Forensic Analysis of Distributed Denial of Service Attacks using National Institute of Standards and Technology Method

Augustav Fahrul Alzaiya
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
Distributed Denial of Service (DDoS) attacks are a threat to computer networks that can disrupt services by flooding the target with large amounts of traffic. This study aims to apply a digital forensics method based on the National Institute of Standards and Technology (NIST) to analyze DDoS attacks on MikroTik RouterOS-based routers. The research method employs the stages of collection, examination, analysis, and reporting, utilizing Wireshark to capture network traffic and router logs as digital evidence. The examination process involves filtering ICMP and TCP SYN packets to identify attack patterns, attacker IP addresses, and attack targets. Test results indicate a surge in traffic that caused the router's CPU load to rise above 90% and degraded network service quality. Analysis of the captured files and router logs confirms that the NIST method is effective for systematically identifying the type of attack, its source, and its impact on the network.

Keywords
DDoS, Digital Forensics, NIST, RouterOS, Wireshark.

1. INTRODUCTION
Distributed Denial of Service (DDoS) attacks are known to cause downtime on university servers, thereby disrupting online academic services [1]. Wireshark is widely used as a network analysis tool to measure Quality of Service (QoS) through parameters such as throughput, delay, jitter, and packet loss in order to detect network traffic anomalies [2]. Additionally, the integration of Snort as an Intrusion Prevention System (IPS) and Splunk as a Security Information and Event Management (SIEM) system has proven effective in mitigating ICMP Flood and SYN Flood attacks by significantly reducing attack traffic [3]. The use of the Simple Queue method on MikroTik routers has also been shown to optimize bandwidth and maintain network stability during traffic spikes [4]. QoS parameters such as throughput, delay, and packet loss are also utilized to evaluate network quality while detecting abnormal traffic [5]. Wireshark is also used in evaluating the performance of Virtual Access Points and Real Access Points, with results showing no packet loss during the testing period [6]. Additionally, the Access Control List (ACL) on MikroTik has proven capable of restricting unauthorized network access, thereby enhancing network security [7]. Snort, as an Intrusion Detection System (IDS), also possesses the ability to detect DDoS attacks, brute-force attacks, and port scanning with a high degree of accuracy [8]. The Differentiated Services (DiffServ) method is known to be effective in managing throughput, delay, and jitter in educational streaming systems [9]. The implementation of Virtual Local Area Networks (VLANs) has also proven capable of reducing delay and packet loss, thereby improving network performance and security [10]. Other research indicates that Suricata, as an Intrusion Detection and Prevention System (IDPS), is capable of detecting and mitigating SYN Flood and SQL Injection attacks with good performance [11]. DDoS and malware threats are also the most common forms of cyberattacks in Indonesia due to a lack of education and law enforcement in the field of cybersecurity [12]. Firewall rules on MikroTik RouterOS are known to be effective in protecting networks from ARP Spoofing and DDoS attacks [13]. Additionally, a security framework based on Software-Defined Networking (SDN) can detect and mitigate slow-rate DDoS attacks with high efficiency using online machine learning methods [14]. The integration of NIST CSF 2.0, ISO/IEC 27001:2022, and CIS Controls is also used to strengthen information security management in electronic government systems [15].

2. LITERATURE STUDY

2.1 Distributed Denial of Service (DDoS)
A Distributed Denial of Service (DDoS) attack is a cyberattack that floods a target server or computer with network traffic until the service becomes slow or inaccessible. These attacks come in various forms, such as UDP Flood, ICMP Flood, SYN Flood, HTTP Flood, and Slowloris, which exploit system vulnerabilities to drain server resources [16]. Therefore, additional security systems like Cloudflare Magic Transit are needed to help protect servers from DDoS attacks [17]. Figure 1 illustrates a DDoS attack workflow diagram.

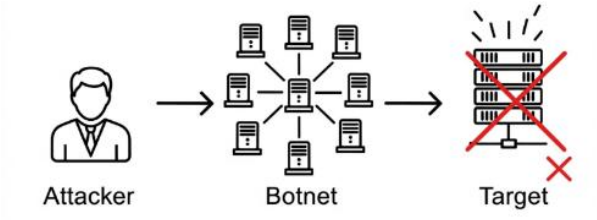

Figure 1 : DDoS Workflow

2.2 Wireshark
A Distributed Denial of Service (DDoS) attack is an attack. Wireshark is an open-source application used to capture and analyze data packets on computer networks to measure network quality through QoS parameters such as throughput, packet loss, delay, and jitter [18]. Additionally, Wireshark is effective in detecting attacks such as TCP SYN Flood by displaying network packet details, statistics, and analysis graphs in real-time through the stages of collection, conversion, and analysis, although it has limitations in automatically detecting suspicious activity as well as attacks using fake or random IP addresses [19]. cyberattacks that flood network traffic on target servers or computers until services become slow or inaccessible. These

attacks include various types such as UDP Flood, ICMP Flood, SYN Flood, HTTP Flood, and Slowloris, which exploit system vulnerabilities to drain server resources [20]. Therefore, additional security systems like Cloudflare Magic Transit are needed to help protect servers from DDoS attacks [21]. An illustration of the Wireshark workflow can be seen in Figure 2.

