International Journal Of Health, Engineering And Technology (IJHET) *E-ISSN 2829 - 8683*
Volume 5, Number 1, May 2026, *Page. 59 - 64*
Email : editorijhess@gmail.com

Network Forensic Approach in Data Breach Crime Investigation

Aghastyar[1)], Bryan Idias[2)], Caelsea Asalyandira Azzahra[3)], Irfan Hakim[4)], Ingrid Bianty Rahmawati[5)], Nimrod Welly Belo[6)], Tri Susanti[7)], Tri Widyasto Prabowo[8)], Yuni Priskila Ginting[9)]*
[1,2,3,4,5,6,7,8,9)] Universitas Pelita Harapan

*Corresponding Author
Email : yuni.ginting@uph.edu

Abstract

This study aims to analyze the application of a network forensics approach in data breach crime investigations and examine its technical and legal implications. The method used is a qualitative approach through case studies, network log analysis, and a literature review. The research object focuses on the 2021 Microsoft Exchange Server attack case to reconstruct the attack chronology based on network artifacts. The results show that network forensics is effective in systematically identifying attack stages, from initial activity to data exfiltration, and is able to uncover communication patterns and attack methods used by perpetrators. However, challenges arise from the use of anonymity and encryption techniques that complicate the investigation process. From a legal perspective, the analysis results can be used as digital evidence in proving cybercrime in accordance with applicable laws and regulations. This study also emphasizes the importance of forensic readiness in organizations through network monitoring, log management, and the utilization of open information. Thus, network forensics plays a crucial role not only in investigations but also in overall cybersecurity strategies.

Keywords: Network Forensics, Data Breach, Cybercrime.

INTRODUCTION

The development of information and communication technology has driven digital transformation in various sectors of life, including government, business, and public services. The use of digital-based systems enables faster and more efficient data management and exchange. However, this progress is also accompanied by an increasing threat of cybercrime, one of which is data breaches or data leaks. A data breach is the illegal access, acquisition, or disclosure of data by unauthorized parties, which can result in financial losses, reputational damage, and privacy violations for individuals and organizations (Silalahi et.al, 2025). This situation demonstrates that data security is a crucial issue in today's digital era. The increase in data breach cases globally demonstrates that information security systems still have many gaps that can be exploited by criminals. Cybersecurity investigation reports indicate that attacks on data are carried out not only through simple methods, but also through complex techniques such as exploiting system vulnerabilities, malware, and network-based attacks (Azizah et.al, 2024). One prominent example is the 2021 attack on Microsoft Exchange Server, where the perpetrators exploited a zero-day vulnerability to gain unauthorized access to the system, steal sensitive data, and install a backdoor to maintain long-term access. This case demonstrates that data breaches are organized, systematic, and difficult to detect without a proper investigative approach.

In facing this complexity, a digital forensic approach, particularly network forensics, is crucial. Network forensics is the process of collecting, monitoring, analyzing, and reconstructing network traffic activity to identify and prove the occurrence of cybercrime (Mursyid et.al, 2025). Through techniques such as packet analysis, log analysis, intrusion detection, and flow analysis, investigators can trace the perpetrator's digital footprint and understand the attack patterns used. This process not only helps identify the perpetrator but also systematically reconstructs the chronology of events and produces legally admissible digital evidence. From a legal perspective, network forensics plays a crucial role in the process of proving cybercrime. In Indonesia, data leaks are related to violations of the Electronic Information and Transactions Law and the Personal Data Protection Law. Digital evidence generated through network forensics can be used as valid evidence in court proceedings, as

long as it is obtained in accordance with applicable procedures (Nababan & Sumardiana, 2025). Therefore, the integration of technical and legal aspects is crucial in handling data breach cases.

The problem that arises in this research is how the network forensics approach can be used effectively in investigating crimes in the form of data breaches, and how the results of this analysis can support the evidentiary process in law enforcement. Furthermore, it is necessary to examine the extent to which network forensics methods are able to uncover increasingly complex attack patterns and adapt to technological developments. Based on these problems, this study aims to analyze the application of the network forensics approach in data breach investigations and examine its role in supporting the effectiveness of law enforcement in the digital era. This research is expected to contribute to the development of science in the fields of cybersecurity and law, as well as serve as a reference for practitioners in handling data breach cases more comprehensively.

