

Restorative network forensics for mitigating goldenEye DDoS attacks on owncloud services using the KUAD method

HERO WINTOLO,^{1*} PETRUS KANISIUS DHADO,² IMAM RIADI,³ ANTON YUDHANA,⁴ SUDARYANTO,⁵ AND ARIS RAKHMADI⁶

Abstract

GoldenEye attacks against an OwnCloud service. A controlled test environment was deployed using OwnCloud on Ubuntu Server 22.04 with Apache2. Network traffic was acquired using Wireshark, while application-layer events were obtained from the Apache access log. Digital evidence was cross-validated at the event level using source IP address, HTTP method, base endpoint, response status, and temporal proximity. The validated attack sources were subsequently blocked using iptables, and mitigation effectiveness was assessed from the change in observed attack activity. Wireshark captured 9,379 attack-related records from three source IP addresses, whereas the access log contained 8,864 candidate HTTP 400 records. A total of 8,853 records were validated, yielding an overall validation rate of 99.88%; the source-specific rates were 100.00%, 100.00%, and 99.60%. The median timestamp difference was 0 seconds, the mean absolute difference was approximately 0.21 seconds, and 97.24% of validated records occurred within ± 1 second. All validated events involved HTTP GET requests to the /OwnCloud/index.php base endpoint and produced HTTP 400 responses. Following iptables-based blocking, the observed attack activity from the identified sources decreased by 100%. These findings demonstrate that KUAD can connect cross-source forensic validation with measurable defensive action and service restoration in a controlled OwnCloud environment.

Keywords

GoldenEye, KUAD, ownCloud, network forensics, iptables

Article History

Received 16 July 2026

Accepted 28 September 2026

How to Cite

Wintolo, H., Dhado, P. K., Riadi, I., Yudhana, A., Sudaryanto, & Rakhmadi, A. (2026). Restorative network Forensics for Mitigating goldenEye DDoS attacks on ownCloud Services Using the KUAD Method. *Jurnal Jaringan Komputer dan Keamanan*, 7(2), 01-13. <https://doi.org/10.61346/jjk.k.v7i2.380>

^{1*} Institut Teknologi Dirgantara Adisutjipto, Indonesia, Corresponding email: herowintolo@itda.ac.id

^{2,5} Institut Teknologi Dirgantara Adisutjipto, Indonesia

^{3,4} Universitas Ahmad Dahlan, Indonesia

⁶ Universitas Muhammadiyah Surakarta, Indonesia

Introduction

The development of cloud computing services has encouraged the increasing adoption of private cloud environments as platforms for independent data storage, collaboration, and management. OwnCloud is one of the most widely used services in private cloud environments because it provides flexible access to data over a network. However, the open accessibility of web-based services also introduces security risks, particularly Distributed Denial-of-Service (DDoS) attacks. DDoS attacks can overwhelm a server with a massive volume of requests, resulting in degraded service performance, increased network traffic, unstable server responses, and potentially complete service failure.

Previous studies have not specifically addressed restorative network forensics to mitigate DDoS attacks on OwnCloud services (Qureshi et al., 2021). In addition, evaluations of forensic tools have rarely focused on GoldenEye attack scenarios, accompanied by validation against server logs (Barik et al., 2021). Several studies have also failed to integrate detection, validation, mitigation, and service recovery into a unified process (Ghabban et al., 2021). Research focusing on model-based detection generally has not treated digital evidence, cross-validation between Wireshark and access.log, and mitigation using Iptables as central components of the analysis (Alghazzawi et al., 2021). The disposition of digital evidence and post-attack restorative measures have also received limited attention in most previous studies (Shieh et al., 2021). Some mitigation approaches have employed blockchain technology, but they have not been based on the validation of digital evidence obtained from Wireshark and access.log (Wani et al., 2021). Other studies have continued to emphasize detection model performance and, therefore, have not developed a restorative forensic framework that links digital evidence to recovery actions (Kushwah and Ranga, 2021). Accordingly, a research gap remains in the use of validated digital evidence as the basis for IP address blocking in the mitigation of GoldenEye DDoS attacks on OwnCloud services (Amrullah, 2025).

Previous studies have largely discussed computer forensics in general and have not specifically addressed the analysis of GoldenEye DDoS attacks on OwnCloud services (Javed et al., 2022). Studies involving OwnCloud have also not applied the KUAD method or emphasized restorative mitigation using Iptables (Damayanti and Hikmah, 2022). Furthermore, digital evidence acquisition and cross-source data validation have rarely been treated as central components of the network forensic analysis process (Danang et al., 2025). Although several studies have examined attack mitigation through bandwidth allocation, these approaches have not been based on forensic evidence or validated IP address blocking (Danang et al., 2025). Other studies have also placed limited emphasis on digital evidence derived from server status codes and on service recovery procedures following an attack (Akgun, Hizal and Cavusoglu, 2022). Research focusing on intrusion detection systems generally emphasizes detection accuracy and has not comprehensively integrated the KUAD method with post-attack mitigation (Sanjalawe and Althobaiti, 2023). In addition, some studies have not specifically examined OwnCloud or private cloud environments, with evidence validation between Wireshark and access.log (Haseeb-ur-rehman et al., 2023). Therefore, a research gap remains in evaluating a restorative mechanism that blocks IP addresses using validated digital evidence to address GoldenEye DDoS attacks on OwnCloud services (Mahdavi Hezavehi and Rahmani, 2023).