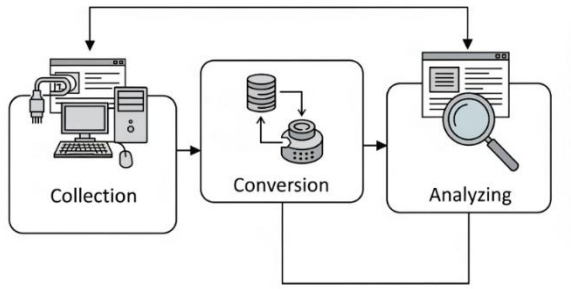

Figure 2 : Wireshark Workflow

2.3 Computer Network

A computer network is a collection of devices connected to one another via wired or wireless media to share data and information. Based on their geographical scope, computer networks are classified into LANs (Local Area Networks), MANs (Metropolitan Area Networks), and WANs (Wide Area Networks), which cover very large areas, even spanning multiple countries [22]. Figure 3 illustrates a WAN computer network.

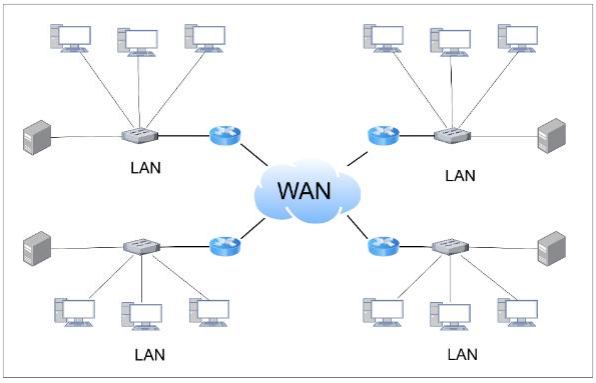

Figure 3 : Wide Area Network

2.4 Digital Forensics

Digital forensics is a field of science focused on the identification, collection, preservation, analysis, and presentation of digital evidence to investigate information technology-based crimes in an objective and legally accountable manner [23]. The digital forensics process includes the stages of identification, collection, preservation, analysis, documentation, and reporting to maintain the integrity of evidence during an investigation [24]. In practice, digital forensics encompasses several branches, such as network forensics to analyze network traffic and detect cyberattacks, database forensics to investigate activities within database systems, computer forensics to analyze computer devices, and device forensics to examine hardware and the digital activities stored within it [23]. The stages of digital forensics are illustrated in Figure 4.

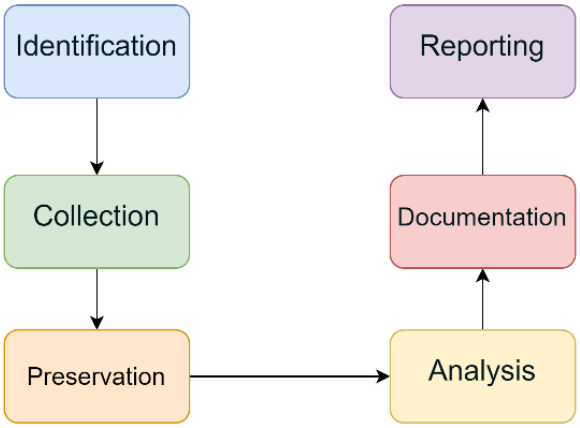

Figure 4 : Stages of Digital Forensics

2.5 Firewall

A firewall is a network security system designed to regulate and control incoming and outgoing data traffic to prevent unauthorized access and protect the network from cyber threats such as hackers, viruses, and other attacks. Additionally, firewalls come in several types, including Packet Filtering Routers, Application-Level Gateways, and Circuit-Level Gateways, and employ techniques to control services, access directions, users, and network behavior to enhance system security [25]. Figure 5 illustrates the firewall workflow.

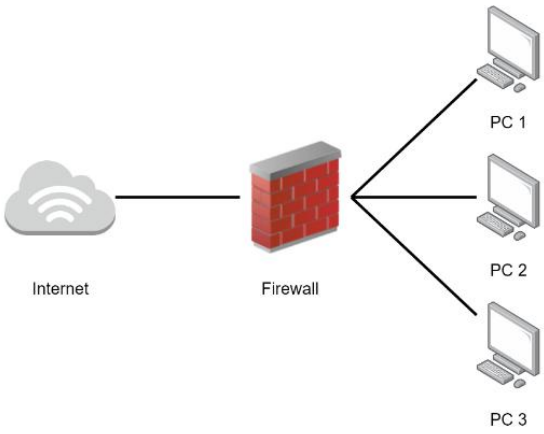

Figure 5 : Firewall Workflow

2.6 National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) method is a digital forensic approach consisting of four main stages—Collection, Examination, Analysis, and Reporting—designed to preserve the integrity of digital evidence throughout the investigative process. This method provides systematic procedures for identifying, collecting, examining, analyzing, and documenting digital evidence so that the results of the investigation are scientifically and legally sound. In practice, the Collection stage is conducted to gather and secure digital evidence; the Examination stage is used to verify data integrity; the Analysis stage aims to identify critical information related to the incident; and the Reporting stage is carried out to compile an investigative report to support the investigative process [26], [27]. Figure 6 illustrates the workflow of the NIST method.

