2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI) | 979-8-3503-6996-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCSAI59793.2023.10421631

Advanced Techniques in Network Traffic Analysis: Utilizing Wireshark for In-Depth Live Data Packet Inspection and Information Capture

Santhosh Chowhan,
Department of Data Analytics and Mathematical Sciences, Jain (deemed to be) University, Bangalore, Karnataka, India
santosh.sc@jainuniversity.ac.in
Orcid id 0000-0003-1107-8287

Abhilash Kumar Saxena,
College Of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India,
abhilashkumar21@gmail.com
Orcid id- 0000-0003-2363-6143

Abstract - **The escalating frequency and sophistication of cyber-attacks have placed a spotlight on the importance of Quality of Service (QoS) and robust network security mechanisms. Effective traffic analysis and distribution are critical for maintaining the integrity of network applications and safeguarding data.Our research focuses on the development and assessment of a network intrusion detection system (NIDS) that utilizes the advanced packet analysis capabilities of Wireshark, a renowned network protocol analyzer. The system is designed to enhance network security by enabling more efficient and accurate data collection through network monitoring tools. This serves as the foundation for detecting and thwarting a wide range of malicious activities, including malware and spyware incursions, within network traffic. The innovation of our approach lies in its integration of packet sniffing technology with AI-driven analysis techniques. By applying Machine Learning algorithms to the data captured by Wireshark, our NIDS is capable of identifying patterns indicative of intrusive behavior, which might elude traditional detection methods. We present a comprehensive evaluation of our system, showcasing its efficacy in real-time intrusion detection and its potential for integration into existing network infrastructures. This study contributes to the ongoing discourse in cybersecurity, offering a sophisticated tool in the battle against digital threats and reinforcing the role of intelligent systems in protecting network environments..**

Keywords- Network Traffic Analysis, Wireshark for Data Packet Inspection, Real-Time Network Monitoring, packets, Data Packet Analysis Techniques, Network Security and Forensics.

I. INTRODUCTION

In an era where the internet has become the backbone of global communication and data exchange, network security stands as a critical pillar of Computer Science and Information Technology [1]. With daily cyber threats escalating in both volume and complexity, the quality of service (QoS) and the reliability of network applications are under constant threat. This has compelled researchers and network operators to devise sophisticated mechanisms for traffic analysis and distribution to preemptively identify and mitigate these threats [2]. The advent of Network Intrusion Detection Systems (NIDS) marks a significant milestone in our ability to defend against cyber-attacks. These systems serve as the sentinels of network security, monitoring traffic to detect malicious activities in their incipiency. Our investigation revolves around one such tool at the forefront of network monitoring technology—Wireshark. Known for its comprehensive packet analysis capabilities, Wireshark enables the meticulous scrutiny of network traffic, thereby forming the crux of our intrusion detection methodology. This paper elucidates the development of an NIDS that harnesses Wireshark's potent packet sniffing functionalities, complemented by AI and Machine Learning techniques [3-4]. By integrating these computational methods, the proposed system goes beyond conventional rule-based detections. It evolves into a dynamic, learning, and predictive model, capable of discerning even the stealthiest of cyber threats.

We provide a detailed introduction to the architecture of our NIDS, the rationale behind selecting Wireshark, and the innovative use of AI to analyze network traffic. This paper sets the stage for a discussion on the intersections of network security, data analysis, and AI, and how this synergy can yield robust solutions to the ever-growing challenges of cyber security.

II. LITERATURE REVIEW

The study conducted by [5] involved an examination of multiple novel intrusion detection methodologies, with a subsequent evaluation of their efficacy utilizing KDD Cup99 intrusion data. The models of Support Vector Machine (SVM) and Gaussian Process (GP) were taken into consideration for the purpose of intrusion detection. Subsequently, a hybrid model comprising SVM and GP was developed, alongside an aggregation technique that employed SVM, GP, and SVM-GP models as the principal means of classification. [6] et al. presented a comprehensive summary of the prerequisites and advantages associated with intrusion detection systems. This paper presents a comprehensive examination of intrusion detection systems, including their various types, lifecycles, geographical distributions, and attack modalities. In contemporary times, Intrusion Detection Systems (IDS) have emerged as a crucial component of safeguarding the security of businesses and network users. The implementation of security measures is regulated by IPS. Throughout the course of a life