Several previous studies have employed Moving Target Defense (MTD) and machine learning (ML) approaches; however, they have neither implemented the KUAD method nor emphasized server log validation as part of the forensic process (Ribeiro, Pereira Fonseca and de Santi, 2023). In addition, the acquisition, validation, and disposition of digital evidence have not been comprehensively addressed throughout the attack-handling process (Kumar and Somani, 2023). Some studies have primarily focused on Software-Defined Networking (SDN) environments and, therefore, have not specifically examined OwnCloud or private cloud services, nor implemented service recovery using iptables (Mansoor et al., 2023). Other studies have also not investigated GoldenEye attacks or the use of evidence obtained from the OwnCloud server's access.log file (Yungaicela-Naula et al., 2023). Several studies have remained broad in scope and have not demonstrated the direct implementation of the KUAD method in an OwnCloud environment (Ouhssini et al., 2024). Research focusing on attack detection and prevention has also not treated digital evidence validation and forensic disposition as essential components of the incident-handling process (Ouhssini et al., 2024). The SDN environments used in several studies differ from the context of OwnCloud services; consequently, iptables-based mitigation supported by digital evidence has not received sufficient attention (Alashhab et al., 2024). Previous research demonstrated that an iptables-based firewall substantially reduced Ping of Death traffic in an SDN environment from 1.021 million to 8.34 thousand packets per second. However, the research focused primarily on traffic suppression and did not integrate cross-source digital evidence validation, forensic analysis, or restorative incident handling in an OwnCloud environment (Saputra, 2021). Studies focusing on SDN-enabled Internet of Things (IoT) environments have likewise not addressed the security requirements of private cloud services or examined the implementation of the KUAD method (Singh and Jain, 2024). Therefore, a research gap remains in evaluating GoldenEye DDoS attacks against OwnCloud using the KUAD approach, which integrates digital evidence validation, server log analysis, and technical mitigation based on iptables (Malik et al., 2024).

The solution proposed in this research is the implementation of the Knowledge Understanding Assessment Defense (KUAD) method as a restorative network forensics approach to address GoldenEye DDoS attacks against OwnCloud services. This method integrates attack detection, evidence acquisition, cross-source data validation, attack impact analysis, mitigation, and documentation of incident-handling outcomes. Unlike conventional network forensics approaches that primarily focus on identifying and reporting digital evidence, the KUAD approach in this research is designed to enable measurable defensive actions by blocking attacker IP addresses with iptables.

This research aims to develop the implementation of the KUAD method as a restorative network forensics approach for handling GoldenEye DDoS attacks on OwnCloud services. It is intended to acquire digital evidence from network traffic and server logs, validate the consistency of evidence obtained from Wireshark and access.log, quantitatively analyze the intensity and impact of the attacks, and implement a mitigation mechanism using iptables. In addition, this research aims to evaluate the effectiveness of the mitigation process based on the reduction in attack activity following IP address blocking.

Methodology

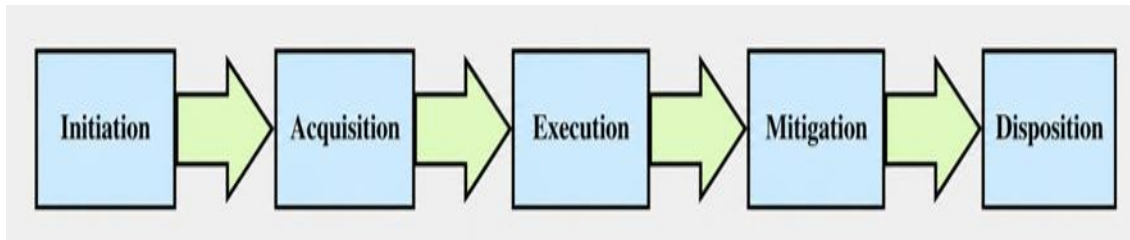
A review of related work was conducted to strengthen the methodological foundation, establish the research position, and demonstrate the continuity of the methodological development adopted in this research. This research does not stand as an isolated investigation; rather, it builds upon several previous studies addressing network forensics, attack detection, digital evidence validation, post-attack mitigation, and the implementation of the KUAD method across various digital service environments. Therefore, this section highlights the relationship between previous studies and the research design developed to investigate GoldenEye DDoS attacks on OwnCloud services.

Previous research investigated intrusion detection in the Open Journal Systems service using the Network Forensics Development Life Cycle (NFDLC) method. The research provided an initial foundation for understanding the network forensics workflow, particularly the initiation, acquisition, implementation, operation, and disposition stages. Its primary contribution was the use of a forensic approach to identify intrusion activity using network data and system logs. These findings serve as an important foundation for the present research, particularly in the acquisition and validation of attack evidence using Wireshark and access.log (Wintolo, Riadi and Yudhana, 2025b).