Figure 6 : NIST Method Workflow

3. RESEARCH METHODOLOGY

3.1 Research Subject

The subject of this study is the PC router device. Analysis of Distributed Denial of Service (DDoS) attacks was conducted using the Wireshark tool to analyze and acquire data from the router device, in order to identify the source of the attack. This facilitates subsequent steps to secure the system and mitigate attacks. This approach also provides accurate forensic evidence that supports the investigation and response process..

3.2 Software and Hardware

This research employs a combination of software and hardware to support the network forensics process in accordance with NIST methods. The software used is Wireshark, serving as the primary tool for data acquisition and analysis of DDoS attacks. The hardware consists of a laptop running Linux and Windows Virtual Machines (VMs). This setup ensures controlled and reliable forensic analysis. Details of the hardware and software specifications are provided in Table 1.

Table 1. Hardware and Software Used

Hardware	Software
Laptop MSI GF63 11ThinUC	Oracle Virtual Machine Mikrotik RouterOS 6.49.15
	Oracle Virtual Machine Kali Linux 2024.03
	Oracle Virtual Machine Ubuntu 24.04.2 LTS
	Wireshark 4.2.2
	Winbox 4.1

3.3 Analysis

The research analysis was conducted to identify system requirements for detecting Distributed Denial of Service (DDoS) attacks using the National Institute of Standards and Technology framework through analysis of network traffic obtained via packet sniffing using Wireshark. This process aims to recognize normal traffic patterns and anomalies such as spikes in SYN, ICMP, and UDP packets, as well as support system requirements for real-time data acquisition, automatic attack trace identification, and digital evidence extraction to build a network security system that is responsive and adaptive to DDoS threats. In addition, the analysis contributes to improving the accuracy of attack detection, optimizing network traffic monitoring, and strengthening the incident response process against potential cyberattacks.

3.4 Implementation

This research was conducted by applying the National Institute of Standards and Technology (NIST) methodology in simulating a Distributed Denial of Service (DDoS) attack on a local network. The implementation process included a preliminary study, network setup using Winbox, and attack simulation and traffic analysis using Wireshark. The forensic stages were carried out through Collection, Examination, Analysis, and Reporting to identify attack patterns and the attacker's IP source, as well as to compile a digital investigation report based on the captured network traffic.

4.1 Collection

The Collection phase in the National Institute of Standards and Technology (NIST) method involves the real-time collection of digital evidence during an ICMP Flood attack using a live acquisition approach. In this study, Wireshark was run on an Ubuntu Linux virtual machine in promiscuous mode to capture all network traffic on the same segment as the target router. The digital evidence collected consists of .pcap files from Wireshark and router logs from Winbox on MikroTik RouterOS, which contain source and destination IP

4. RESULTS AND DISCUSSION

A research simulation was conducted to analyze Distributed Denial of Service (DDoS) attacks against routers using the National Institute of Standards and Technology (NIST) methodology. During the Pre-Incident phase, investigators prepared for the investigation by installing Wireshark, synchronizing device times, and documenting network conditions. During the Incident phase, an ICMP Flood attack caused a surge in traffic, causing the router's CPU load to reach 100% and disrupting the network. Investigators then performed live packet capture using Wireshark and obtained a .pcap file as the primary digital evidence. Next, in the Post-Incident phase, the Examination, Analysis, and Reporting processes were carried out to identify attack patterns, the attacker's IP address, the impact on the router, and to formulate prevention recommendations such as firewall rules and rate limiting.

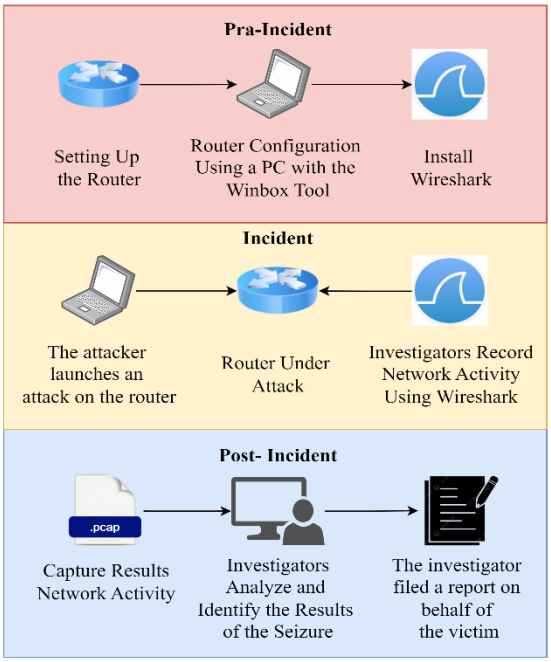

Figure 7 : Case Simulation Pra-Incident, Incident and Post-Incident

In figure 7, the stages of handling and analysing network attacks, which consist of three phases: Pre-Incident, Incident and Post-Incident. During the Pre-Incident stage, the administrator prepares the router, configures it using Winbox, and installs Wireshark as a network monitoring tool. Next, in the Incident stage, the attacker launches an attack on the router while the administrator records network activity using Wireshark. Once the attack is over, the Post-Incident stage involves analysing the network capture file (.pcap) to identify the attack activity and reconfigure the router to block the attacker's IP address and enhance network security.

information, timestamps, packet sizes, connection activity, and unusual traffic spikes. The combination of these two types of evidence serves as the primary basis for the Examination and Analysis phases.

