LEVERAGING WIRESHARK FOR THE DETECTION AND COLLECTION OF INDICATORS OF COMPROMISE IN MALICIOUS NETWORK TRAFFIC

[1]*Gaylord Ogbonna Asoronye, [2]Emmanuel Okekenwa, & [3]Alexander Anthony Anunwa

[1]Department of Computer Engineering
[2&3]Electrical Electronic Engineering Department
Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State.
Corresponding email: *asorgay@gmail.com
Corresponding phone contact: *+2348069145552

Abstract

Maintaining constant vigilance against malicious traffic is essential for ensuring network security. Indicators of Compromise (IOCs) play a crucial role in identifying such activities. This study examines the effectiveness of Wireshark, a free and widely-used network packet capture and analysis tool, in collecting these IOCs. The importance of network security and the role of IOCs in threat detection, a brief introduction to Wireshark, detailed capabilities and usage in network traffic inspection are discussed by researchers. Various types of IOCs relevant to network traffic analysis, including IP addresses, network ports, URLs, and file hashes are identified. There is a description of how Wireshark can be used to extract each type of IOC by analysing communication patterns, suspicious connections, domain names, and captured packet content. The research concludes by highlighting benefits and limitations of using Wireshark for IOC collection. These include cost-effectiveness, deep packet inspection, and customisable filters. Conversely, the need for proficiency, time-consuming nature of analysis, and the potential for false positives are acknowledged. Indeed, this study validates the value of Wireshark as a powerful tool for network security professionals, capable of facilitating the collection of critical IOCs for early detection and response to malicious activities.

Keywords: Security, Network, IOCs, Wireshark, Forensics

1.0 Introduction

An era of unprecedented connectivity has ushered in the digital age, but with it comes a growing concern: network security (Al-Naqeeb & Choi, 2022). As organisations increasingly rely on interconnected systems, they become vulnerable to a vast array of cyber threats. These threats, ranging from malware infections to sophisticated cyberattacks, can cripple operations, steal sensitive data, and cause significant financial losses (Sharma et al., 2023). Therefore, effective threat detection mechanisms are paramount for maintaining a secure network environment.

One crucial approach involves identifying Indicators of Compromise (IOCs) (Al-Rubaie & Atiquzzaman, 2020). IOCs are observable signs that a system or network may have been compromised by malicious activity. These indicators can manifest in various forms, such as suspicious network traffic patterns, unauthorised access attempts, or the presence of known malware signatures. By actively monitoring for and analysing IOCs, security professionals can gain valuable insights into potential threats. This allows for early detection and swift response, minimising the damage caused by cyberattacks. Fortunately, a range of tools exist to assist in the identification and analysis of IOCs (Jiang et al., 2020). Among these, Wireshark stands out as a powerful and freely available network packet capture and analysis tool (Yoo et al., 2021).

Network security relies heavily on the ability to understand and analyze the flow of data across a network. This process, known as Network Traffic Analysis (NTA), plays a vital role in identifying suspicious activity and potential threats (Sharma et al., 2023). NTA involves capturing and examining network packets, which are the individual units of data transmitted between devices on a network. One common technique used for NTA is packet sniffing. Packet sniffers are software programs that operate in promiscuous mode, allowing them to capture all network traffic on a specific segment, regardless of its intended recipient (Yoo et al., 2021). This comprehensive capture capability makes packet sniffing a powerful tool for network administrators and security professionals (Garcia-Fernandez., 2020). Wireshark stands out as a widely-used and free packet sniffer (Yoo et al., 2021).

It offers a robust suite of features for capturing, inspecting, and analysing network traffic. Wireshark can decode packets based on various network protocols, allowing users to delve into the details of communication flows. Additionally, it provides powerful filtering and search capabilities, enabling

security professionals to identify specific patterns or anomalies within captured traffic. Network protocols are the foundation of communication on a network. They define the rules and formats for data exchange between devices. Common protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), and DNS (Domain Name System) (Sharma et al., 2023). Understanding these protocols is crucial for interpreting captured network traffic and identifying potential IOCs. For example, unusual communication patterns on ports typically used for secure connections (e.g., port 443 for HTTPS) could indicate a potential attempt to bypass security measures.

1.2 Identifying IOCs with Wireshark

Indicators of Compromise (IOCs) come in various forms, each offering valuable insights into potential malicious activity on a network. Wireshark's comprehensive traffic analysis capabilities make it a powerful tool for identifying these diverse IOCs (Al-Rubaie &Atiquzzaman, 2020). Let's explore how Wireshark can be leveraged to extract different types of network traffic-related IOCs.