Subsequent research developed a post-attack approach for the Open Journal Systems service using the Knowledge Understanding Assessment Defense (KUAD) method. The research demonstrated that the forensic process should not end with the identification and reporting of digital evidence but should be followed by mitigation measures. This concept provides an essential basis for the present research because GoldenEye DDoS attacks are not only analyzed from a digital evidence perspective but also addressed by blocking attacker IP addresses using iptables as a defensive and service-recovery measure (Wintolo, Riadi and Yudhana, 2025c).

Another study implemented the KUAD method to improve the security of private clouds against Distributed Denial-of-Service (DDoS) attacks. This research is directly related to the present research because both use private cloud services as the testing environment and focus on DDoS attacks. However, the present research specifically evaluates GoldenEye attacks on OwnCloud services and incorporates quantitative analyses, including the digital evidence validation rate, the contribution of each attacker IP address, the prevalence of the HTTP 400 status code, the attack rate, and mitigation effectiveness (Wintolo, Riadi and Yudhana, 2025a). Furthermore, the KUAD method has also been used to conduct forensic analysis of Trojan backdoor attacks in a private cloud environment. The research demonstrated that KUAD can be applied not only to DDoS attacks but also to other types of attacks targeting private cloud environments. This finding reinforces the flexibility of the KUAD method as a network forensics approach for understanding attack characteristics, assessing their impacts, and determining appropriate defensive measures (Wintolo et al., 2026).

Figure 1. *KUAD Method*



Based on the related studies discussed above, this research adopts the KUAD method, as illustrated in Figure 1, as the primary approach for conducting forensic analysis of the restorative network of GoldenEye DDoS attacks against OwnCloud services. Previous studies have provided a conceptual foundation concerning the NFDLC method, digital evidence validation, post-attack mitigation, and private cloud security. This research extends those efforts by emphasizing the quantitative evaluation of mitigation effectiveness, including a 100% digital evidence validation rate, the dominance of the HTTP 400 status code as an attack indicator, the identification of three attacker IP addresses, and a 100% reduction in attack activity following the implementation of IP address blocking using iptables. Therefore, this research contributes to strengthening the implementation of KUAD as a network forensics method that is not only investigative but also restorative and quantitatively measurable.

Results and Discussion

The testing environment in this research was designed to support the simulation, acquisition, validation, monitoring, and mitigation of GoldenEye attacks on the OwnCloud service. Each component served a specific function to ensure that the testing process was conducted systematically, including the provision of the target server, network connectivity, monitoring devices, and network forensic tools. The components, specifications, and functions of each device are presented in Table 1.

Table 1. *Testing environment for goldeneye attacks on owncloud*

No	Components	Specifications	Functions
1	Server	Ubuntu Server 22.04, Apache2, OwnCloud	Attack target
2	Router	Mikrotik CCR1016-12G	Network interconnection
3	Monitoring computer	Kali Linux 2025.1	Network traffic acquisition
4	Tools	Wireshark, Ettercap, access.log, nload, Iptables	Acquisition, validation, monitoring, and mitigation

Table 1 presents the main components used in the GoldenEye attack testing environment. The Ubuntu Server 22.04 system, running Apache2 and OwnCloud, served as the attack target. The MikroTik CCR1016-12G router served as the network interconnection device, while the monitoring computer running Kali Linux 2025.1 was used to acquire traffic. Several tools,

including Wireshark, Ettercap, access.log, nload, and iptables, supported data acquisition, evidence validation, traffic monitoring, and attack mitigation. The characteristics of the GoldenEye attack before mitigation were analyzed based on network traffic captured using Wireshark and the Apache2 access log file. The observed data included the attacker IP addresses, attack timestamps, HTTP methods, accessed target URLs, and server-generated status codes. The detailed characteristics of the attack before mitigation are presented in Table 2.

Table 2. *Characteristics of the goldeneye attack before mitigation*

No.	Attacker IP Address	Attack Time	HTTP Method	Target URL	Status Code	Data Source
1	140.213.174.152	18:04–18:05	GET	/OwnCloud/index.php	400	Wireshark dan access.log
2	140.213.172.203	18:04–18:05	GET	/OwnCloud/index.php	400	Wireshark dan access.log
3	36.72.217.84	18:05	GET	/OwnCloud/index.php	400	Wireshark dan access.log

Table 2 shows that the GoldenEye attack originated from three IP addresses: 140.213.174.152, 140.213.172.203, and 36.72.217.84. All three IP addresses sent HTTP GET requests to the /OwnCloud/index.php endpoint within a closely spaced time interval. All activities resulted in an HTTP 400 status code, indicating abnormal or invalid requests to the server. The consistency between the Wireshark data and the access.log records confirms that these three IP addresses were the sources of the attack activity before mitigation was implemented.

The attack evidence was validated by comparing the data captured by Wireshark with the Apache2access.logfile. This validation process aimed to ensure that the IP addresses detected in the network traffic were also recorded in the server logs at the corresponding times. The validation parameters included the timestamp, the source IP address, and the consistency of records across both data sources. The results of the attack evidence validation based on Wireshark.

