WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Network Traffic Analysis Using Wireshark

***Dr. B. Kalaiselvi[1], Aruna. K[2]***

[1] ASP/Computer Science and Engineering, Kalaiselvib@mahendra.info, kalairs2003@gmail.com
[2]Final Year / Cyber Security, Mahendra Engineering College, Namakkal, Email: arunakumar2326@gmail.com
DOI: https://doi.org/10.55248/gengpi.4.1223.123506

**ABSTRACT**

Network traffic analysis plays a pivotal role in securing and optimizing modern computer networks. This research leverages Wireshark, a widely-used network protocol analyzer, to delve into the intricate details of data exchanges within a network. This paper focuses on real-time packet-level analysis, dissecting communication patterns, and identifying potential vulnerabilities. Employing a comprehensive methodology, the research aims to unveil insights into network behavior, detect anomalies, and enhance overall network performance. The project employs Wireshark's robust capabilities to capture and analyze data packets, providing a granular understanding of network protocols, traffic types, and communication flows. Through statistical and visual representations, the paper seeks to reveal patterns, anomalies, and potential security threats. By combining protocol analysis with statistical metrics, the research aims to contribute valuable insights for network administrators and cybersecurity professionals, aiding in the proactive identification and mitigation of network issues. Ultimately, this research endeavors to enhance the overall reliability, security, and efficiency of computer networks through the utilization of Wireshark as a powerful tool for network traffic analysis.

**Keywords:** Network traffic analysis, Network protocols, Potential Vulnerability, Wireshark.

## 1. Introduction

In today's interconnected world, the integrity and security of network communications are paramount. Network administrators, security professionals, and researchers rely on robust tools and methodologies to monitor, analyze, and safeguard their network infrastructures. Among these tools, Wireshark stands as a prominent and indispensable choice for network traffic analysis. This paper provides a comprehensive introduction to the practice of network traffic analysis using Wireshark

**Objective:**

The objective of network traffic analysis using Wireshark is to gain insights into the communication patterns and behaviors within a computer network. By capturing and examining the data packets traversing the network, this analysis aims to identify potential security threats, troubleshoot network issues, and optimize overall performance. Wireshark, a powerful open-source packet analyzer, allows for the granular inspection of network traffic, enabling professionals to understand the flow of data, pinpoint anomalies, and enhance the overall integrity and efficiency of the network.

**Overview:**

Network traffic analysis involves the examination of data packets exchanged between devices in a network. Wireshark facilitates this process by capturing and displaying these packets in a comprehensible manner. The tool enables users to dissect the content of each packet, revealing valuable information such as source and destination addresses, protocols used, and the timing of data transfers. Through real-time monitoring or retrospective analysis, Wireshark assists in the identification of abnormal network behavior, potential security breaches, and performance bottlenecks. This comprehensive insight into network communications empowers administrators and security professionals to make informed decisions for the optimization and safeguarding of their network infrastructure.

## 2. Literature Review

Bindu Dodiya. *et al.* [1] developed a method with the utilization of Wireshark, an efficient open-source packet analysis tool, for tracing and categorizing various attack signatures in network forensics. Wireshark's ability to capture live data at a microscopic level allowed administrators to identify malicious online behavior, detect data breaches, and reveal indicators of compromise for malware. The advantage lay in Wireshark's comprehensive analysis, providing a detailed understanding of network packets and enabling proactive measures to enhance cybersecurity. However, despite its effectiveness in uncovering a wide range of security threats, Wireshark had limitations as it lacked intrusion detection capabilities. Unlike dedicated systems, Wireshark

did not offer real-time warnings or actively prevent unauthorized activities, underscoring the importance of implementing complementary security measures for proactive threat detection and response.

Giovanni Barbieri. *et al.* [2] implemented a comparative analysis method, contrasting Shodan-only assessments with large-scale traffic analysis at an Internet Exchange Point (IXP) via sFlow sampling. This approach, utilizing sFlow sampling, allowed the identification of Industrial Control Systems (ICS) endpoints engaged in genuine industrial traffic, overcoming Shodan's limitations. The methodology not only detected scanning activities but also differentiated between industrial and IT traffic, providing a more comprehensive understanding of insecure industrial protocol usage. Despite its advantage, the study's limitation was the reliance on a 31-day sampled traffic capture, potentially missing transient industrial traffic patterns. Furthermore, while effective in identifying legitimate industrial traffic, the proposed analytic framework might not address real-time threats or evolving cyber threats adequately, potentially limiting its immediate threat detection capabilities.