Table 2 : Command Line Interface for Opening MikroTik Logs

"To open and view the log" /log print "View logs in real time" /log print follow "Display only the latest logs" /log print where topics~"info" "Display logs related to the firewall" /log print where topics~"firewall" "Display logs related to attacks or connections" /log print where message~"connection" "Clear all logs" /log clear

The MikroTik CLI commands in Table 2 are used to access and manage system logs via the Winbox terminal. The /log print command displays all router activity, while /log print follow is used to monitor logs in real time. Additionally, filters are available, such as /log print where topics~"info" for general information logs, /log print where topics~'firewall' for firewall activity, and /log print where message~"connection" to search for specific connection activities. The /log clear command is used to clear all logs before monitoring or testing begins.

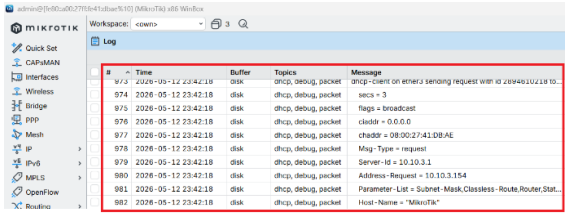

Figure 8 : Log Time, Buffer, and Topics from MikroTik

In Figure 8, the section highlighted in red in the Log window of MikroTik RouterOS Winbox displays detailed information regarding recorded DHCP activity. The Time column displays network activity occurring within a very short timeframe; a disk value in the Buffer column indicates that the log is permanently stored on the router's storage media; and the Topics column displays "dhcp," "debug," and "packet," indicating that DHCP activity is logged at the data packet level. In the Message section, details of the DHCP process are visible, such as the client's IP address (ciaddr and yiaddr), the DHCP server's address (siaddr), and the client device's MAC address (chaddr). A message with Msg-Type = ack indicates that the server has successfully confirmed the assignment of an IP address to the client, while the Server-Id, lease time, subnet mask, and domain server information record the network configuration sent during the IP allocation process, indicating that the router is intensively logging network activity and saving it as a permanent record in the system.

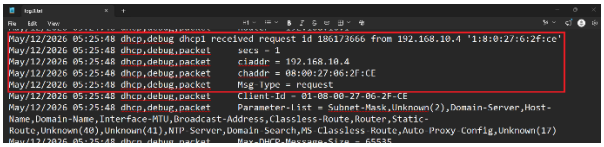

Figure 9 : Exported Mikrotik Log

In Figure 9, the timestamp May/12/2026 05:25:48 with the topics dhcp, debug, and packet in the exported log results matches the time in the Winbox log, thus proving that the .txt file is a detailed record of identical DHCP activity, marked by information such as ciaddr, chaddr, Msg-Type, and Server-Id that are recorded synchronously. In the "Message" section of the exported log results, DHCP parameters such as ciaddr, yiaddr, siaddr, chaddr, Msg-Type, Server-Id, Address-Time, Subnet-Mask, Domain-Server, and Router are visible; their contents match the logs in Winbox but are presented more comprehensively in text format. This consistency in timing and content demonstrates the reliability of RouterOS's logging mechanism in recording network activity, even across different formats, thereby reinforcing the validity of the digital evidence captured by the system.

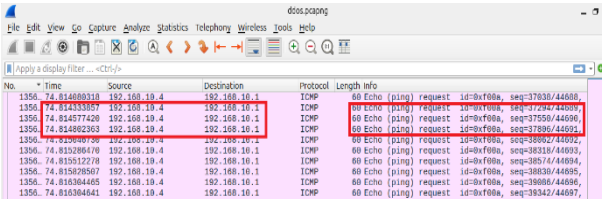

Figure 10 : Wireshark capture results for Time, Source, and Destination

In Figure 10, the time column shows packets recorded in very close time intervals, indicating rapid and consecutive data transmission, with Source IP 192.168.10.4 as the consistent sender and Destination IP 192.168.10.1 as the single destination, revealing a massive one-way communication pattern occurring simultaneously. Meanwhile, the Protocol column shows that all packets use ICMP, Length indicates a uniform packet size of 60 bytes, and the Info column shows Echo (ping) requests with continuously increasing sequence numbers, indicating the repeated, sequential transmission of a large number of ICMP Echo Requests with a consistent packet structure.

Table 3 : MD5 hashes of digital evidence

File	MD5
log.0.txt	66082F7546EA6DA229FF9F7074ADC5A2
ddos.pcapng	a90eaab57ff044b5dd45cd3b74733f7e

Table 3 shows the MD5 values of two pieces of evidence: a .pcap file captured by Wireshark and a .txt file exported from the router log. The MD5 values are used as an integrity verification method to ensure that neither file has been altered since it was first collected. By comparing the hash values, the authenticity of the data can be proven technically and objectively. The use of MD5 at this stage helps maintain the validity of the digital evidence throughout the forensic analysis process.