To evaluate the consistency of the acquired network evidence, the Wireshark packet-capture records were compared with the corresponding web-server access-log entries. The comparison focused on traffic originating from the identified GoldenEye attack IP addresses, while the access-log analysis was limited to HTTP responses with status code 400. The matching process produced a validated dataset, as summarized in Figure 2.

Figure 2. *Summary of wireshark attack records, access-log HTTP 400 records, validated records, and validation rate*

Wireshark attack records 9.379	Access-log HTTP 400 records 8.864	Validated records 8.853	Validation rate 99,88%
-----------------------------------	--------------------------------------	----------------------------	---------------------------

Figure 2 shows that Wireshark recorded 9,379 attack-related network packets, whereas the access log contained 8,864 HTTP 400 records associated with the identified attack sources. The validation process successfully matched 8,853 records, corresponding to a validation rate of 99.88%. Only 11 access-log records were not matched during the validation process, indicating a very high level of consistency between the network-layer evidence acquired using Wireshark and the application-layer evidence recorded in the web-server access log.

To examine the consistency of attack evidence across different data sources, the numbers of records obtained from Wireshark, the web-server access log, and the validation process were compared according to the identified source IP addresses. This comparison provides a source-specific assessment of the correspondence between network-layer traffic captured by Wireshark and application-layer activities recorded in the access log, as presented in Figure 3.

Figure 3. *Comparison of Wireshark, Access-Log, and Validated Attack Records by Source IP Address*

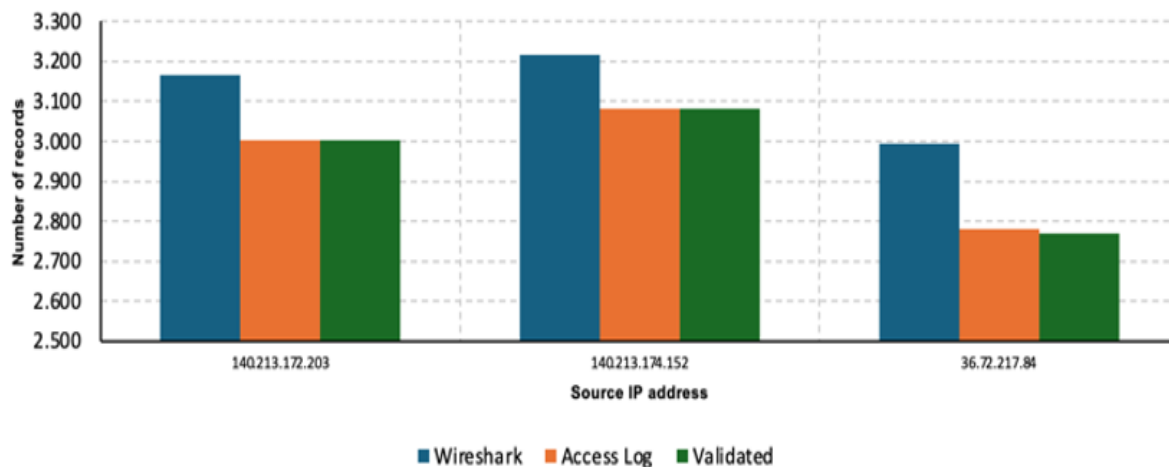


Figure 3 shows that the source IP address 140.213.174.152 generated the highest number of records, consisting of 3,218 Wireshark records and 3,081 access-log records, all of which were successfully validated. The IP address 140.213.172.203 produced 3,167 Wireshark records and 3,003 access-log records, with all access-log records also successfully validated. Meanwhile, the IP address 36.72.217.84 generated 2,994 Wireshark records and 2,780 access-log records, of which 2,769 were validated. These results demonstrate a high degree of consistency between the Wireshark acquisition data and the web-server access-log evidence for all three attack sources, although 11 access-log records associated with 36.72.217.84 were not matched during the validation process.

To examine the temporal distribution of the detected GoldenEye attack, the Wireshark acquisition records, web-server access-log entries, and validated records were aggregated at one-minute intervals. This comparison illustrates changes in attack intensity over time and evaluates the consistency between network-layer and application-layer evidence, as shown in Figure 4.

Figure 4. Minute-by-Minute Comparison of Wireshark, Access-Log, and Validated Attack Records