+Muhammad Farrid Affiq Harirul Kamal. *et al.* [3] developed a dynamic Android botnet detection method using network analysis, offering real-time insights into application behavior. Extracting five features from Wireshark and SSL Packet Capture, the approach demonstrated promising accuracy, ROC value, and low FP value when tested with the Artificial Neural Network (ANN) algorithm. However, the study's limitation was its reliance on datasets from APKPure, Github, and Koodous, potentially limiting the representation of diverse Android applications and botnet behaviors. Despite achieving positive results, the proposed network traffic features may have had constraints in capturing nuanced variations in Android botnet characteristics, suggesting the need for further refinement and exploration in subsequent research.

Sujith Bebortta. *et al.* [4] implemented a method addressing the challenge of network traffic administration for diverse IoT devices. The focus was on efficiently characterizing inter-arrival rates through packet-level and flow-level analysis, facilitating the crucial identification and management of IoT devices for stable network activities and enhanced cybersecurity. The approach provided a precise understanding of network flows and insights into the strengths, weaknesses, and future scopes of state-of-the-art technologies for managing the expanding IoT landscape. However, a limitation emerged in the absence of specific details on proactive measures for identifying and isolating network vulnerabilities, warranting further exploration in subsequent research.

Ali Siddiqui. *et al.* [5] developed a method utilizing Wireshark as a network protocol analyzer for forensic analysis on network security attacks. Wireshark facilitated ethical hackers in collecting and analyzing data to uncover evidence of network intrusions, exposing vulnerabilities in cyber security at the user level. The advantage of Wireshark's functionality as a sniffing network tool allowed live capture and breakdown of network transmissions and various packets. This facilitated a detailed analysis of protocols like HTTP, TCP, and UDP, enhancing the understanding of network activity and identification of website vulnerabilities. However, a limitation in this work was the focus on classifying websites as secure or vulnerable solely based on Wireshark's packet sniffing, potentially oversimplifying the evaluation of website security.

## 3. Proposed Method

In this, proposed method for network traffic analysis using Wireshark encompasses a systematic and comprehensive approach to extract meaningful insights from network packets. Utilize Wireshark’s packet capturing capabilities to collect network traffic data at strategic points within the network, such as routers or switches. Ensure adequate packet sampling for accuracy.

### *3.1 Data Filtering:*

Employ Wireshark's advanced filtering options to eliminate noise and isolate packets of interest. Filters may include IP addresses, port numbers, or specific protocols, depending on the analysis goals.

### *3.2 Packet Decoding:*

Leverage Wireshark's deep packet inspection capabilities to decode packets and extract protocol-specific information. This step helps in understanding the nature of the traffic, such as HTTP requests or DNS queries.

### *3.3 Flow Analysis:*

Group packets into flows or connections, considering source-destination pairs and their respective protocols. This aids in tracking communication patterns and identifying abnormal behavior.

### *3.4 Statistical Profiling:*

Calculate various statistical metrics, including packet counts, packet size distributions, and traffic patterns over time. Wireshark provides tools for statistical analysis and graph generation.

### *3.4 Protocol Analysis:*

Perform protocol-specific analysis, such as identifying protocol-specific anomalies or detecting irregularities in protocol handshake processes (e.g., TCP SYN-ACK).

### *3.5 Behavioral Analysis:*

Employ heuristic or machine learning-based methods to identify abnormal network behavior. Train models on historical data to detect deviations from expected traffic patterns.

### *3.6 Security Signature Matching:*

Utilize Wireshark's signature-based detection features to identify known attack patterns or malware signatures within the captured traffic. Implement an alerting system that triggers notifications for detected anomalies or potential security threats. Wireshark can be integrated with alerting mechanisms to automate this process. Create visual representations of network traffic patterns, including time-series graphs, heatmaps, and network topology diagrams, using Wireshark's visualization capabilities.

### *3.7 Forensic Analysis:*

For security incidents, utilize Wireshark's ability to save packet capture files for later forensic analysis. This step is crucial for post-incident investigations.

### *3.8 Reporting:*

Generate detailed reports summarizing the findings, including observed anomalies, security threats, and recommendations for network optimization and security enhancement. Implement continuous network traffic monitoring using Wireshark or compatible tools to ensure ongoing network security and performance.