4.2 Examination

The examination phase involved analyzing the .pcap file using

Wireshark with an ICMP filter to display specific traffic. The results showed a sudden surge in echo request packets, indicating an attack. Additionally, the timestamps in Wireshark were compared with the MikroTik RouterOS logs to confirm that all data originated from the same attack event.

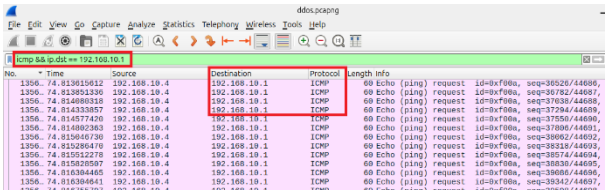

Figure 11 : Filtering of Wireshark Capture Results

In figure 11, the traffic dominated by ICMP Echo Request packets from IP 192.168.10.4 to IP 192.168.10.1, with continuously increasing sequence numbers and very short intervals. Packet details show ICMP Type 8 (Echo Request), a hallmark of an ICMP Flood attack that overloads the router's resources due to the high volume of requests being processed. This indicates a recurring attack pattern that disrupts network performance.

Figure 12 : MikroTik CPU Load

In figure 12, the results of a MikroTik RouterOS resource check via Winbox to identify abnormal activity leading to a DDoS attack. The CPU Load is seen reaching 100%, indicating the router is under heavy load due to a surge in network traffic such as an ICMP Flood, SYN Flood, or UDP Flood, while information on CPU Frequency, memory capacity, and uptime is used to support analysis of the system's condition during the attack. In the Resources view, the Free Memory value of 35.0 MiB out of a total of 64.0 MiB indicates that part of the memory has been used by system processes and network traffic. In the NIST Examination phase, this memory check is crucial for identifying the impact of DDoS attacks, which can increase memory usage, degrade system performance, and disrupt network services; thus, memory usage serves as a critical indicator in network forensic analysis of abnormal traffic activity.

4.3 Analysis

The Analysis phase is the core process of digital forensics, involving the analysis of data captured by Wireshark and MikroTik RouterOS logs to identify the patterns, sources, and impact of DDoS attacks on the network. The analysis is conducted by filtering ICMP packets to detect large volumes of repetitive Echo Request activity within a short timeframe, which indicates the characteristics of an ICMP Flood attack. The analysis results show a significant increase in ICMP traffic, causing high load on the router's CPU and memory, as well as resulting in latency, connection disruptions, and request timeouts. Additionally, a correlation is performed between Wireshark data and RouterOS logs based on timestamps, source IP addresses, protocol types, and packet patterns to confirm that the abnormal traffic originates from an ICMP Flood attack. The results of this Analysis phase serve as the basis for validating digital evidence, as well as for compiling reports and mitigation recommendations to prevent similar attacks in the future.

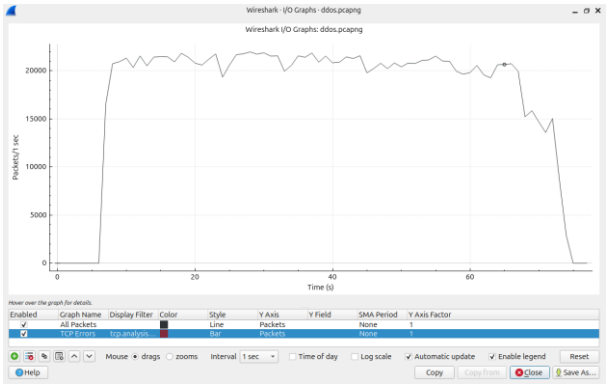

Figure 13 : Input/Output Graph from Wireshark Capture Results

In figure 13, the results of network traffic analysis using the I/O Graph feature in Wireshark during a Distributed Denial of Service (DDoS) attack. The graph shows a very high traffic spike of over 20,000 packets per second, indicating massive and continuous packet transmission that caused network overload due to an ICMP Flood attack. The stable traffic pattern over a specific period indicates flooding activity not found under normal network conditions, thus categorizing it as a DDoS attack anomaly. At the end of the graph, a drop in traffic to near zero is visible, indicating that the attack has ceased. Additionally, the appearance of TCP Errors indicates communication disruptions caused by high network traffic. The results of this graph serve as digital evidence in the Analysis phase of the National Institute of Standards and Technology (NIST) method for identifying the patterns and intensity of network attacks.

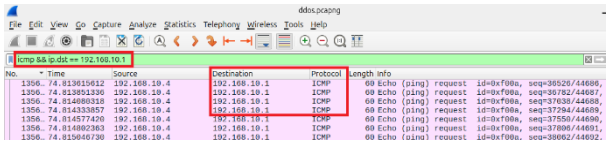

Figure 14 : Wireshark Ip Destination Filtering

In figure 14, the process of analyzing network packets using the Wireshark application during the Analysis phase of the National Institute of Standards and Technology (NIST) method. In this process, packet filtering is performed to identify anomalous traffic indicative of a Distributed Denial of Service (DDoS) attack, specifically the ICMP Flood type. The system displays only ICMP protocol packets addressed to the target IP address 192.168.10.1. This filter is used to simplify the identification of attack packets by focusing the analysis on ICMP traffic directed at the target device.

