International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 6, Nov-Dec-2024, ISSN (Online): 2395-566X

# Forensic Readiness Using Tcpdump, Wireshark, and Log Analysis

**Shalini Mehra, Pavan Krishnan, Rituja Deshpande, Anil Borkar**
Indira Gandhi National Open University, New Delhi, India

**Abstract- Forensic readiness is a crucial component of modern cybersecurity, enabling organizations to effectively detect, analyze, and respond to security incidents. In a landscape where cyber threats are becoming increasingly sophisticated, forensic readiness ensures that organizations are prepared to collect and preserve digital evidence in a way that supports investigative processes and legal proceedings. This paper explores the role of network traffic capture tools, such as tcpdump and Wireshark, alongside log analysis, in forensic readiness. Tcpdump, a command-line tool for network packet capture, and Wireshark, a graphical network protocol analyzer, are instrumental in collecting real-time network data and identifying suspicious activities during security incidents. Log analysis plays a complementary role by providing detailed records of system and application events, helping investigators build a comprehensive timeline of the attack. Together, these tools enable organizations to monitor network traffic, correlate system activities, and preserve evidence, ensuring a rapid and efficient response to cyber threats. This paper discusses the features, practical applications, and benefits of using tcpdump, Wireshark, and log analysis in forensic investigations, highlighting their critical role in enhancing cybersecurity defenses and ensuring regulatory compliance.**

**Index Terms- forensic readiness, tcpdump, Wireshark, log analysis, network traffic capture, cybersecurity, incident response, digital evidence, packet analysis, security breach detection, network monitoring, real-time traffic analysis, event correlation, data preservation, cyberattack detection, regulatory compliance.**

## I. INTRODUCTION

In today's world, where cyber threats and data breaches have become increasingly prevalent, organizations need to be equipped with the right tools and strategies to identify, mitigate, and respond to these threats swiftly. One of the essential components of effective cybersecurity management is forensic readiness. This concept refers to an organization's preparedness to collect, preserve, and analyze digital evidence in the event of a security incident. It allows businesses to detect attacks in real-time, understand their causes, and ensure that the evidence gathered is legally admissible for further analysis or legal proceedings. Being able to gather and preserve digital evidence before and during an attack is vital for investigating security breaches and preventing future occurrences.

At the core of forensic readiness is the ability to effectively capture and analyze network traffic and system logs. Tools like tcpdump, Wireshark, and log analysis platforms are crucial for this purpose. These tools enable security professionals to capture network packets, analyze protocols, and correlate system activities to identify unusual or malicious behavior. By implementing forensic readiness through the use of these tools, organizations can ensure that they are prepared for potential security incidents, enabling them to respond faster and more efficiently.

Tcpdump and Wireshark are widely recognized for their packet capture and network traffic analysis capabilities. While tcpdump is a command-line tool useful for capturing and filtering network traffic, Wireshark offers a graphical interface that provides a more in-depth analysis of packets. Combining these with log analysis ensures that organizations not only track network traffic but also correlate this with system logs to build a comprehensive picture of the attack. The importance of forensic readiness cannot be overstated, as it plays a critical role in improving an organization's ability to handle and mitigate security threats, minimizing potential damage, and ensuring regulatory compliance.

## II. FORENSIC READINESS: THE NEED FOR CYBERSECURITY PREPAREDNESS

Forensic readiness is a crucial aspect of modern cybersecurity. As organizations continue to store and process large volumes of sensitive data, the risks of cyberattacks and data breaches have increased significantly. Cybercriminals are leveraging increasingly sophisticated methods to breach security defenses, steal data, and disrupt business operations. To counter these threats, organizations must be prepared to quickly respond to incidents by collecting and analyzing evidence, preserving critical data, and taking appropriate action. Forensic readiness ensures that, when a cyberattack or security incident occurs, organizations are well-equipped to investigate the incident effectively and mitigate its impact.

The primary goal of forensic readiness is to ensure that organizations can quickly detect, collect, and preserve evidence in a manner that is useful for analysis, incident response, and potential legal proceedings. This includes monitoring and capturing network traffic, user activities, system logs, and application logs to build a timeline of events leading to the attack. These logs and captured network traffic provide invaluable insights into what transpired during the breach, what vulnerabilities were exploited, and how the attackers navigated through the system.

A forensic readiness plan involves several key components. First, organizations need a robust system for data collection that can capture network traffic and log events in real-time. Tools like tcpdump and Wireshark play a significant role in capturing and analyzing network traffic. Second, data must be properly stored and preserved to prevent tampering. Forensic teams use specialized storage systems that ensure the integrity of evidence, often employing write-blocked drives or cloud-based storage for preservation. Third, organizations must have clear incident response procedures to ensure that evidence is collected systematically, and appropriate actions are taken during an ongoing breach. Lastly, staff members, especially IT and security teams, must be trained on how to handle and preserve evidence during an incident.