This comprehensive method harnesses Wireshark's rich feature set and analytical capabilities to provide network administrators and security professionals with a powerful toolset for enhancing network visibility, security, and performance. It enables proactive threat detection, rapid incident response, and data-driven decision-making in the dynamic landscape of network management and cybersecurity**.**

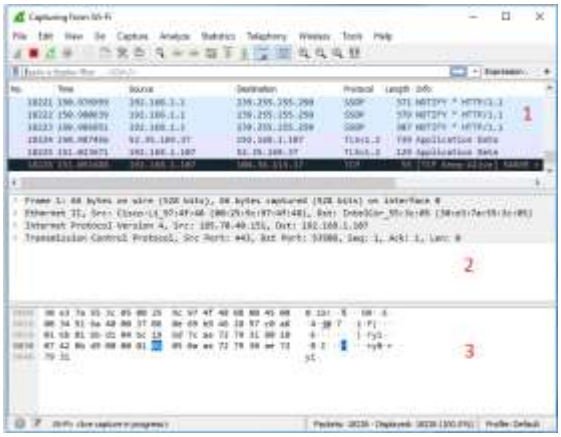
## 4. Discussion

In this section, it delve into the implications and significance of this network traffic analysis using Wireshark. This paper address the effectiveness of Wireshark in enhancing network security through anomaly detection and its role in network troubleshooting and optimization. This approach also discuss the potential challenges, such as privacy concerns and the need for continuous monitoring. Additionally, explore future directions, including the integration of advanced machine learning techniques and the development of custom Wireshark plugins to further enhance its capabilities. Overall, the findings underscore the crucial role of Wireshark as a versatile tool in the arsenal of network professionals, enabling proactive network management and cybersecurity.