Copyright © IEEE–2023 ISBN: 979-8-3503-6996-0

cycle, distinct phases emerge and subsequently attain greater clarity. There exist additional obstacles that must be addressed. This particular methodology is executed with the express purpose of identifying irregularities and detecting instances of maltreatment, while alternative methodologies may also be employed. The study conducted by [7] highlighted the necessity of enhancing intrusion detection and prevention systems to enhance the security of computer networks. The unreliability of these tools, primarily attributed to the occurrence of false positives and false negatives, renders their usage challenging. Presently, it is evident that these systems are imperative in guaranteeing the security of enterprises. It is advisable to integrate multiple detection mechanisms to guarantee the security of the computing system. The Inertial Particle Separator (IPS) has been found to offer only limited mitigation of the aforementioned issues and is therefore deemed insufficiently robust for application in the construction industry. The authors in [8] explicate the function and influence of intrusion detection and prevention systems within network settings. The Intrusion Prevention System (IPS) is capable of identifying and intercepting harmful packets originating from malware, bots, viruses, and targeted attacks. Additionally, it possesses the ability to proactively mitigate network damage by preventing any further network activity.

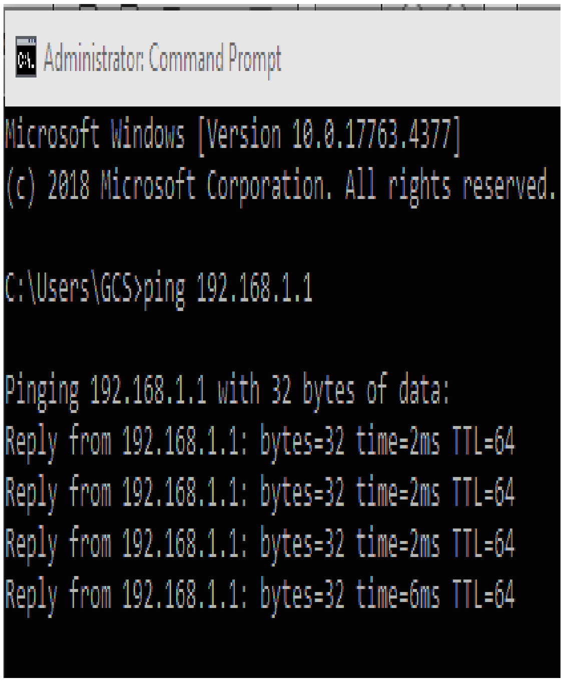
III. WIRESHARK INFORMATION

Wireshark comprises advanced functionalities that enable users to identify potential network intrusions [9] and suspicious behaviors. Presented below is an inventory of sophisticated functionalities of Wireshark.

Wireshark offers two distinct filter categories: capture filters and display filters. It is not possible to modify a capture filter. Display filters are employed based on specific criteria for the purpose of presenting packets in Wireshark. Display filters allow users to selectively view packets of interest while temporarily concealing those that are uninteresting. The I/O graph is a feature of Wireshark that provides a summary of packet flow. The I/O Graphs feature of Wireshark presents a visual representation of the aggregate network traffic contained within the captured data, typically quantified in terms of bytes or packets per second. There are colors defined for background of packets indicating suspicious packets in red color.

IV. RESULTS AND DISCUSSION

In order to attain the intended objective of the system, Wireshark and Snort are utilized for the creation of an intrusion detection system. According to [10], Snort is presently the most extensively utilized open source IDS system, and it is compatible with Windows operating systems. The aforementioned task is accomplished through the observation of inbound network traffic, which is commonly transmitted via LANs and Wi-Fi that links the server to the network hub. The traffic is cross-referenced with a repository of established signatures and irregularities associated with attacks, and notifications are generated upon identification of a breach. The utilization of signatures is prevalent in contemporary cybersecurity practices, as they are designed to counteract emerging forms of hacking and keep pace with updates to exploit databases. The Network Intrusion Detection System (NIDS) [11] is a system designed for monitoring network intrusions. The process of intrusion detection is executed utilizing analogous methodologies to those employed in signature pattern matching and anomaly detection. The technique of error detection involves the monitoring of regular network operations to identify any atypical network behaviors, such as abrupt spikes in the volume of network traffic (measured in IP packets per second). The technique of signature pattern comparison involves the comparison of network data with pre-existing attack techniques stored in a database.



