251.

[2] Cheng, Z., Liu, H., Tan, Y., Li, T., & Qian, Z. (2020). FlowLens: Enabling an efficient flow-level network traffic analyzer. IEEE/ACM Transactions on Networking, 28(5), 2072–2085.

[3] Kreibich, C., Han, J., & Paxson, V. (2010). VAST: A unified platform for interactive network traffic analysis. In USENIX Workshop on Cyber Security Experimentation and Test.

[4] Nguyen, T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys & Tutorials, 10(4), 56–76.

[5] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167.

[6] Roesch, M. (1999). Snort: Lightweight intrusion detection for networks. In LISA (Vol. 99, No. 1, pp. 229–238).

[7] Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers & Security, 31(3), 357–374.

[8] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE Symposium on Security and Privacy (pp. 305–316). IEEE.

[9] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (pp. 1–6). IEEE.

[10] Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: A survey. Journal of Big Data, 2(1), 1–41.