RESEARCH METHODS

This study uses a qualitative approach with a juridical-normative approach and descriptive analysis. A qualitative approach is a research method that aims to understand phenomena in depth based on context and meaning, rather than numbers or statistics (Niam et.al, 2024). The focus of this study is to examine the application of network forensics in data breach crime investigations from a technical and legal perspective. The research materials consist of secondary data including scientific literature, case reports, and laws and regulations such as the ITE Law and the Personal Data Protection Law. This study uses the 2021 Microsoft Exchange Server data breach case as the object of analysis. The network forensics method used includes general stages such as data collection, monitoring, analysis, reconstruction, and reporting (Mahendra et.al, 2024). The research design used is a case study with a purposive sampling technique, selecting cases based on their relevance and impact. The variables studied include the effectiveness of network forensics methods in identifying attacks, reconstructing events, and supporting legal evidence. Data collection was conducted through literature review, while data analysis used a descriptive-analytical method and a juridical approach. This research does not use a statistical model because it is qualitative, but it is still carried out systematically to produce valid conclusions.

RESULTS AND DISCUSSION

Through a case study of the 2021 Microsoft Exchange Server attack, a network forensic investigation systematically reconstructed the attack chronology based on digital traces in activity logs, packet capture (PCAP), and communication patterns between systems. This chronology encompasses early stages, such as scanning and exploiting security vulnerabilities, through to more advanced stages, such as installing web shells and exfiltrating data. Each stage leaves a distinctive pattern of activity that can be analyzed to identify the attack method and the perpetrator's goals, enabling network forensics to serve as a tool for "reading" the hidden traces behind complex data traffic. This approach emphasizes not only technical identification but also a comprehensive and contextual reconstruction of the event narrative, where network artifacts serve as a primary source for building a comprehensive understanding of how the attack occurred, developed, and had an impact. The investigation goes beyond the discovery of technical evidence to interpret the relationships between network activities that form a logical sequence of events.

Furthermore, this approach emphasizes the importance of contextual analysis in understanding network activity. Not all anomalies can be directly categorized as attacks, so the ability to distinguish between normal and suspicious activity based on the pattern, frequency, and characteristics of data communication is necessary. Analysis of communication patterns, such as the relationship between IP addresses, connection frequency, and the type of protocol used, is key to identifying unusual interactions. Furthermore, the relationships between network activities also need to be analyzed

holistically to identify the relationship between one event and another, allowing for a logical and accountable attack flow. Network forensics serves not only as a technical tool but also as an analytical approach that integrates data, context, and interpretation to produce a comprehensive understanding of cybercrime. This aligns with the view that digital forensic investigations require the ability to connect various pieces of information into a coherent narrative, thus serving as the basis for decision-making and legal evidence (Rojabi, 2025). Thus, the network forensics approach makes a significant contribution to uncovering data breach crimes in a more in-depth and systematic manner.

Incident Chronology Based on Network Analysis

The attack began with server scanning activity characterized by a spike in requests from multiple foreign IP addresses within a short period of time. This pattern indicates a systematic system exploration effort to identify exploitable security vulnerabilities. In the context of the analysis,*packet capture*(PCAP) using Wireshark, the activity can be identified through repetitive request patterns, unusual IP address distribution, and significantly increased connection frequency compared to normal traffic (Fanani et.al, 2026). This indicates that the initial stage of the attack is not random, but rather planned as part of a process.*reconnaissance*.

The next stage shows the exploitation of system gaps, which in this case is related to techniques.*Server-Side Request Forgery*(SSRF). Unusual requests to specific endpoints indicate that the attacker successfully manipulated the system to access internal resources without going through legitimate authentication mechanisms. This pattern can be observed through anomalies in network logs, such as requests to rarely used endpoints or request parameters that do not conform to normal patterns. This finding emphasizes the importance of network traffic analysis not only for detecting suspicious activity but also for identifying specific attack methods.