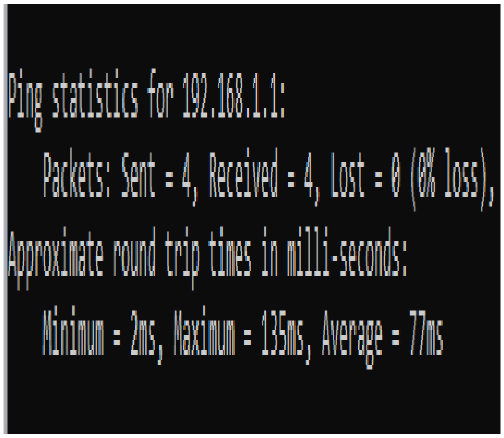
```
Microsoft Windows [Version 10.0.17763.4377]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\GCS>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
```

Fig. 1. Server is being tested for intrusion detection

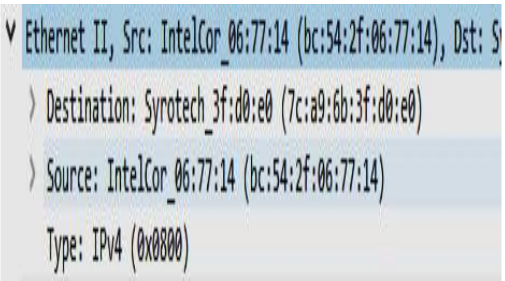
The testing of server for processing is shown in figure1.



```
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 135ms, Average = 77ms
```

Fig. 2. No loss of packets at 192.168.1.1 address

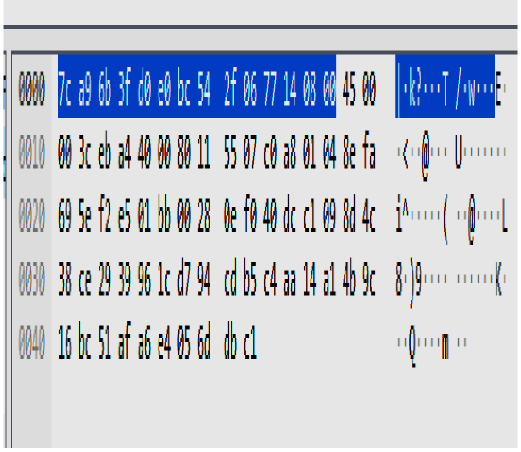
Figure2 shows the sending and receiving of packets for intrusion detection systems. It means no loss of packets is seen at IP address 192.168.1.1



```
∨ Ethernet II, Src: IntelCor_06:77:14 (bc:54:2f:06:77:14), Dst: S
  〉 Destination: Syrotech_3f:d0:e0 (7c:a9:6b:3f:d0:e0)
  〉 Source: IntelCor_06:77:14 (bc:54:2f:06:77:14)
    Type: IPv4 (0x0800)
```

Fig. 3. Information sent on the network

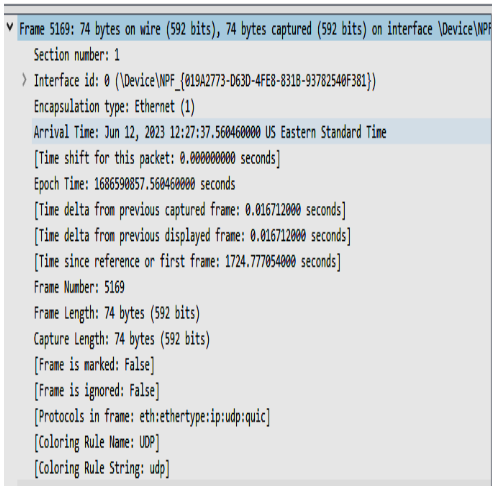
Figure 3 shows the type of information that is being sent on network. It comprises type of protocol used, destination address and source address.



```
0000  7c a9 6b 3f d0 e0 bc 54  2f 06 77 14 08 00 45 00   |·k?···T /·w···E·
0010  00 3c eb a4 40 00 80 11  55 07 c0 a8 01 04 8e fa   ·<··@··· U·······
0020  69 5e f2 e5 01 bb 00 28  0e f0 40 dc c1 09 8d 4c   i^·····(  ··@···L
0030  38 ce 29 39 96 1c d7 94  cd b5 c4 aa 14 a1 4b 9c   8·)9····  ······K·
0040  16 bc 51 af a6 e4 05 6d  db c1                     ··Q····m ··
```