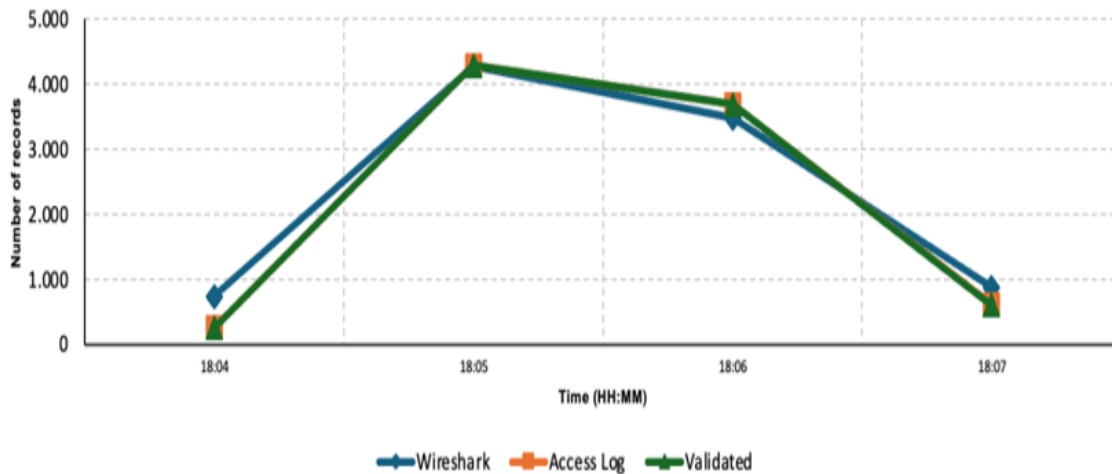


Figure 4 shows that the attack activity increased sharply from 18:04 to its highest level at 18:05. At 18:04, Wireshark captured 740 records, while the access log and validated dataset each contained 260 records. The highest activity occurred at 18:05, with 4,282 Wireshark records and 4,292 records in both the access log and validated dataset. The number of records then decreased at 18:06 to 3,480 in Wireshark and 3,690 in both the access log and validated data. At 18:07, the activity declined further to 877 Wireshark records, 622 access-log records, and 611 validated records. The nearly overlapping access-log and validation curves indicate a high level of agreement between the application-layer evidence and the validation results, with only 11 unmatched records occurring at 18:07.

The impact of the GoldenEye attack on server performance was analyzed using several key indicators, including the number of HTTP requests, the dominant status code, the presence of attacker IP addresses, server responses, and network traffic conditions. These indicators were used to describe the server's condition before mitigation and to determine the extent of disruption caused by the attack on the OwnCloud service. Details of the impact of the GoldenEye attack on server performance are presented in Table 3.

Table 3. Impact of the GoldenEye Attack on Server Performance

No.	Indicators	Condition Before Mitigation
1	Number of HTTP requests	Very high
2	Dominant status code	400 Bad Request
3	Attacker IP addresses	Detected
4	Server response	Slow or unstable
5	Network traffic	Increased significantly

Table 3 shows that, prior to mitigation, the server experienced a significant increase in workload due to the GoldenEye attack. This condition is reflected in the very high number of HTTP requests, the dominance of the HTTP 400 Bad Request status code, and the detection

of several attacker IP addresses in the network traffic. These conditions caused the server response to become slow and unstable. In addition, network traffic increased significantly because the server had to process many requests within a short period. These findings indicate that the GoldenEye attack directly contributed to the degradation of OwnCloud service performance before the IP blocking mechanism was implemented.

The comparison of attack activity before and after mitigation was visualized using a radar chart to illustrate differences in data patterns across four observation sources. This visualization compares the Wireshark data and log file before mitigation and the Wireshark data and log file after mitigation, for several IP addresses identified during testing. The radar chart is presented in Figure 5.

Figure 5. *Data distribution before and after mitigation*

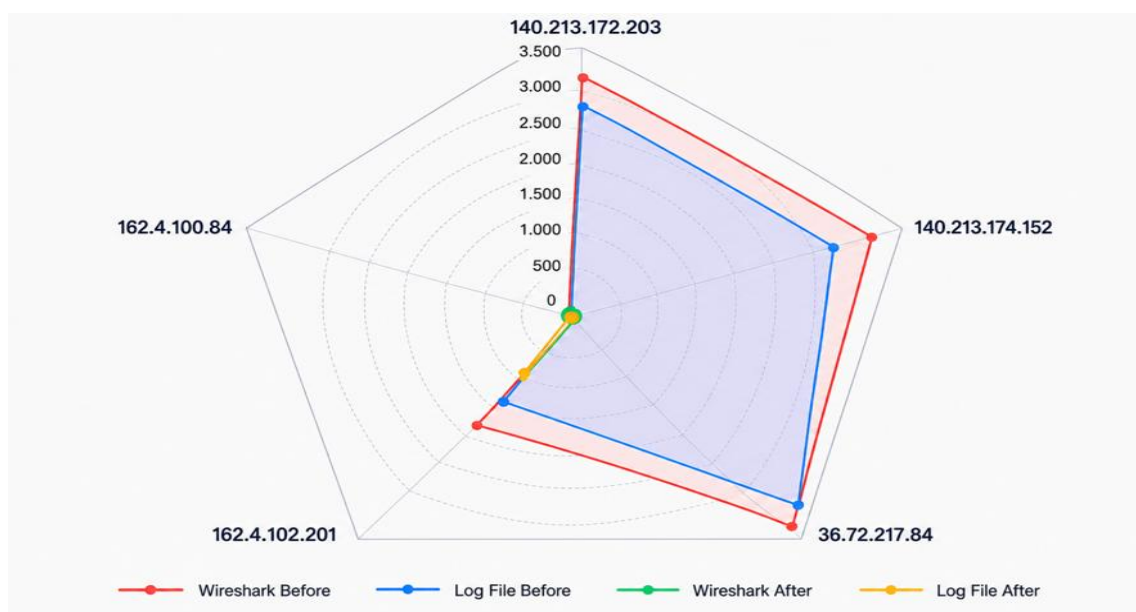


Figure 5 shows that attack activity before mitigation was high for several attacker IP addresses, particularly 140.213.172.203, 140.213.174.152, and 36.72.217.84. This pattern is represented by the red and blue lines, which indicate the Wireshark and log file data before mitigation, respectively. After mitigation was implemented, the green and yellow lines were positioned very close to the center of the chart, indicating a substantial reduction in attack activity. These results demonstrate that IP address blocking successfully suppressed attacks associated with the HTTP 400 status code, achieving a 100% reduction.