1.3 Categorises of IOCs

IP addresses and ports: Deviations from expected network traffic patterns are key indicators of potential threats. Wireshark allows users to filter and analyse communication based on source and destination IP addresses and ports (Yoo et al., 2021). Examining connections to unusual or blacklisted IP addresses, or communication on ports not typically used by legitimate applications, can raise red flags. For instance, a sudden spike in traffic towards a known command-and-control server IP address could signal a malware infection attempting to communicate with its remote controller.

Uniform resource locators (URL's) and domain names: Malicious actors often utilise websites or domains for phishing attacks, malware distribution, or data exfiltration. Wireshark can capture URLs embedded within HTTP traffic packets, allowing security professionals to identify suspicious domain names or unauthorised website access attempts (Al-Naqeeb & Choi, 2022). By comparing captured URLs against known malicious domain lists, analysts can gain valuable insights into potential threats.

Protocols: Network communication relies on established protocols like TCP/IP for reliable data exchange. Wireshark enables users to decode captured traffic based on various protocols (Sharma et al., 2023). The presence of non-standard or unexpected protocols may indicate the use of custom

malware or communication channels designed to evade detection. While encrypted traffic analysis with Wireshark has limitations due to encryption methods, unusual protocol usage patterns can still provide valuable clues.

File hashes: Malware often carries unique identifiers in the form of file hashes. Wireshark can capture data payloads within packets, potentially containing malware signatures (Alsaadi et al., 2021). By comparing captured file hashes with known malware databases, security professionals can identify potential malware infections on a network. However, it's important to note that this approach may not be foolproof, as malware creators can employ techniques to obfuscate file hashes.

2.0 Materials and Methods.

Materials:

- Wireshark version 3.6.0
- Pcaps
- Virustotal.com

2.1 Methods

The methods used in collecting indicators of compromise with Wireshark are enumerated below:

2.2 Collecting indicators of compromise with wireshark

Monitoring for indicators of compromise enables organisations to better detect and respond to security compromises (Sharma et al., 2023). Collecting and correlating IOCs in real time means that organisations can more quickly identify security incidents that may have gone undetected by other tools and provides the necessary resources to perform forensic analysis of incidents. When a host is infected or otherwise compromised, security professionals need to quickly review packet captures (pcaps) of suspicious network traffic and these pcaps can be used to identify affected hosts and users. There are many sites that provide pcaps for analysis. The researchers have used pcaps from Traffic analysis exercise "Pizza Bender" to demonstrate how Wireshark is used to capture and analyse IOC's.

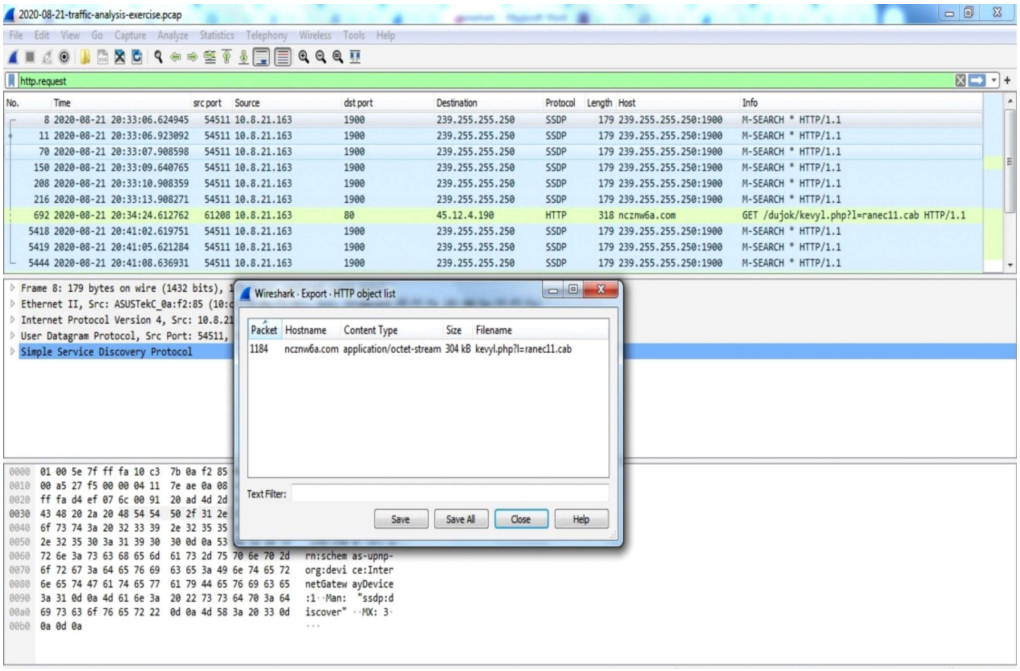

Figure 1: Infected file hash captured by Wireshark

First, the file hash of the infected file is captured as shown in figure 1 above then the result is scanned on virustotal.com as depicted in figure 2 below.