Fig. 4. Information received on the network

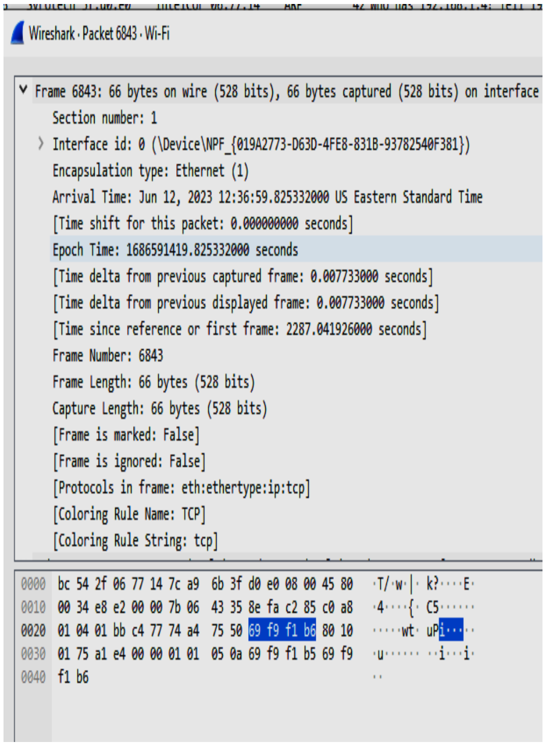
Figure4 shows packets and their codes in networking language.



```
∨ Frame 5169: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF
    Section number: 1
  〉 Interface id: 0 (\Device\NPF_{019A2773-D63D-4FE8-831B-93782540F381})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 12, 2023 12:27:37.560460000 US Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1686590857.560460000 seconds
    [Time delta from previous captured frame: 0.016712000 seconds]
    [Time delta from previous displayed frame: 0.016712000 seconds]
    [Time since reference or first frame: 1724.777054000 seconds]
    Frame Number: 5169
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:quic]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

Fig. 5. Intrusion information over LAN

Figure 5 shows brief information over network such as section number, interface id, encapsulation type used, arrival time, epoch time, frame length, capture length and time framework for packets.



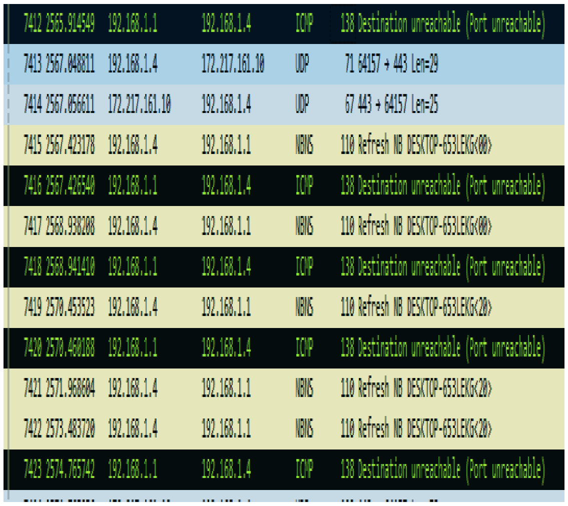
Wireshark · Packet 6843 · Wi-Fi

```
∨ Frame 6843: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
    Section number: 1
  〉 Interface id: 0 (\Device\NPF_{019A2773-D63D-4FE8-831B-93782540F381})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 12, 2023 12:36:59.825332000 US Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1686591419.825332000 seconds
    [Time delta from previous captured frame: 0.007733000 seconds]
    [Time delta from previous displayed frame: 0.007733000 seconds]
    [Time since reference or first frame: 2287.041926000 seconds]
    Frame Number: 6843
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]