Without forensic readiness, organizations may struggle to identify the source and nature of an attack, making it harder to respond effectively. Furthermore, the lack of readiness can lead to difficulties in identifying the attackers, understanding the full scope of the damage, and taking preventive measures. Forensic readiness is thus essential not only for effective incident response but also for preventing future attacks by identifying vulnerabilities and strengthening defenses.

## III. TCPDUMP: A COMMAND-LINE NETWORK PACKET CAPTURING TOOL

Tcpdump is a command-line network packet capturing tool widely used in cybersecurity for analyzing network traffic. As a lightweight, fast, and flexible tool, tcpdump allows network administrators and forensic investigators to capture, filter, and analyze packets on a network interface. By intercepting network traffic, tcpdump provides real-time insights into data being transmitted across the network, making it a powerful tool for both proactive network monitoring and post-incident forensic analysis.

One of the primary features of tcpdump is its ability to capture raw network packets, including headers and data payloads, across the network interface. This ability is critical for forensic investigations because it allows investigators to see exactly what data was transferred during an attack or security breach. For instance, if a malware attack is suspected, tcpdump can capture the traffic that originates from infected machines or unauthorized devices, providing critical evidence for identifying the scope of the attack.

Additionally, tcpdump’s filtering capabilities allow users to isolate specific types of traffic. Filters can be based on various criteria such as IP addresses, ports, and protocols. This functionality is crucial during an investigation, as it allows forensic investigators to focus on traffic that is most relevant to the investigation while ignoring unrelated traffic. For example, if an attacker uses a specific port for communication with a remote server, tcpdump can filter for that port, ensuring that only the relevant traffic is captured and analyzed.

Tcpdump also supports real-time analysis, providing immediate feedback on network activities. By continuously capturing traffic, administrators can monitor the network for signs of suspicious activity, such as unusual traffic spikes, unauthorized communication attempts, or abnormal packet patterns that could indicate an attack. Furthermore, tcpdump allows captured packets to be saved in formats like pcap (packet capture), which can be later analyzed using more detailed tools like Wireshark, which provides a graphical interface for deeper analysis.

Forensic investigations often involve capturing a large amount of data to ensure no evidence is missed. Tcpdump helps in this by offering the capability to capture traffic over extended periods of time. It is particularly useful for network forensics, where investigators need to trace the origins of malicious traffic, identify the protocols used by attackers, and understand the sequence of events during a security incident.

## IV. WIRESHARK: A GRAPHICAL NETWORK PROTOCOL ANALYZER

While tcpdump is a powerful tool for packet capture, Wireshark takes network traffic analysis a step further by offering a comprehensive, user-friendly graphical interface. Wireshark is one of the most widely used network protocol analyzers and is indispensable for forensic investigations. It enables investigators to capture, display, and analyze packets in real-time, providing a detailed view of all network communications. Unlike tcpdump, which presents data in a command-line interface, Wireshark offers an intuitive graphical user interface (GUI) that simplifies the process of network analysis.

Wireshark decodes hundreds of network protocols, including TCP/IP, HTTP, DNS, FTP, and many others. This extensive support for various protocols allows forensic investigators to view network traffic in a human-readable format, making it easier to identify malicious behavior. For example, Wireshark can be used to analyze HTTP traffic to detect signs of data exfiltration, such as the unauthorized transfer of sensitive files from an internal server to an external IP address.

A key feature of Wireshark is its ability to perform deep packet inspection (DPI). DPI analyzes the contents of packets at a granular level, revealing not just headers but also data payloads. This capability is crucial in forensic investigations, as it helps identify the exact nature of the traffic, including any potential malicious data, such as the payload of an attack, malicious commands, or stolen data. For example, an attacker may use encryption to hide the contents of a communication, but Wireshark can still display metadata such as packet size, destination, and timing.

Wireshark also offers robust filtering options, allowing investigators to narrow down the traffic to specific protocols, IP addresses, or ports of interest. The tool's filtering system is flexible and powerful, supporting various expressions to filter traffic based on different conditions. This helps forensic investigators focus on the most relevant traffic without wading through unrelated data. Additionally, Wireshark's real-time capture capability allows security analysts to monitor ongoing network activity, making it ideal for detecting live attacks.

Wireshark also enables investigators to export captured data to various formats, such as pcap or txt, for further analysis. The data can be analyzed in more depth using other forensic tools or shared with other team members for collaborative analysis. The graphical presentation of Wireshark, including color-coded traffic and packet breakdowns, makes it easier for analysts to spot anomalies and suspicious activities quickly.

## V. LOG ANALYSIS: CORRELATING EVENTS AND IDENTIFYING PATTERNS

In addition to network packet capture tools like tcpdump and Wireshark, log analysis plays an essential role in forensic readiness. System and application logs provide a detailed record of activity on a machine, including login attempts, system errors, application events, and more. Logs offer valuable insights into the sequence of events surrounding an attack, helping investigators understand what happened before, during, and after a breach.

System logs, such as syslog on Linux or Windows Event Logs, provide a high-level view of system activity. They typically capture information about system startups, shutdowns, user logins, and critical errors. In the case of a security incident, system logs can provide valuable context about how an attacker gained access to the system, what actions they took, and whether they escalated their privileges.