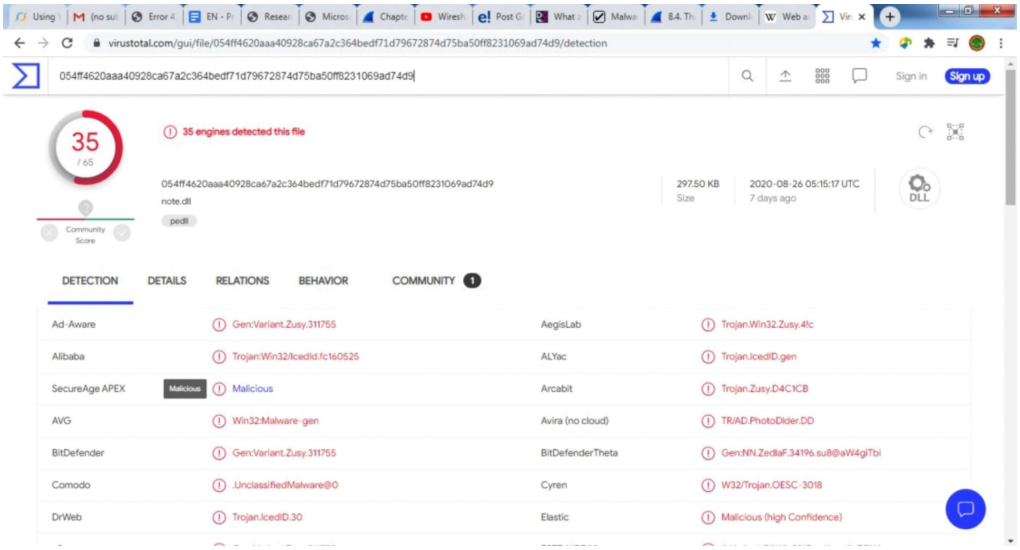

Figure 2: Result scanning on virustotal.com

Having detected that the file is compromised, the researchers proceeded to investigate the host name, domain address and Internet Protocol (IP) address of the infected host as clearly shown in figure 3, 4 and 5 respectively. Network traffic analysis at the packet level is very necessary, owing to the fact that it can identify many different threats and attacks that could remain unnoticed by antivirus software. In the past, packet analyzers were very expensive and patented. Wireshark has changed all that. Wireshark is one of the best open source packet analysers available today, and it displays packet data as detailed as possible.