The validation process compared the network traffic acquired using Wireshark with the web-server access-log records, producing the validated records presented. Data from wireshark contains 9,740 captured records, of which 9,379 originated from the three identified GoldenEye attack sources. Data from acces log contains 9,228 access-log entries, including 8,864 candidate attack records characterized by the same source IP addresses, the HTTP GET method, requests to the /owncloud/index.php/ endpoint, and the HTTP 400 response code. A total of 8,853 records were included, resulting in an overall access-log validation rate of 99.88%; see Table 4.

Table 4. *Validation results of wireshark acquisition data against access-log records by source ip address*

Source IP address	Wireshark	Access log	Validated	Validation rate
140.213.172.203	3,167	3,003	3,003	100.00%
140.213.174.152	3,218	3,081	3,081	100.00%
36.72.217.84	2,994	2,780	2,769	99.60%
Total	9,379	8,864	8,853	99.88%

The source-specific results demonstrate that all 3,003 access-log records associated with IP address 140.213.172.203 and all 3,081 records associated with 140.213.174.152 were successfully validated. For IP address 36.72.217.84, 2,769 of 2,780 access-log records were validated, leaving only 11 unmatched records. These unmatched records occurred during the final observation period at approximately 18:07. Consequently, the small validation gap was concentrated in a single source IP address and did not affect the overall identification of the attack pattern. Compared with the 9,379 attack-related Wireshark records, validated data represents 94.39% of the acquisition records. The difference between Wireshark and access-log record counts is reasonable because packet-level network acquisition may contain requests or transmissions that do not generate separate application-layer log entries.

The temporal comparison also indicates strong consistency between the two evidence sources. The median difference between the Wireshark timestamp and the corresponding access-log timestamp was 0 seconds, while the mean absolute timestamp difference was approximately 0.21 seconds. A total of 7,374 records, or 83.29%, occurred within the same second; 8,609 records, or 97.24%, were within ± 1 second; and all validated records were within a maximum difference of ± 5 seconds. This close temporal alignment indicates that the network-layer activity captured by Wireshark corresponded closely with the application-layer requests recorded by the web server.

In terms of forensic attributes, all records in data validated consistently contain the HTTP GET method, the /owncloud/index.php/base endpoint, one of the three identified attacker IP addresses, and the HTTP 400 response code. Although only 20 records had exactly identical complete URLs between the Wireshark information field and the access-log URL, the base endpoint matched in all 8,853 records. This condition is consistent with GoldenEye attack behavior, which generates randomized query parameters for repeated requests. Therefore, the validation was primarily established through source IP address, request method, base URL, response status, and temporal proximity rather than through an exact comparison of the randomized query strings.

A structural examination of the validated data shows that the 8,853 rows represent 8,853 distinct access-log events but are associated with 315 unique Wireshark source-IP and timestamp signatures. These signatures cover 315 of the 328 active source-IP-per-second groups identified in data from Wireshark, equivalent to 96.04% temporal-group coverage. Thus, the results should be interpreted as an event-level validation using representative Wireshark records within a defined temporal interval, rather than as 8,853 independent one-to-one packet matches.

Overall, the validation results demonstrate a very high degree of agreement between the Wireshark acquisition data and the web-server access log. The 99.88% validation rate, consistent attack attributes, and close timestamp alignment support the reliability of the data

as validated digital evidence of the GoldenEye attack. Nevertheless, the reporting should clearly state that the matching process was conducted at the source-IP, endpoint, and temporal-group levels, particularly because the randomized query strings prevented strict one-to-one matching of complete request URLs.

Conclusion

This research demonstrates that the KUAD method can be implemented as a restorative network forensics workflow for detecting, validating, analyzing, and mitigating GoldenEye DDoS attacks against the OwnCloud service. Wireshark captured 9,379 attack-related records from three source IP addresses, while the web-server access log contained 8,864 candidate HTTP 400 records. Of these, 8,853 records were validated, yielding an overall validation rate of 99.88%. The source-specific validation rates were 100.00% for 140.213.172.203 and 140.213.174.152 and 99.60% for 36.72.217.84, with only 11 unmatched access-log records. The temporal evidence was also closely aligned, with a median timestamp difference of 0 seconds, a mean absolute difference of approximately 0.21 seconds, and 97.24% of validated records occurring within plus or minus 1 second. All validated events consistently involved the HTTP GET method, the /OwnCloud/index.php base endpoint, one of the three identified source IP addresses, and the HTTP 400 response code. After iptables-based blocking was applied, the observed attack activity associated with these sources decreased by 100%, indicating that validated forensic evidence can provide a reliable basis for measurable defensive action and service restoration.