0000  bc 54 2f 06 77 14 7c a9  6b 3f d0 e0 08 00 45 80   ·T/·w·|· k?····E·
0010  00 34 e8 e2 00 00 7b 06  43 35 8e fa c2 85 c0 a8   ·4····{· C5······
0020  01 04 01 bb c4 77 74 a4  75 50 69 f9 f1 b6 80 10   ·····wt· uPi·····
0030  01 75 a1 e4 00 00 01 01  05 0a 69 f9 f1 b5 69 f9   ·u······ ··i···i·
0040  f1 b6                                              ··
```

Fig. 6. System captures packets and informs user about suspicious packets

In figure6, the packets are captured live by the system and the user is informed about suspicious or malicious packets while capturing of packets through router over LAN.

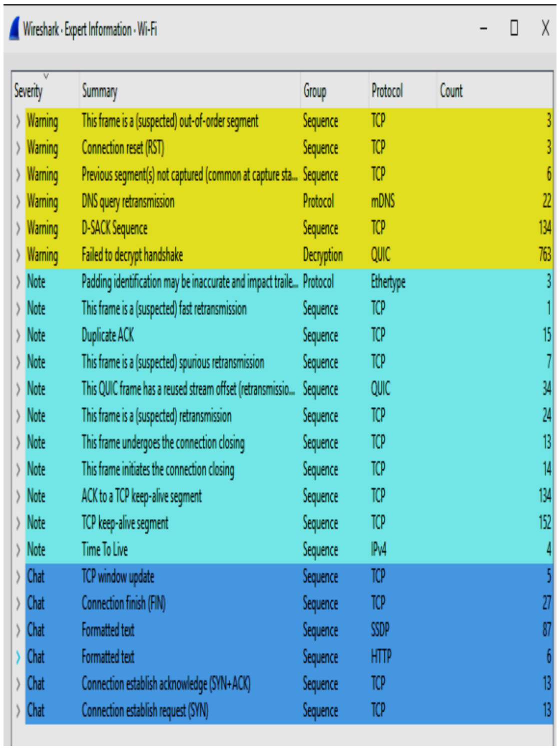