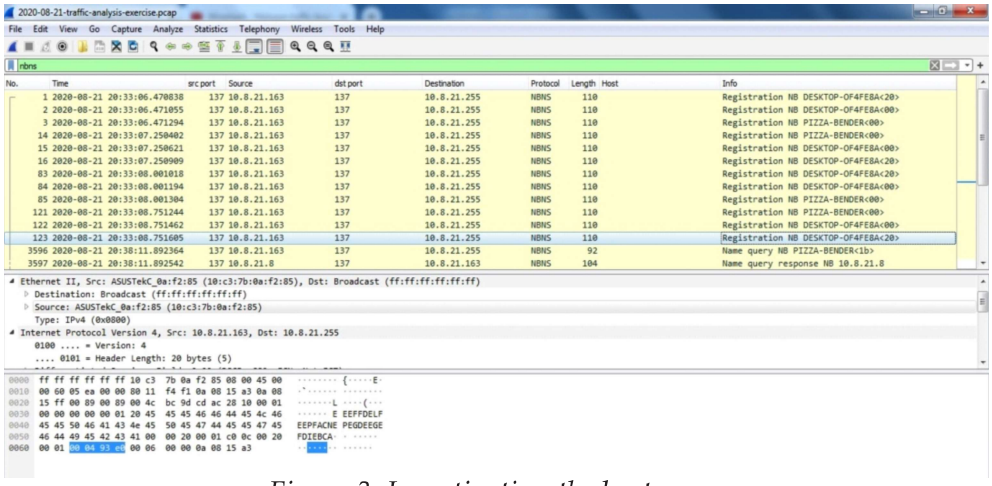

Figure 3: Investigating the host name

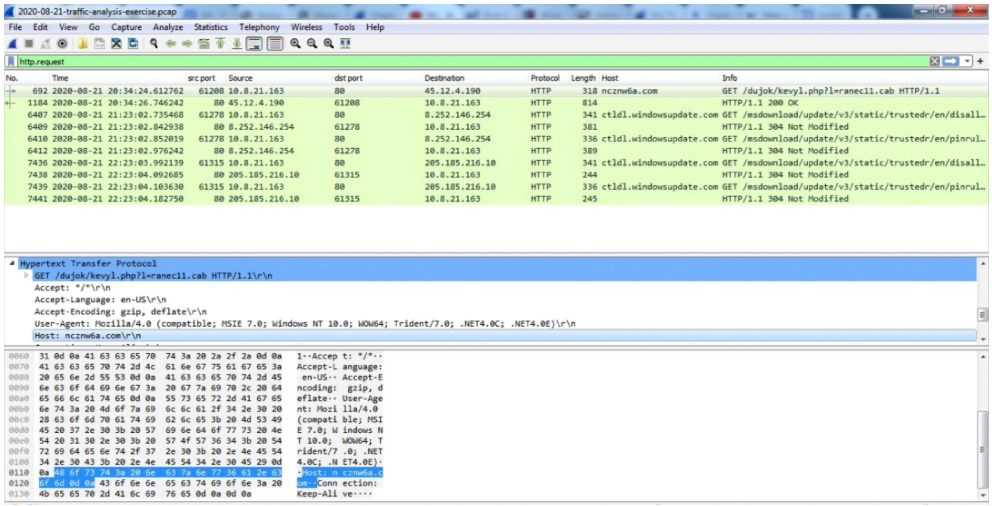

Figure 4: Investigating the Domain address

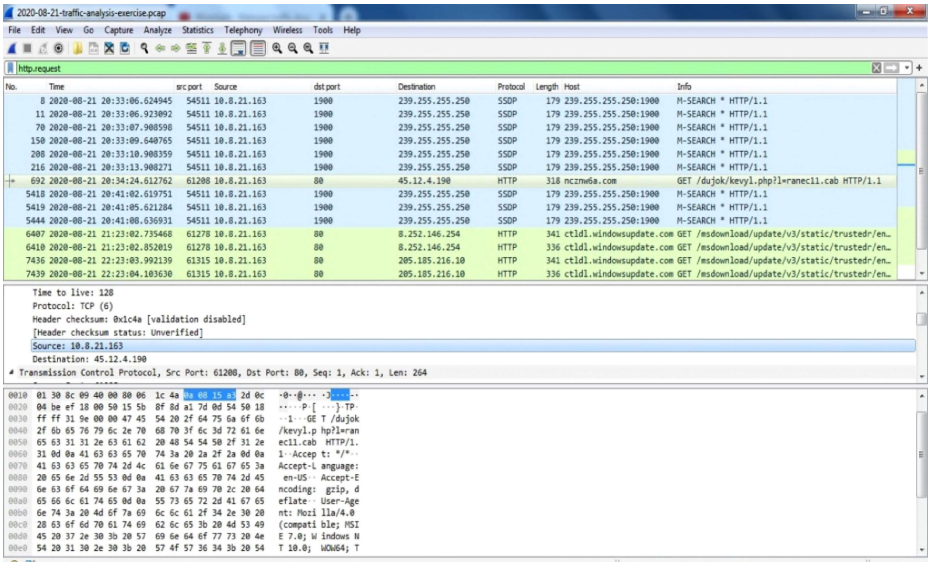

Figure 5: Investigating the IP address of the infected host

2.3 Benefits and Limitations of using Wireshark for IOC Collection

2.3.1 Benefits

- **Cost-effective:** Wireshark is a free and open-source tool, making it readily accessible to individuals and organisations of all sizes. This eliminates the need for expensive commercial network traffic analysis software.

- **Deep Inspection:** Wireshark provides deep inspection capabilities for network traffic. It can decode packets based on various protocols, allowing users to examine the details of communication flows. This granular level of analysis is crucial for identifying subtle anomalies and extracting meaningful IOCs.

- **Customisable Filters:** Wireshark offers a powerful filtering engine. This allows security professionals to tailor their analysis to specific needs. By filtering traffic based on pre-defined criteria (e.g., IP addresses, ports, protocols), analysts can quickly pinpoint suspicious activity and focus on relevant data for IOC extraction.