After successfully gaining access, the perpetrator continued his actions by uploading files via the HTTP POST method which led to the installation.*web shell*. Existence*web shell*is an important indicator in investigations because it serves as a tool to maintain continuous access (*persistent access*). In network log analysis, this activity is characterized by the presence of HTTP requests containing a specific payload and repeated communication between the victim server and an unknown IP address. This communication pattern indicates the presence of a*command and control*(C2 communication), where the perpetrator can control the system remotely in a hidden manner.

The final stage of the attack chronology was marked by data exfiltration activity, which was seen from the spike in outgoing traffic (*outbound traffic*) to an external server. This activity is typically characterized by large data transfers or consistent but unusual communication patterns. In some cases, the exfiltration process utilizes encryption or other obfuscation techniques to avoid detection by security systems. This suggests that the perpetrators are not solely focused on data collection but also attempt to obscure their activities (Aditya & Yudiantara, 2025).

The chronology of this incident shows that the data breach attack took place through interrelated stages, starting from*reconnaissance*, exploitation, access maintenance, and data exfiltration. Each stage leaves a digital footprint in the form of network artifacts that can be analyzed and reconstructed. Thus, a network forensics approach has proven capable of providing a comprehensive picture of the attack flow and strengthening the digital evidence-based investigation process (Rahman et al., 2026).

Thematic Findings of Network Forensic Artifacts

Several key themes emerge in network forensic investigations that illustrate the characteristics and dynamics of data breaches. The first theme is structured attack patterns, where the perpetrators execute a systematic series of steps starting from the initial stage.*reconnaissance*, exploitation, to*exfiltration*This pattern indicates that the attack was not carried out spontaneously, but rather through careful, multi-layered planning. Each stage had a specific objective, such as gathering initial information, exploiting security vulnerabilities, and even illegally obtaining data. These findings reinforce the view that modern cybercrime is organized and often involves complex strategies. In

network forensics, recognizing these patterns is crucial for understanding attack paths and anticipating potential follow-up attacks.

The second theme is the existence of digital traces in the form of network artifacts, such as activity logs, traffic patterns, and communications between servers. These artifacts are a key resource in the investigative process because they record every interaction that occurs within the network system. Even if the perpetrator attempts to disguise their activities, digital traces can still be discovered through in-depth analysis of network data. For example, repeated communication patterns, the use of specific protocols, or anomalies in data flows can be indicators of suspicious activity. In this case, network forensics acts as an interpretive tool that transforms raw data into meaningful information that can be used to reconstruct events (Riadi et al., 2026). Thus, network artifacts serve not only as technical evidence but also as a foundation for building a comprehensive investigative narrative.

The third theme is the perpetrators' use of anti-forensic techniques, such as data encryption, IP address obfuscation, and the use of stealth communications to avoid detection. These techniques indicate that the perpetrators are not only focused on the success of the attack but also on obscuring the digital footprints they leave behind. In practice, the use of encryption can make it difficult for investigators to identify the content of communications, requiring analysis to focus on metadata and traffic patterns. Furthermore, techniques such as the use of*proxy*or anonymous networks make the process of tracing the source of an attack more complex. These findings emphasize that network forensic investigations face challenges that are not only technical but also strategic in addressing detection evasion efforts (Addari et.al, 2026).

In addition to these three main themes, the analysis also reveals a correlation between network artifacts, forming a pattern that can be used to reconstruct the entire incident. Correlations between system logs, traffic patterns, and network communications allow investigators to identify causal relationships for each activity. This demonstrates that the success of an investigation depends not only on a single type of data, but on the ability to comprehensively integrate various sources of information. These thematic findings demonstrate that a network forensics approach serves not only as a technical tool for identifying attacks but also as an analytical approach capable of uncovering the structure, patterns, and strategies behind data breaches. By understanding these themes, investigators can gain a deeper understanding of the perpetrator's modus operandi and improve the effectiveness of future cybercrime investigations and prevention efforts.