```
7412 2565.914549  192.168.1.1    192.168.1.4    ICMP  138 Destination unreachable (Port unreachable)
7413 2567.048811  192.168.1.4    172.217.161.10 UDP    71 64157 → 443 Len=29
7414 2567.056611  172.217.161.10 192.168.1.4    UDP    67 443 → 64157 Len=25
7415 2567.423178  192.168.1.4    192.168.1.1    NBNS  110 Refresh NB DESKTOP-653LEKG<00>
7416 2567.426540  192.168.1.1    192.168.1.4    ICMP  138 Destination unreachable (Port unreachable)
7417 2568.938208  192.168.1.4    192.168.1.1    NBNS  110 Refresh NB DESKTOP-653LEKG<00>
7418 2568.941410  192.168.1.1    192.168.1.4    ICMP  138 Destination unreachable (Port unreachable)
7419 2570.453523  192.168.1.4    192.168.1.1    NBNS  110 Refresh NB DESKTOP-653LEKG<20>
7420 2570.460188  192.168.1.1    192.168.1.4    ICMP  138 Destination unreachable (Port unreachable)
7421 2571.968604  192.168.1.4    192.168.1.1    NBNS  110 Refresh NB DESKTOP-653LEKG<20>
7422 2573.483720  192.168.1.4    192.168.1.1    NBNS  110 Refresh NB DESKTOP-653LEKG<20>
7423 2574.765742  192.168.1.1    192.168.1.4    ICMP  138 Destination unreachable (Port unreachable)
```

Fig. 7. Suspicious packets as identified during intrusion

The highlighted packets shown in figure 7 depict malicious or suspicious packets where intruders try to access the system.

Copyright © IEEE–2023 ISBN: 979-8-3503-6996-0



Severity	Summary	Group	Protocol	Count
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	3
Warning	Connection reset (RST)	Sequence	TCP	3
Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	6
Warning	DNS query retransmission	Protocol	mDNS	22
Warning	D-SACK Sequence	Sequence	TCP	134
Warning	Failed to decrypt handshake	Decryption	QUIC	763
Note	Padding identification may be inaccurate and impact traile...	Protocol	Ethertype	3
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	1
Note	Duplicate ACK	Sequence	TCP	15
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	7
Note	This QUIC frame has a reused stream offset (retransmissio...	Sequence	QUIC	34
Note	This frame is a (suspected) retransmission	Sequence	TCP	24
Note	This frame undergoes the connection closing	Sequence	TCP	13
Note	This frame initiates the connection closing	Sequence	TCP	14
Note	ACK to a TCP keep-alive segment	Sequence	TCP	134
Note	TCP keep-alive segment	Sequence	TCP	152
Note	Time To Live	Sequence	IPv4	4
Chat	TCP window update	Sequence	TCP	5
Chat	Connection finish (FIN)	Sequence	TCP	27
Chat	Formatted text	Sequence	SSDP	87
Chat	Formatted text	Sequence	HTTP	6
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	13
Chat	Connection establish request (SYN)	Sequence	TCP	13

Fig. 8. Expert analysis by intrusion detection system showing warning for the suspicious packets

Figure 8 shown above uses expert analysis algorithm to predict warning messages regarding suspicious packets in the network.

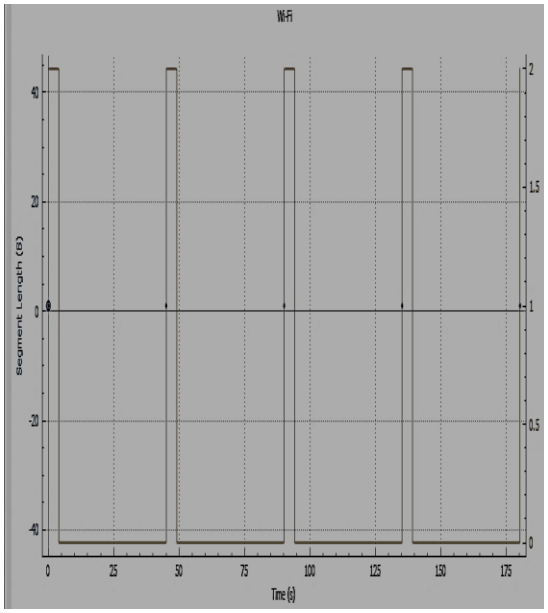


Fig. 9. Segment length vs. Time graph for 192.168.1.1

In figure 9, a graph is shown depicting segment length of packets in y-axis over a particular time in x-axis. It is done for network with address 192.168.1.1

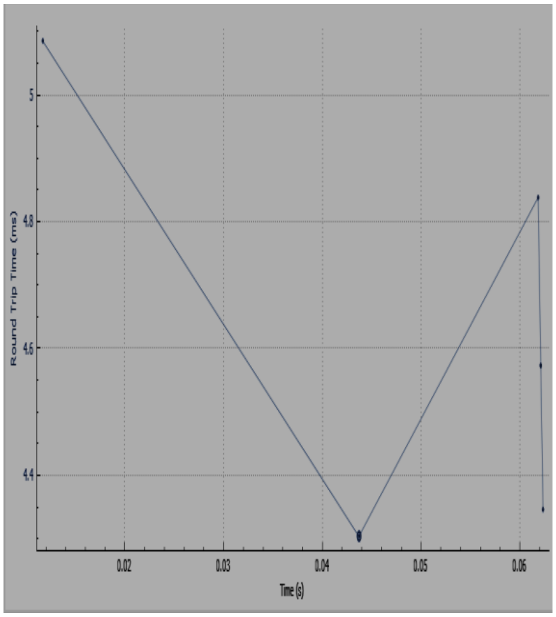


Fig. 10. Round trip time in response to figure 6

In figure10, calculation of round trip time over time intervals is depicted for packets captured in figure6 by the network.

V. CONCLUSION & FUTURE WORK

A very important tool is Wireshark, which offers a wide range of sophisticated capabilities including display filters, I/O graphs, color coding, and expert information. The features stated above may be effectively used to identify different kinds of network intrusions on computer systems. Through the use of the packet analyser program Wireshark [12, 13] , the study developed a novel framework for collecting data packets in real-time and detecting potentially harmful behaviors or packets. With the present approach, real data packets from the network were captured using Wireshark and manually mapped to the attack pattern dictionary. [14-18]

The model is used to identify different types of network intrusions. The findings of the current inquiry imply that Wireshark has a wide range of capabilities, functioning not only as a tool for packet analysis and problem-solving but also as an effective method for spotting unwanted access attempts. Using Wireshark, a person with knowledge of data packets, protocols, and related topics may find illegal access.