2.3.2 Limitations:

- **Need for Proficiency**: Effective use of Wireshark requires a strong understanding of network protocols, traffic analysis techniques, and network security concepts. This can be a barrier for users with limited technical expertise.
- **Time-Demanding Analysis:** Analysing captured network traffic with Wireshark can be a time-consuming process. Depending on the volume of traffic and the complexity of the investigation, it can take significant effort to identify and extract relevant IOCs.
- **Probability of False Positives:** While Wireshark offers valuable insights, it's important to acknowledge the potential for false positives. Unusual traffic patterns or communication with unknown entities may not always be malicious. Careful analysis and correlation with other threat intelligence sources are essential to avoid mistaking legitimate activity for a threat.

3.0 Conclusion

Early detection is paramount in the fight against cyberattacks. Indicators of Compromise (IOCs) serve as crucial early warnings, allowing security professionals to identify and respond to potential threats before significant damage occurs. By actively collecting and analysing IOCs, security teams gain valuable insights into suspicious activity on their networks. Wireshark emerges as a powerful and versatile tool for network security professionals. This free software excels at capturing and analysing network traffic in detail, making it ideal for identifying various network traffic-related IOCs. With its deep inspection capabilities, customisable filters, and cost-effectiveness, Wireshark empowers security teams to effectively investigate suspicious activity and extract relevant IOCs for a swift and targeted incident response. Looking ahead, automation and integration with security frameworks offer exciting possibilities for streamlining IOC collection and analysis, further enhancing Wireshark's value in the ever-evolving cyber threat landscape.

4.0 Recommendations

- Based on the findings of this research, it is strongly recommended that organisations adopt the following strategies to enhance their network security posture through effective IOC collection and analysis using Wireshark:
- **Prioritise IOC collection:** Given the critical role of IOCs in early threat detection, organisations should make IOC collection a top priority in their security strategies.
- **Invest in Wireshark:** Wireshark's capabilities and cost-effectiveness make it a valuable investment for network security teams. Organisations should consider deploying Wireshark on their networks to capture and analyse network traffic for IOCs.
- **Train staff:** Ensure that network security professionals are adequately trained in using Wireshark and interpreting IOCs. This will enable them to effectively leverage the tool's capabilities and maximise its benefits.
- **Integrate Wireshark with other security tools:** To streamline IOC collection and analysis, explore opportunities to integrate Wireshark with other security tools and frameworks. This can automate certain tasks and provide a more comprehensive view of network activity.
- **Stay updated on IOC types:** As cyber threats evolve, new IOC types may emerge. Network security professionals should stay informed about the latest IOC trends and ensure that their IOC collection and analysis processes are adapted accordingly.
- **Automation:** It is necessary to explore automation techniques to reduce the manual effort involved in IOC collection and analysis. This can help improve efficiency and reduce the risk of human error.

References

Al-Naqeeb, M., & Choi, Y. (2022). A comprehensive survey on network threat detection techniques. *IEEE International Conference on Information Networking (ICOIN)* (pp. 726-731).

Al-Rubaie, A., & Atiquzzaman, M. (2020). Indicators of compromise: A review of taxonomies and applications. *IEEE International Conference on Computational Intelligence for Security (ICCIS)* (pp. 1-9).

Alsaadi, T., Al-Janabi, S., Al-Saedi, A., & Anuar, N. B. (2021, December). A framework for network forensic analysis using deep learning for malware detection. *Sensors*, *21*(24), 8543.

Garcia-Fernandez, A., Garcia-Saiz, J., & Gil-Herrera, J. (2020). A comprehensive taxonomy of network intrusion detection systems. *ACM Computing Surveys (CSUR)*, *54*(2), 1-32.

https://www.malware-traffic-analysis.net/trainingexercises.html 2020-08-21-- Traffic analysis exercise - Pizza-Bender.

Jiang, Y., Ding, Z., Ma, J., & Li, L. (2020). A review of network traffic analysis techniques for detecting internet of things (IoT) botnets. *ACM Computing Surveys (CSUR)*, *53*(3), 1-37.

Sharma, R., Bhadoria, A., Deep, K., & Moon, S. I. (2023). A survey on network traffic analysis for cyber security. *Journal of Network and Computer Applications*, 222, 103837.

Yoo, S., Park, J., & Kim, H. (2021). A survey of network forensic analysis techniques for network intrusion detection systems. *Symmetry, 13*(12), 2526.