Based on the analysis results described, it can be interpreted that the network forensics approach has a high level of effectiveness in uncovering data breach crimes, particularly in reconstructing the chronology of events and identifying the attack methods used by the perpetrators. Through the analysis of network artifacts such as activity logs, traffic patterns, and communication between systems, investigators can systematically and comprehensively construct the flow of events. This capability demonstrates that network forensics functions not only as a detection tool but also as a reconstruction tool capable of providing a complete picture of the dynamics of cyberattacks. This aligns with the view that network analysis is a crucial component in digital forensic investigations because it can uncover activities that are not directly visible within the system (Rahman et al., 2026).

In addition, the network forensic approach has also been proven to be able to identify specific attack methods, such as exploiting system vulnerabilities, installing*web shell*, as well as communication patterns*command and control*This identification provides a deeper understanding of the perpetrator's modus operandi, making it useful not only in the investigation process but also in future prevention efforts. Thus, the analysis results have strategic value because they can be used as a basis for developing a security system that is more adaptive to cyber threats. However, this study also shows challenges in implementing network forensics, particularly related to perpetrator anonymity and the use of encryption techniques. Cybercriminals tend to use various methods to hide their identities, such as using dynamic IP addresses,*proxy*, or anonymous networks, making the tracking process more complex. On the other hand, the use of encryption in data communications makes message content impossible to analyze directly, requiring investigators to rely on analysis of metadata

and network traffic patterns (Riadi et al., 2026). This situation demonstrates that while network forensics is effective, there are limitations that must be addressed through the development of more sophisticated methods and technologies.

From a legal perspective, these findings have important implications for proving cybercrime in Indonesia. Digital evidence generated through network forensics, such as activity logs and communication traces, can be used to demonstrate illegal access, data interception, and unauthorized transfer of information. This relates to the provisions of the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP). Thus, network forensics results not only have technical value as an investigative tool but also have legal force as evidence in law enforcement proceedings (Mursyid et.al, 2025). In line with these findings, it is important for organizations to improve their forensic readiness (*forensic readiness*) in facing potential data breaches. This readiness includes the ability to anticipate, detect, and respond to incidents effectively. One step that can be taken is to implement a network monitoring system.*real-time*capable of detecting suspicious activity early. Furthermore, structured and continuous activity logging is crucial, as this data will form the primary basis for forensic investigations.

Furthermore, log management must address integrity and security aspects to ensure digital evidence remains valid and accountable. In this regard, forensic readiness depends not only on technology but also on organizational policies and procedures for managing data. Furthermore, the integration of technical*Open Source Intelligence*(OSINT) can be a complement to investigations, as it allows organizations to obtain open-source information regarding potential external threats. A proactive approach through*forensic readiness*This allows organizations to not only react to attacks that have already occurred but also anticipate potential future threats. Thus, network forensics serves not only as an investigative tool but also as an integral part of a broader cybersecurity strategy, encompassing prevention, detection, and incident response (Firmansyah, 2025). The integration of network forensics interpretation, legal implications, and organizational preparedness demonstrates that this approach plays a strategic role in addressing data breaches. Despite various challenges, implementing network forensics supported by sound organizational preparedness can improve the effectiveness of investigations while continuously strengthening security systems.

CONCLUSION

Based on the research results and discussion, it can be concluded that the network forensics approach plays a significant role in data breach crime investigations. Through the analysis of network artifacts such as activity logs, traffic patterns, and inter-system communications, this approach can systematically and structuredly uncover the chronology of attacks, starting from the initial stage.*reconnaissance*, exploiting security vulnerabilities, maintaining access, and even exfiltrating data. These capabilities demonstrate that network forensics serves not only as an incident identification tool but also as a comprehensive reconstruction tool for understanding the dynamics of cyberattacks. The research also shows that data breach crimes are complex and organized, with perpetrators employing various sophisticated techniques such as exploiting system vulnerabilities and installing malicious software.*web shell*, and communication*command and control*to maintain access and control of systems. On the other hand, the use of anti-forensic techniques such as encryption, identity theft, and the use of anonymous networks poses a major challenge in the investigation process. This situation demands improved network forensic analysis capabilities that are more adaptive and based on the integration of various analysis techniques.