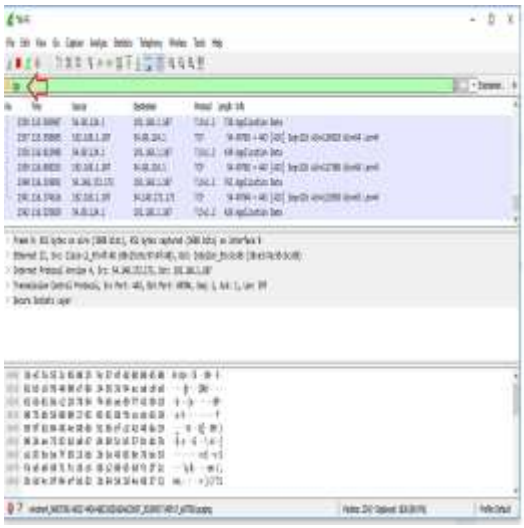
## 5. Result

Capture the packets of windows

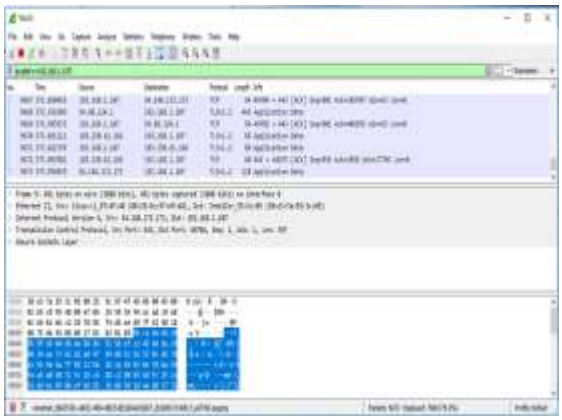
Analysis the window



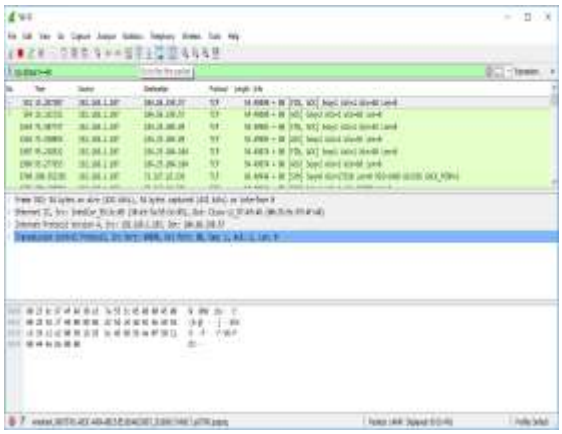
Creating filters



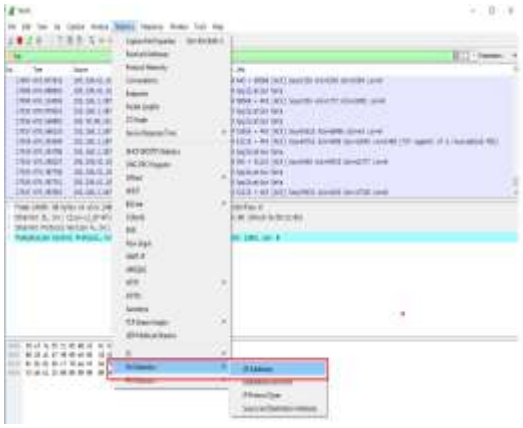
Data filtering



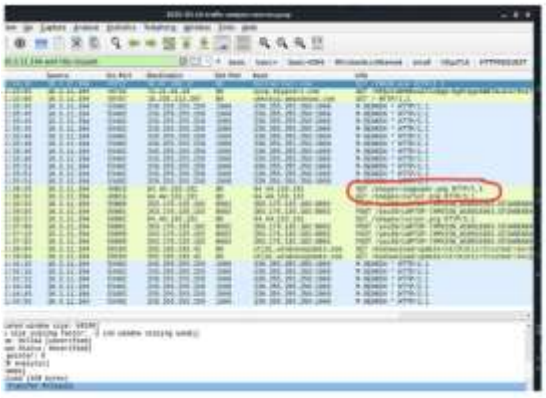
To identify the protocol-specific anomalies or detecting irregularities in protocol handshake processes (eg. TCP)



Statistic profiling



Forensic Analysis and reporting



## 6. Limitation & Future work

In this paper, there is a certain limitations, including the inability to capture encrypted traffic, potential performance overhead during continuous monitoring, and the need for skilled personnel for in-depth analysis. Future research can focus on addressing these limitations by exploring techniques for analyzing encrypted traffic, optimizing Wireshark's resource usage, and developing user-friendly interfaces for less experienced users. Additionally, the integration of artificial intelligence and machine learning algorithms for more advanced threat detection and network optimization is an exciting avenue for future work. Furthermore, expanding the scope of analysis to emerging technologies like 5G networks and IoT devices presents intriguing research opportunities.

## 7. Conclusion

In conclusion, this approach highlights the invaluable role of Wireshark in network traffic analysis, offering insights into network security, troubleshooting, and performance optimization. While Wireshark proves to be a versatile and powerful tool, it is not without its challenges, such as the

limitations in analyzing encrypted traffic. However, with continuous development and integration of advanced technologies, the future of network traffic analysis using Wireshark holds promise. Network professionals and security experts can leverage Wireshark's capabilities to proactively manage and secure their networks in an ever-evolving digital landscape. As the move forward, the need for skilled analysts and innovative solutions will remain paramount in ensuring the integrity and resilience of network infrastructures.

**References**

[1]. Dodiya, B. and Singh, U.K., 2022. Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise. Int J Comput Appl, 183(53), pp.1-6.

[2]. Barbieri, G., Conti, M., Tippenhauer, N.O. and Turrin, F., 2021, July. Assessing the use of insecure ics protocols via ixp network traffic analysis. In 2021 International Conference on Computer Communications and Networks (ICCCN) (pp. 1-9). IEEE.

[3]. Kamal, M.F.A.H., Hamid, I.R.A., Abdullah, N., Abdullah, Z., Ahmad, M. and Shah, W.M., 2022, May. Android botnet detection based on network analysis using machine learning algorithm. In international conference on soft computing and data mining (pp. 282-291). Cham: Springer International Publishing.

[4]. Bebortta, S. and Senapati, D., 2021. Empirical characterization of network traffic for reliable communication in IoT devices. Security in cyber-physical systems: foundations and applications, pp.67-90.

[5]. Siddiqui, A., Olufunmilayo, O., Gohel, H. and Pandey, B., 2021, June. Digital Healthcare System Vulnerability Analysis using Network Forensic Tool. In 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT) (pp. 881-885). IEEE.

**Books:**

[6]. Learn Wireshark – A definitive guide to expertly analyzing protocols and troubleshooting networks using wireshark, 2nd Edition.

[7]. Wireshark Certified Network Analyst Certification – WCNA getting certified on the world's popular Network Analyzer Tool.

[8]. Wireshark 101 – Essential Skills for Network Analysis (Second Edition): Wireshark Solution Series.

**Links:**

[9]. https://www.wireshark.org/

[10]. https://www.google.com/search?q=network+traffic+analysis+using+wireshark&oq=network+traffic+analysis+using&gs_lcrp