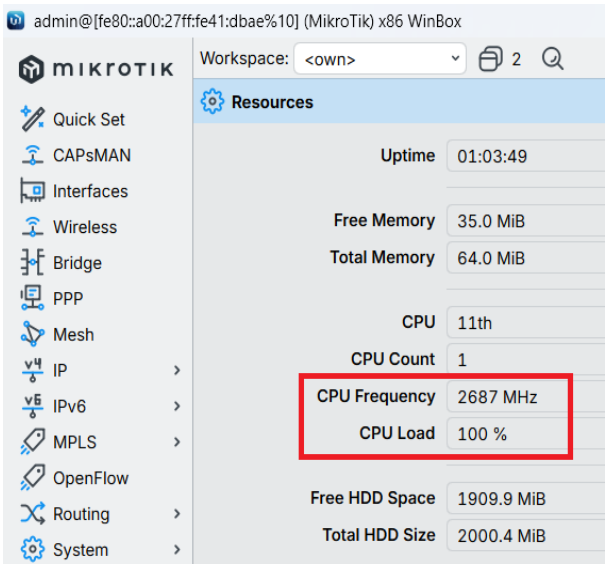

Figure 15 : MikroTik RouterOS Resources

In figure 15, the resource status on MikroTik RouterOS during a Distributed Denial of Service (DDoS) attack. The CPU Load reaches 100% as the router continuously processes a large volume of network traffic, while Free Memory stands at 35.0 MiB out of a total of 64.0 MiB, indicating system overload. Compared to normal conditions with low CPU Load and stable memory usage, a DDoS attack causes a significant increase in resource usage, leading to reduced router performance and triggering network disruptions such as unstable connections, response delays, and request timeouts.

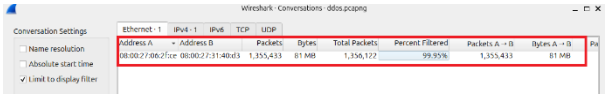

Figure 16 : Wireshark Capture Statistics – Conversations

In figure 16, the analysis results from the Conversations menu in Wireshark for the ddos.pcapng file. The capture results reveal extremely high network traffic between MAC addresses 08:00:27:06:2f:ce and 08:00:27:31:40:d3 via the IPv4 protocol, totaling approximately 1,355,433 packets with a data size of 81 MB. Of the total 1,356,122 packets analyzed, 99.95% consisted of filtered traffic relevant to the attack activity. A massive spike in traffic over a short period indicates a DDoS attack, so these analysis results aid the network forensic investigation process in identifying the source and characteristics of the attack.

4.4 Reporting

In the Reporting phase, based on the NIST framework, all findings from the collection, examination, and analysis processes are compiled into a systematic, coherent, and accountable report. This report includes a timeline from pre-incident to post-incident, accompanied by digital evidence in the form of MikroTik RouterOS firewall logs, .pcap files from Wireshark, and screenshots of Resources showing CPU Load reaching 100% and memory pressure. This section explains the identification of the attacker's IP, the target IP (router), the targeted ICMP protocol, and the pattern of massive echo requests that degraded the router's performance, leading to the logical conclusion that the service disruption was caused by an ICMP flood DDoS attack and serving as the basis for network security enhancements.

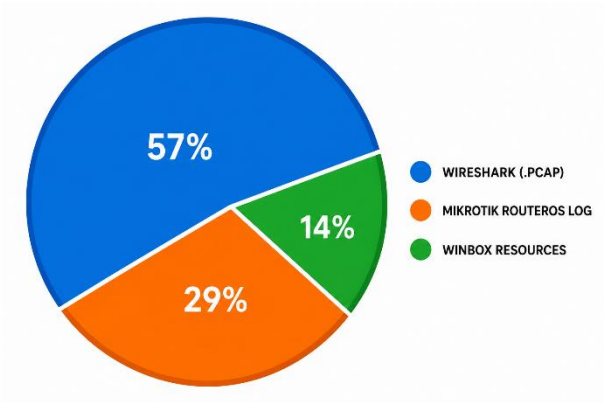

Figure 17 : Pie Chart of Findings from Digital Evidence

In figure 17, a pie chart showing the distribution of forensic evidence sources in the ICMP Flood attack investigation. A total of 57% of the findings originated from the analysis of .pcap files in Wireshark, 29% from logs in MikroTik RouterOS, and 14% from the Resources menu in Winbox, which indicated a rise in CPU load. This distribution confirms that forensic evidence is supported by a combination of several digital artifacts that reinforce each other in confirming the occurrence of an ICMP Flood DDoS attack. This result shows that packet analysis provides the most dominant contribution in identifying attack patterns and abnormal traffic behavior. At the same time, system logs and resource monitoring serve as supporting evidence that strengthens the accuracy and validity of the forensic investigation. This also improves the reliability of the investigation results.