Application logs, on the other hand, offer insights into the behavior of specific software or services running on a system. These logs capture events such as failed login attempts to a web server, successful or unsuccessful data queries on a database, and error messages generated by application software. By analyzing application logs, investigators can trace an attacker's movements across different layers of the application, helping them determine the scope of the attack.

Event correlation is a critical aspect of log analysis. Security professionals often correlate logs from multiple sources to piece together the full picture of a breach. For example, by correlating failed login attempts in system logs with suspicious network activity captured by tcpdump or Wireshark, investigators can identify patterns that suggest an attempted intrusion or a brute force attack.

One of the most useful aspects of log analysis is its ability to provide a timeline of events. Investigators can create a timeline of malicious activity by correlating logs from different systems, helping them determine how the attack unfolded. This timeline can be invaluable in understanding the attack's origin, method of execution, and impact, as well as in planning preventive measures for the future.

Additionally, log analysis tools, such as ELK Stack (Elasticsearch, Logstash, and Kibana), offer powerful features for real-time monitoring and automated analysis. These tools can aggregate logs from various sources, filter relevant events, and even trigger alerts when suspicious activity is detected, allowing organizations to respond promptly to incidents.

## VI. CONCLUSION

Forensic readiness is a vital aspect of modern cybersecurity, enabling organizations to be prepared for the inevitability of a cyberattack. By leveraging network traffic capture tools such as tcpdump and Wireshark, as well as log analysis, organizations can collect, preserve, and analyze critical evidence in real-time. These tools help identify malicious activity, track the progression of an attack, and ensure that digital evidence is preserved for further investigation.

Through effective forensic readiness, organizations can not only respond quickly to incidents but also enhance their ability to prevent future attacks by understanding the tactics and techniques used by attackers. Incorporating tcpdump, Wireshark, and log analysis into a comprehensive forensic readiness strategy ensures that organizations are well-equipped to protect their data, mitigate the impact of breaches, and comply with legal and regulatory standards.

## REFERENCES


1. Coad, B. A. (2017). Network Packet Management Optimisation for Business Forensic Readiness (Doctoral dissertation, Auckland University of Technology).
2. Biswas, A., Singh, B. K., & Chowdhury, S. (2018). Network Forensics Analysis. RCC Institute of Information Technology.
3. Datt, S. (2016). Learning network forensics. Packt Publishing Ltd.
4. Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H., & Stoddart, K. (2016, August). Forensic readiness for SCADA/ICS incident response. In 4th International Symposium for ICS & SCADA Cyber Security Research 2016. BCS Learning & Development.
5. Johansen, G. (2017). Digital forensics and incident response. Packt Publishing Ltd.
6. Bhusal, J. (2016). Network analysis with open source packet analyzers: case wireshark.
7. Madamanchi, S. R. (2021). Linux server monitoring and uptime optimization in healthcare IT: Review of Nagios, Zabbix, and custom scripts. International Journal of Science, Engineering and Technology, 9(6), 1–8.
8. Madamanchi, S. R. (2021). Disaster recovery planning for hybrid Solaris and Linux infrastructures. International Journal of Scientific Research & Engineering Trends, 7(6), 1–8.
9. Madamanchi, S. R. (2021). Mastering enterprise Unix/Linux systems: Architecture, automation, and migration for modern IT infrastructures.
10. Madamanchi, S. R. (2022). The rise of AI-first CRM: Salesforce, copilots, and cognitive automation.
11. Madamanchi, S. R. (2023). Efficient Unix system management through custom Shell, AWK, and Sed scripting. International Journal of Scientific Development and Research, 8(9), 1295–1314.
12. Bullock, J., & Parker, J. T. (2017). Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework. John Wiley & Sons.
13. Joshi, R. C., Pilli, E. S., Joshi, R. C., & Pilli, E. S. (2016). Network forensic tools. Fundamentals of Network Forensics: A Research Perspective, 71-93.
14. Van Staden, F. R. (2017). Investigating and Implementing an Email Forensic Readiness Architecture. University of Pretoria (South Africa).
15. Muniz, J., & Lakhani, A. (2018). Investigating the cyber breach: the digital forensics guide for the network engineer. Cisco Press.
16. Doshi, A., & Sharma, P. (2020). Digital forensics analysis for network related data. International Research Journal of Engineering and Technology (IRJET), 7(4), 1390-1398.
17. Da-Yu, K. A. O., Chang, E. C., & Fu-Ching, T. S. A. I. (2019, February). Extracting Suspicious IP Addresses from WhatsApp Network Traffic in Cybercrime Investigations. In 2019 21st International Conference on Advanced Communication Technology (ICACT) (pp. 1108-1115). IEEE.
18. Shashidhara, D., & Minavathi. (2019). A Survey: On Network Forensic Data Acquisition and Analysis Tools. In Emerging Research in Electronics, Computer Science and Technology: Proceedings of International Conference, ICERECT 2018 (pp. 649-659). Springer Singapore.