The findings should nevertheless be interpreted within the scope of the experimental design. The evaluation was conducted in a controlled simulation involving a single GoldenEye scenario, three identified source IP addresses, and one OwnCloud endpoint; therefore, the results do not represent the full diversity and scale of DDoS attacks in operational environments. In addition, the validation process was performed at the source-IP, request-method, base-endpoint, response-status, and temporal-group levels rather than as a strict one-to-one packet-to-log match because GoldenEye generated randomized query strings. The reliability of this process also depends on accurate time synchronization between monitoring and server systems. Furthermore, static iptables rules can block previously identified sources but may be less effective against attacks using rapidly changing, spoofed, or widely distributed IP addresses.

Future research should evaluate KUAD in larger and more realistic environments using diverse attack types, including HTTP floods, SYN floods, and slow HTTP attacks, as well as a greater number of distributed sources. The mitigation stage should be extended through automated detection, dynamic rule updates, rate limiting, and integration with intrusion detection or prevention systems. Evaluation should also include CPU utilization, memory consumption, bandwidth use, response time, packet loss, service availability, false-positive rates, and recovery time. These extensions would allow the KUAD method to be assessed not only as a forensic investigation procedure but also as an adaptive and sustainable framework for evidence-based mitigation and recovery.

Disclosure Statement

No potential conflict of interest was reported by the authors.

References

Akgun, D., Hizal, S. and Cavusoglu, U. (2022) "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity," *Comput. Secur.*, 118(C), doi: [10.1016/j.cose.2022.102748](https://doi.org/10.1016/j.cose.2022.102748)

- Alashhab, A.A. *et al.* (2024) “Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model,” *IEEE Access*, 12, pp. 51630–51649, doi: [10.1109/ACCESS.2024.3384398](https://doi.org/10.1109/ACCESS.2024.3384398)
- Alghazzawi, D. *et al.* (2021) “Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection,” *Applied Sciences (Switzerland)*, 11(24), doi: [10.3390/app112411634](https://doi.org/10.3390/app112411634)
- Amrullah, A. (2025) “Lightweight Edge-Based Security System Design for DDoS Attack Mitigation in Industrial IoT Infrastructure,” *Intellithings Journal is a scientific research-based informatics journal* [Preprint], (1).
- Barik, K. *et al.* (2021) “Exploring user requirements of network forensic tools,” *Global Transitions Proceedings*, 2(2), pp. 350–354, doi: [10.1016/j.gltp.2021.08.043](https://doi.org/10.1016/j.gltp.2021.08.043)
- Damayanti, T.H. and Hikmah, I.R. (2022) “Network Forensic Serangan DoS pada Jaringan Cloud berdasarkan Generic Framework for Network Forensics (GFNF),” *Edumatic: Jurnal Pendidikan Informatika*, 6(2), pp. 334–343, doi: [10.29408/edumatic.v6i2.6466](https://doi.org/10.29408/edumatic.v6i2.6466)
- Danang Danang, Eko Siswanto and Nuris Dwi Setiawan (2025) “Hybrid Zero Trust Container Based Model for Proactive Service Continuity under Intelligent DDoS Attacks in Cloud Environment,” *International Journal of Computer Technology and Science*, 2(3), pp. 41–49, doi: [10.62951/ijcts.v2i3.291](https://doi.org/10.62951/ijcts.v2i3.291)
- Danang Danang, Indra Ava Dianta and Agustinus Budi Santoso (2025) “Hybrid CNN GRU Framework for Early Detection and Adaptive Mitigation of DDoS Attacks in SDN using Image Based Traffic Analysis,” *International Journal of Information Engineering and Science*, 2(2), pp. 57–70, doi: [10.62951/ijies.v2i2.292](https://doi.org/10.62951/ijies.v2i2.292)
- Ghabban, F.M. *et al.* (2021) “Comparative Analysis of Network Forensic Tools and Network Forensics Processes,” *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pp. 78–83, doi: [10.1109/ICSCEE50312.2021.9498226](https://doi.org/10.1109/ICSCEE50312.2021.9498226)
- Haseeb-ur-rehman, R.M.A. *et al.* (2023) “High-Speed Network DDoS Attack Detection: A Survey,” *Sensors*. Multidisciplinary Digital Publishing Institute (MDPI), doi: [10.3390/s23156850](https://doi.org/10.3390/s23156850)
- Javed, A.R. *et al.* (2022) “A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions,” *IEEE Access*, 10, pp. 11065–11089, doi: [10.1109/ACCESS.2022.3142508](https://doi.org/10.1109/ACCESS.2022.3142508)
- Kumar, A. and Somani, G. (2023) “Service separation assisted DDoS attack mitigation in cloud targets,” *Journal of Information Security and Applications*, 73, p. 103435, doi: [10.1016/j.jisa.2023.103435](https://doi.org/10.1016/j.jisa.2023.103435)
- Kushwah, G.S. and Ranga, V. (2021) “Optimized extreme learning machine for detecting DDoS attacks in cloud computing,” *Computers & Security*, 105, p. 102260, doi: [10.1016/j.cose.2021.102260](https://doi.org/10.1016/j.cose.2021.102260)
- Mahdavi Hezavehi, S. and Rahmani, R. (2023) “Interactive anomaly-based DDoS attack detection method in cloud computing environments using a third party auditor,” *Journal of Parallel and Distributed Computing*, 178, pp. 82–99, doi: [10.1016/j.jpdc.2023.04.003](https://doi.org/10.1016/j.jpdc.2023.04.003)
- Malik, A.W. *et al.* (2024) “Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges,” *Sensors*. Multidisciplinary Digital Publishing Institute (MDPI), doi: [10.3390/s24020433](https://doi.org/10.3390/s24020433)
- Mansoor, A. *et al.* (2023) “Deep Learning-Based Approach for Detecting DDoS Attack on Software-Defined Networking Controller,” *Systems*, 11(6), doi: [10.3390/systems11060296](https://doi.org/10.3390/systems11060296)