Table 4 : Forensic Results of the ICMP Flood Attack

Source of Evidence	Observed Parameters	Findings	Notes
Wireshark capture .pcap file	Dominant protocol	ICMP	There is a very high spike in ICMP Echo Requests
File .pcap	Source IP address	192.168.10.4	This IP address has been identified as the sender of the most packets
File .pcap	Destination IP Address	192.168.10.1	The router's IP address as the target of the attack
MikroTik RouterOS logs	ICMP traffic logs	Constant requests	Impacting router performanc e
Resources Menu in Winbox	CPU Load	95–100%	Occurs during an attack
Packet statistics in Wireshark	Number of packets per second	Very high (flood)	Indicates a DDoS pattern
Log Router	Event Time	Based on the time in the .pcap file, identify DDoS patterns	Time synchroniza tion of evidence

Table 4 shows the results of the forensic analysis of the .pcap file in Wireshark, which reveals a dominance of the ICMP protocol with a surge in Echo Requests. IP 192.168.10.4 was identified as the source of the attack and 192.168.10.1 as the target (router). The logs on MikroTik RouterOS show continuous ICMP requests overloading the router, corroborated by the Resources view in Winbox showing CPU usage at 95–100%. The extremely high packet statistics and the time alignment between the router logs and the .pcap file confirm that all evidence stems from the same ICMP Flood DDoS attack method.

5. CONCLUSION

Based on the study entitled "Forensic Analysis of Distributed Denial of Service (DDoS) Attacks Using the National Institute of Standards and Technology (NIST) Methodology," it can be concluded that DDoS attacks can be effectively detected through network traffic analysis using Wireshark by employing packet sniffing and filtering techniques for ICMP, SYN, and UDP packets to identify traffic spikes, abnormal communication patterns, and incomplete connections as early indicators of an attack. The experimental results demonstrated that the ICMP Flood attack generated a significant increase in network traffic, causing the MikroTik RouterOS CPU Load to reach 95–100% and degrading overall network performance. Furthermore, the NIST digital forensics methodology, consisting of the Collection, Examination, Analysis, and Reporting phases, proved effective in systematically identifying attack patterns, packet characteristics, attack timestamps, source IP addresses, and the overall impact of the attack. The correlation between Wireshark packet captures, MikroTik RouterOS logs, router resource monitoring, and MD5 hash verification strengthened the validity and integrity of the digital evidence throughout the forensic investigation process. Therefore, the proposed approach provides a structured and reliable framework for detecting, analyzing, and documenting DDoS attacks, making it suitable for implementation in educational institutions and small-to-medium-sized organizations. Future research may extend this work by evaluating additional DDoS attack types, including SYN Flood, UDP Flood, HTTP Flood, and Slowloris, under various network environments, as well as integrating machine learning techniques with intrusion detection and prevention systems such as Snort and Suricata to improve detection accuracy and enable automated mitigation. In addition, future studies may investigate cloud-based protection services and Software-Defined Networking (SDN) approaches to provide more adaptive, scalable, and effective defense mechanisms against increasingly sophisticated DDoS attacks.

6. REFERENCES

[1] T. Aula Madina and M. Fadhli, "Analisis Serangan DDOS pada Website Prodi Pendidikan Teknologi Informasi," Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 7, no. 6, 2024.

[2] R. Albar, M. Bayu Wibawa, and I. Tawakalna, "Point to Point Network Performance Analysis in Video Live Streaming Activities Based on QOS (Quality of Service) Method on Ubontv Television," Journal of Informatics and Computer Science, vol. 9, no. 1, 2023.

[3] M. R. Hidayat, R. Saragih, S. Basuki, A. Charisma, and A. D. Setiawan, "Implementasi Threat Mitigation dan Traffic Policy Menggunakan UTM pada Jaringan Tcp/Ip," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 11, no. 2, pp. 437–446, Aug. 2024, doi: 10.25126/jtiik.20241127528.

[4] B. D. Ramanda, D. Irawan, and A. Hidayat, "Rancang Bangun Manajemen Bandwidth Menggunakan Metode Simple Queue Mikrotik Router pada SMK N 1 Trimurjo," vol. 5, no. 1, pp. 86–95, 2024.

[5] A. M. Alhimni, "Analisis Kualitas Jaringan Internet Menggunakan Parameter Quality Of Service di Kecamatan Bangkalan," Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 7, no. 6, 2024.

[6] J. Natada, T. Hidayat, and Z. Zainal, "Optimasi Jaringan Wireless pada Jaringan Akses Fakultas Teknik Universitas Serambi Mekkah Menggunakan Virtual Access Point," Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 7, no. 3, 2024.

[7] S. Nawawi et al., "Implementasi Access Control List (ACL) pada Perangkat MikroTik untuk Mengamankan Koneksi Jaringan Internet di SMK Nurusshaleh Kato Timur," Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 7, no. 4, 2024.

[8] H. P. Fitrian, S. Sopian Nudiansyah, M. R. Raihan, R. Faturohman, and A. Antareza, "Efektivitas SNORT Sebagai Sistem Deteksi Intrusi pada Berbagai Macam Pola Serangan Siber," Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 7, no. 6, 2024.

[9] N. Saputri, M. Nasir, and I. Safar, "JAISE : Journal of Artificial Intelligence and Software Engineering Analisis Kualitas pada Video Streaming Pembelajaran Menggunakan Metode Differentiated Service."

