QOMARUNA
Journal of
Multidisciplinary Studies

E-ISSN: 3026-5266
https://jurnal.uqgresik.ac.id/index.php/qjms

# Digital Forensic Study on Network Security Systems to Improve User Trust in Digital Technology

**Ammar Yasir Nasution**[1*]

[1]Universitas Al-Azhar, Padang Bulan-Medan, Indonesia, 20142
* Correspondence: yasirnasti0396@gmail.com

Received: 2 February 2026
Revised: 5 June 2026
Accepted: 23 June 2026

**Citation:**

Nasution, A. Y. . Digital Forensic Study on Network Security Systems to Improve User Trust in Digital Technology: english. *Qomaruna: Journal of Multidisciplinary Studies*, *3*(2), 140–147. https://doi.org/10.62048/qjms.v3i2.161



**ABSTRACT**

*This study proposes an integrated framework that combines digital forensics, machine learning-based intrusion detection, and user trust assessment to enhance network security. A quantitative field-experimental approach was employed in a simulated network environment. A dataset of 5,000 network log records was used to train and evaluate a Random Forest classifier for cyberattack detection. In addition, a survey of 100 users was conducted to assess perceived security and trust using a 10-point Likert scale. The results indicate that the proposed approach improved attack detection accuracy from 80% to 95% while reducing the average detection time from 7 to 5 seconds. The Random Forest model achieved an area under the receiver operating characteristic curve (ROC-AUC) of 0.90, demonstrating strong classification performance. Furthermore, the mean user trust score increased from 6.8 to 8.5 following system implementation. These findings suggest that integrating digital forensic analysis with machine learning has the potential to improve both technical network security performance and users' perceived trust in digital systems.*

***Keywords:*** *digital forensics, network security, trust users, cyber-attacks, digital technology*

**ABSTRACT**

Penelitian ini mengusulkan suatu kerangka terintegrasi yang menggabungkan digital forensik, sistem deteksi intrusi berbasis machine learning, dan evaluasi kepercayaan pengguna untuk meningkatkan keamanan jaringan. Penelitian menggunakan pendekatan kuantitatif dengan desain eksperimen lapangan pada lingkungan jaringan yang disimulasikan. Sebanyak 5.000 data log jaringan digunakan untuk melatih dan mengevaluasi model Random Forest dalam mendeteksi serangan siber. Selain itu, survei terhadap 100 pengguna dilakukan untuk mengukur persepsi terhadap keamanan dan tingkat kepercayaan menggunakan skala Likert 10 poin. Hasil penelitian menunjukkan bahwa pendekatan yang diusulkan meningkatkan akurasi deteksi serangan dari 80% menjadi 95% serta menurunkan waktu deteksi rata-rata dari 7 detik menjadi 5 detik. Model Random Forest memperoleh nilai area under the receiver operating characteristic curve (ROC-AUC) sebesar 0,90 yang menunjukkan kinerja klasifikasi yang baik. Selain itu, rata-rata skor kepercayaan pengguna meningkat dari 6,8 menjadi 8,5 setelah sistem diterapkan. Temuan ini menunjukkan bahwa integrasi analisis digital forensik dengan machine learning berpotensi meningkatkan kinerja teknis keamanan jaringan sekaligus memperkuat kepercayaan pengguna terhadap sistem digital.

**Kata kunci:** digital forensik, keamanan jaringan, kepercayaan pengguna, serangan siber, teknologi digital

## Introduction

Digital technologies have become indispensable across nearly every sector, including business, education, healthcare, finance, and public services. As organizations increasingly rely on interconnected information systems, the volume and sophistication of cyber threats have also grown substantially. Recent estimates indicate that cybercrime continues to impose significant economic losses worldwide, while concerns regarding data security and privacy remain major barriers to digital technology adoption (Almaiah et al., 2023; Putri et al., 2024). Consequently, ensuring effective network security has become a critical challenge for both organizations and end users.

Conventional network security mechanisms, including intrusion detection systems (IDS), are effective in identifying many known attacks but often struggle to detect sophisticated or stealthy threats, such as Advanced Persistent Threats (APTs), which may remain undetected for extended periods while compromising sensitive information (Malik et al., 2024; Erdodi et al., 2025). These limitations highlight the need for complementary analytical approaches capable of identifying hidden attack patterns and supporting post-incident investigations.