From a legal perspective, the findings of this study confirm that network forensics have strategic value as digital evidence in proving cybercrimes. The resulting evidence, such as traces of illegal access, data interception, and unauthorized information transfer, can be used to fulfill the elements of violations under applicable legal provisions, particularly the Electronic Information and Transactions Law and the Personal Data Protection Law. Thus, the network forensics approach not

only has technical value but also possesses legal force in supporting law enforcement processes. Furthermore, this study also emphasizes the importance of implementing forensic preparedness (*forensic readiness*) within an organization as part of a broader cybersecurity strategy. This readiness includes the ability to conduct continuous network monitoring, structured activity log management, and the integration of external information sources to identify potential threats early. This approach enables organizations to not only respond to incidents that have occurred but also anticipate and prevent future attacks. This research confirms that a network forensics approach is an effective and relevant tool in addressing data breaches in the digital age. Despite facing various challenges, implementing this approach, supported by organizational readiness and the integration of technical and legal aspects, can increase the effectiveness of investigations while continuously strengthening information security systems.

REFERENCES

Aditya, K. M. S., & Yudiantara, I. G. N. N. K. (2025). Criminological analysis of personal data theft crimes in the digital era.*Journal of Academic Media (JMA)*, 3(2).

Addari, M. A., Siregar, G. R., Lubis, A. B., Ariestia, C. I., & Zatalini, Z. (2026). Literature study on the evolution of computer viruses: Spread mechanisms, forensic investigations, and artificial intelligence-based detection strategies.*JIKUM: Journal of Computer Science*, 2(1), 22–25.

Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Cybersecurity as the foundation for developing mobile financial applications: A literature study on cybercrime and its mitigation.*Accounting and Information Technology*, 17(2), 221–237.

Fanani, G. P. I., Luthfiana, D. A., Pramurwitasari, A., Najich, M. N., & Putra, A. T. (2026). Analysis of network traffic patterns during DDoS attacks using Snort IDS.*Scientific: Journal of Computer Science and Informatics*, 3(1), 10–23.

Firmansyah, R. A. (2025).*Digital forensic readiness and information security management system integration framework in government environment*(Doctoral dissertation, Islamic University of Indonesia).

Mahendra, B. A., Utomo, Y. B., & Kurniadi, H. (2024). Implementation of network forensic methods for monitoring Windows Server computers.*Journal of Information System and Computer*, 3(1), 1–8.

Mursyid, M., Putera, A., & Jannah, M. (2025). Reconstructing the role of digital forensics in cybercrime investigations: A critical analysis of the construction of criminal law in Indonesia.*Tana Mana Journal*, 6(2), 289–296.

Nababan, F. E., & Sumardiana, B. (2025). The crime of personal data theft through cyber phishing and its evidentiary system in court: A study of Decision No. 697/Pid. Sus/2024/PN. Sda.*Bookchapter Law and Environment*, 1, 627–650.

Niam, M. F., Rumahlewang, E., Umiyati, H., Dewi, N. P. S., Atiningsih, S., Haryati, T., ... & Wajdi, F. (2024).*Qualitative research methods*.

Rahman, R., Inayah, F. M. N., & Apriyani, D. (2026). Digital forensic analysis of malware attack incidents on operating systems.*INOMATEC: Journal of Innovation and Contemporary Multidisciplinary Studies*, 1(03).

Riadi, I., Rochmadi, T., Wintolo, H., Handoyo, J., Syukri, M., Suhartono, B., & Umar, R. (2026).*Digital forensic analysis*.

Rojabi, M. A. (2025). *Cyber crime & digital forensics: The current role of digital forensics from hoaxes to proving fake diplomas*. Afdan Rojabi Publisher.

Silalahi, R. S., Mulyadi, M., & Trisna, W. (2025). Legal analysis of cyber data breach crimes in the digital era based on the Electronic Information and Transactions Law (Study of Decision Number 2447/Pid. Sus/2024/PN Mdn).*SIBATIK Journal: Scientific Journal in the Fields of Social, Economic, Cultural, Technology, and Education*, 4(9), 2425–2440.