[10] N. Umah, F. A. Yudanto, and E. Rilvani, "Evaluasi Segmentasi VLAN dalam Optimalisasi Kinerja dan Keamanan pada Jaringan LAN di Universitas Pelita Bangsa."

[11] S. Sahren, R. A. Dalimunthe, H. Saputra, and D. Y. Kurnia Sirni, "IDPS Performance Analysis for Mitigating SQL Injections and Syn Flood Attacks," JURTEKSI (Jurnal Teknologi dan Sistem Informasi), vol. 10, no. 1, pp. 171–178, Dec. 2023, doi: 10.33330/jurteksi.v10i1.2880.

[12] R. D. Hapsari and K. G. Pambayun, "Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis," Jurnal Konstituen, vol. 5, no. 1, pp. 1–17, Oct. 2023, doi: 10.33701/jk.v5i1.3208.

[13] M. Luthfi Arsalan and H. Teja Sukmana, "Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt. Akurat.Co)," 2023.

[14] A. Kadam, "SDN-Driven Security Framework for DDOS Attack Detection and Mitigation," Int. J. Res. Appl. Sci. Eng. Technol., vol. 12, no. 11, pp. 620–625, Nov. 2024, doi: 10.22214/ijraset.2024.65142.

[15] D. F. Tanjung, O. Dwi Nurhayati, and A. Wibowo, "Design Information Security in Electronic-Based Government Systems Using NIST CSF 2.0, ISO/IEC 27001: 2022 and CIS Control," International Journal of Innovative Science and Research Technology (IJISRT), pp. 523–530, Jun. 2024, doi: 10.38124/ijisrt/ijisrt24jun1212.

[16] S. Suharti, A. Yudhana, and I. Riadi, "Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary," MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 21, no. 3, pp. 567–582, Jul. 2022, doi:

10.30812/matrik.v21i3.1732.

[17] Sukma Aji, Davito Rasendriya Rizqullah Putra, I. Riadi, A. Fadlil, and M. N. Faiz, "A Classification Data Packets Using the Threshold Method for Detection of DDoS," Journal of Innovation Information Technology and Application (JINITA), vol. 6, no. 1, pp. 28–36, Jun. 2024, doi: 10.35970/jinita.v6i1.2224.

[18] H. Wintolo, I. Riadi, and A. Yudhana, "Analisis Deteksi Penyusup pada Layanan Open Journal System Menggunakan Metode Network Forensic Development Life Cycle," SKANIKA: Sistem Komputer dan Teknik Informatika, vol. 8, no. 1, pp. 133–144, 2025.

[19] R. Indraguna, U. A. Dahlan, and I. Riadi, "Web Server Security Analysis from DDoS Attack using Information Systems Security Assessment Framework Method," 2021.

[20] Gregorius Hendita Artha Kusuma, "Sistem Firewall untuk Pencegahan DDoS Attack di Masa Pandemi Covid-19," Journal of Informatics and Advanced Computing (JIAC), vol. 3, May 2022, doi: https://doi.org/10.35814/jiac.v3i1.3853.

[21] D. Tymoshchuk, O. Yasniy, M. Mytnyk, N. Zagorodna, and V. Tymoshchuk, "Detection and classification of DDoS flooding attacks by machine learning method," 2024.

[22] Junirma Buttu, "Analisis Kinerja Jaringan Wlan pada Sekolah Menengah Pertama Negeri 6 Palopo," Jurnal Informatika dan Teknologi Komputer, vol. 01, no. 01, 2023, doi: https://doi.org/10.53769/bandwidth.v1i1.380.

[23] Herman, K. O. Haris, Handrawan, A. S. Abdullah, A. Rizyky, and R. S. Indah, "Penggunaan Digital Forensik dalam Pembuktian Tindak Pidana Pencemaran Nama Baik di Media Sosial Berdasarkan UU ITE," Halu Oleo Legal Research, vol. 6, no. 2, 2024, doi: https://doi.org/10.33772/holresch.v6i2.788.

[24] E. Setiawan and Hartiwiningsih, "Pemanfaatan Digital Forensik dan Teknologi Informasi Dalam Proses Pembuktian Tindak Pidana Pemalsuan Dokumen Elektronik," Prosiding Seminar Nasional Ilmu Hukum, vol. 1, no. 2, pp. 179–193, 2024, doi: 10.62383/prosemnashuk.v1i2.39.

[25] N. Abidin, "Optimalisasi Firewall pada Jaringan Komputer Berskala Luas," JSI (Jurnal Sistem Informasi) Universitas Suryadarma, vol. 1, no. 1, 2021, doi: https://doi.org/10.35968/jsi.v1i1.36.

[26] W. Agustiono, D. Wulan Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," Jurnal Teknologi dan Informasi (JATI), vol. 14, 2024, doi: 10.34010/jati.v14i2.

[27] H. Wintolo, I. Riadi, and A. Yudhana, "Enhancing Private Cloud Security Using Knowledge Understanding Assessment Defense Method for Distributed Denial of Service Attack Mitigation," International Journal of Safety and Security Engineering, vol. 15, no. 11, pp. 2323–2331, Dec. 2025, doi: 10.18280/ijsse.151112.