REFERENCES

[1] Amrita A. and Brajesh P, An overview on intrusion detection system and types of attacks it can detect considering different protocols. International Journal of Advanced Research in Computer Science and Software Engineering, 2(8), 94-98, 2012

[2] Asmaa S. A. and Sharad G, Intrusion detection system (IDS) & intrusion prevention system (IPS): case study. International Journal of Scientific & Engineering Research, Vol.2, Issue 7, pp.1-3, 2011

[3] Dheerendra K. P. and Raj K. P, A review on variety of intrusion detection system and their functional approaches. International Journal of Engineering Sciences & Management. Patel & Paul, 6(3), 2016

[4] Faizal, M.A., MohdZaki M., Shahrin S., Robiah, Y., Siti R., S., and Asrul H., Y, Time based intrusion detection on fast attack for network intrusion detection system [Conference Session]. Second International Conference on Network Applications, Protocols and Services, (IEEE), Malaysia, 2010 http://doi.org/10.1109/NETAPPS.2010.33

[5] Jaydip S, An agent-based intrusion detection system for local area networks. International Journal of Communication Networks and Information Security, 2(2), 128-140, 2010

[6] Karl L, Intrusion detection: Current capabilities and future direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2002

[7] Ramesh, T. R., Lilhore, U. K., Poongodi, M., Simaiya, S., Kaur, A., & Hamdi, M. (2022). PREDICTIVE ANALYSIS OF HEART DISEASES WITH MACHINE LEARNING APPROACHES. Malaysian Journal of Computer Science, 132-148.

[8] Poongodi, M., Malviya, M., Hamdi, M., Vijayakumar, V., Mohammed, M. A., Rauf, H. T., & Al-Dhlan, K. A. (2022). 5G based Blockchain network for authentic and ethical keyword search engine. IET Commun., 16(5), 442-448.

[9] Poongodi, M., Malviya, M., Kumar, C., Hamdi, M., Vijayakumar, V., Nebhen, J., &Alyamani, H. (2022). New York City taxi trip duration prediction using MLP and XGBoost. International Journal of System Assurance Engineering and Management, 13(1), 16-27.

[10] "Poongodi, M., Hamdi, M., & Wang, H. (2022). Image and audio caps: automated captioning of background sounds and images using deep learning. Multimedia Systems, 1-9.

[11] Poongodi, M., Hamdi, M., Gao, J., & Rauf, H. T. (2021, December). A Novel Security Mechanism of 6G for IMD using Authentication and Key Agreement Scheme. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[12] Mohammad S. H. Abdul M. and Abu N. B, An implementation of intrusion detection system using genetic algorithm. International Journal of Network Security & Its Applications, 4(2), 109-120. 2012, http://doi.org/10.5121/ijnsa.2012.4208

[13] Nureni A. A., Taiwo M. B., Sanjay M., Adewole A., Charles V. V. and Ravin A, Intrusion detection and prevention systems: an updated review. Data Management, Analytics and Innovation, 685-696.2020, http://doi.org/10.1007/978-981-32-99498_48

[14] Parati N. and Potteti S, Intelligent intrusion detection system using SVM and Genetic Algorithm (SVM-GA). International Journal of Science and Applied Information Technology, 4(2), 1–5, 2015

[15] Santos B. K., Chandra T. S., Raju P., Ratnakar M., Dawood B. Sk. and Sudhakar N, Intrusion detection system – types and prevention. International Journal of Computer Science and Information Technologies, 4(1), 77–82, 2013

[16] A. Siddiqui, O. Olufunmilayo, H. Gohel and B. Pandey, "Digital Healthcare System Vulnerability Analysis using Network Forensic Tool,"10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 2021, pp. 881-885, doi: 10.1109/CSNT51715.2021.9509647.

[17] M. Kassim, A. R. Mahmud, M. Amirullah Ramli and R. A. Rahman, "Network Analysis of Students' Online Activities via Port mirroring Switch Port Analyzer," IEEE 12th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 2022, pp. 49-54, doi: 10.1109/ISCAIE54458.2022.9794504.

[18] M. T. Naing, T. T. Khaing and A. H. Maw, "Evaluation of TCP and UDP Traffic over Software-Defined Networking," International Conference on Advanced Information Technologies (ICAIT), Yangon, Myanmar, 2019, pp. 7-12, doi: 10.1109/AITC.2019.8921086.

Copyright © IEEE–2023 ISBN: 979-8-3503-6996-0