- Ouhssini, M., Afdel, K., Akouhar, M., *et al.* (2024) “Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches,” *Egyptian Informatics Journal*. Elsevier B.V, doi: [10.1016/j.eij.2024.100517](https://doi.org/10.1016/j.eij.2024.100517)
- Ouhssini, M., Afdel, K., Agherrabi, E., *et al.* (2024) “DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing,” *Journal of King Saud University - Computer and Information Sciences*, 36(2), doi: [10.1016/j.jksuci.2024.101938](https://doi.org/10.1016/j.jksuci.2024.101938)
- Qureshi, S. *et al.* (2021) “Network Forensics: A Comprehensive Review of Tools and Techniques,” *IJACSA International Journal of Advanced Computer Science and Applications*, 12(5), doi: [10.14569/IJACSA.2021.01205103](https://doi.org/10.14569/IJACSA.2021.01205103)
- Ribeiro, M.A., Pereira Fonseca, M.S. and de Santi, J. (2023) “Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks,” *Computers & Security*, 134, p. 103462, doi: [10.1016/j.cose.2023.103462](https://doi.org/10.1016/j.cose.2023.103462)
- Sanjalawe, Y. and Althobaiti, T. (2023) “DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning,” *Computers, Materials and Continua*, 75(2), pp. 3571–3588, doi: [10.32604/cmc.2023.037386](https://doi.org/10.32604/cmc.2023.037386)
- Saputra, H. (2021) “Mitigasi Serangan Distributed Denial of Service (DDoS) pada Arsitektur Software Defined Networking (SDN) Menggunakan Firewall Iptables,” *Jurnal Jaringan Komputer dan Keamanan JJKK*, 3(3), pp. 55–59.
- Shieh, C.S. *et al.* (2021) “Detection of unknown ddos attacks with deep learning and gaussian mixture model,” *Applied Sciences (Switzerland)*, 11(11), doi: [10.3390/app11115213](https://doi.org/10.3390/app11115213)
- Singh, C. and Jain, A.K. (2024) “A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network,” *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, 8, doi: [10.1016/j.prime.2024.100543](https://doi.org/10.1016/j.prime.2024.100543)
- Wani, S. *et al.* (2021) “Distributed denial of service (Ddos) mitigation using blockchain—a comprehensive insight,” *Symmetry*. MDPI AG, pp. 1–21, doi: [10.3390/sym13020227](https://doi.org/10.3390/sym13020227)
- Wintolo, H. *et al.* (2026) “Forensic Analysis of Trojan Backdoor (Gacor) Attacks on Private Cloud Environments using KUAD Method,” *Jurnal Informatika Medis (J-INFORMED)*, 4(1), pp. 16–22, doi: [10.52060/im.v4i1.4196](https://doi.org/10.52060/im.v4i1.4196)
- Wintolo, H., Riadi, I. and Yudhana, A. (2025a) “Enhancing Private Cloud Security Using Knowledge Understanding Assessment Defense Method for Distributed Denial of Service Attack Mitigation,” *International Journal of Safety and Security Engineering*, 15(11), pp. 2323–2331, doi: [10.18280/ijssse.151112](https://doi.org/10.18280/ijssse.151112)
- Wintolo, H., Riadi, I. and Yudhana, A. (2025b) “Intrusion Detection Analysis on Open Journal System Services Using Network Forensic Development Life Cycle Method,” *SKANIKA: Sistem Komputer dan Teknik Informatika*, 8(1), pp. 133–144, doi: [10.36080/skanika.v8i1.3284](https://doi.org/10.36080/skanika.v8i1.3284)
- Wintolo, H., Riadi, I. and Yudhana, A. (2025c) “Post Attack Mitigation on Open Journal System Services using Knowledge Understanding Assessment Defense (KUAD) Method,” *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, doi: [10.22219/kinetik.v10i4.2279](https://doi.org/10.22219/kinetik.v10i4.2279)
- Yungaicela-Naula, N.M. *et al.* (2023) “Physical Assessment of an SDN-Based Security Framework for DDoS Attack Mitigation: Introducing the SDN-SlowRate-DDoS Dataset,” *IEEE Access*, 11, pp. 46820–46831, doi: [10.1109/ACCESS.2023.3274577](https://doi.org/10.1109/ACCESS.2023.3274577)
-