Digital forensics provides a systematic framework for collecting, preserving, examining, and interpreting digital evidence associated with cyber incidents. Beyond supporting criminal investigations, digital forensic techniques can strengthen network security by enabling more comprehensive attack detection, event reconstruction, and incident response (Oyadeyi et al., 2024). More recently, advances in machine learning have further enhanced forensic capabilities by enabling automated analysis of large-scale network log data and improving the detection of anomalous activities that may be overlooked by traditional rule-based approaches.

Despite these technological advances, cybersecurity effectiveness should not be evaluated solely from a technical perspective. Users' trust in digital systems plays an equally important role in determining technology adoption and continued use. Previous studies have shown that perceptions of system security and privacy strongly influence users' willingness to engage with digital technologies (Roca et al., 2009; Alotaibi & Alghamdi, 2022). However, most existing studies have examined either the technical performance of digital forensic systems or users' perceptions of security independently. Limited attention has been given to understanding how improvements in forensic-based security mechanisms may influence users' trust in digital systems.

Therefore, this study proposes an integrated approach that combines digital forensic analysis, machine learning-based intrusion detection, and user trust assessment within a network security framework. Specifically, the study evaluates the effectiveness of digital forensic techniques in improving cyberattack detection while simultaneously examining users' perceived security and trust following system implementation. By integrating technical performance with human-centered evaluation, this research seeks to provide a more comprehensive understanding of how digital forensics can contribute not only to stronger cybersecurity but also to greater confidence in digital technologies.

## Literature Review

### Digital Forensics in Network Security

Digital forensics has traditionally been defined as the systematic process of collecting, preserving, examining, and interpreting digital evidence for cybercrime investigation and incident response (Khan et al., 2022). In network security, however, digital forensics has evolved beyond its conventional role in post-incident investigation. It is increasingly applied to support log analysis, attack reconstruction, anomaly identification, and incident response, thereby strengthening overall cybersecurity capabilities. As cyber threats become more sophisticated, conventional security mechanisms often struggle to detect attacks that exploit previously unknown vulnerabilities or operate stealthily over extended periods. Consequently, digital forensic techniques have become an important complementary component of modern cybersecurity because they provide contextual evidence that enhances both attack detection and forensic investigation.

**Digital Forensics, Intrusion Detection, and Machine Learning**

Recent studies have increasingly integrated digital forensic techniques with intrusion detection systems (IDS) to improve cyberattack detection and response (Oyadeyi et al., 2024). While IDS effectively identify many known attack signatures, they frequently experience limitations when detecting sophisticated or low-frequency attacks.

Machine learning has emerged as a promising solution to address these limitations. By learning complex patterns from network traffic and system logs, machine learning models can automatically identify anomalous behavior and previously unseen attacks. Ensemble learning algorithms, such as Random Forest, have demonstrated competitive classification performance while maintaining robustness against noisy network data. The integration of digital forensic analysis with machine learning therefore offers opportunities for more proactive and intelligent cybersecurity systems.

**Digital Forensics for Advanced Persistent Threat Detection**

Advanced Persistent Threats (APTs) represent one of the greatest challenges in modern cybersecurity because attackers maintain unauthorized access over prolonged periods while minimizing their visibility. Traditional signature-based detection methods frequently fail to detect these attacks until significant damage has occurred (Malik et al., 2024; Erdodi et al., 2025). Previous studies suggest that forensic analysis of network logs, digital artifacts, and system events can significantly improve the identification of hidden attack patterns associated with APTs. By reconstructing attack sequences and analyzing digital traces, digital forensics provides valuable contextual information that complements conventional intrusion detection approaches.

**User Trust in Secure Digital Systems**

Technical security alone does not guarantee successful adoption of digital technologies. User trust remains a critical determinant of technology acceptance and continued use. Previous research consistently demonstrates that perceived security, privacy protection, and system reliability positively influence users' trust in digital services (Roca et al., 2009; Alotaibi & Alghamdi, 2022). Although digital forensic techniques are expected to strengthen users' confidence by improving transparency, accountability, and incident response capability, relatively few empirical studies have directly examined whether improvements in forensic-based security systems translate into greater user trust.

**Challenges in Digital Forensic Implementation**

Despite considerable advances in digital forensic technologies, several practical challenges remain. Processing large volumes of network data requires substantial computational resources, while timely forensic analysis is essential for effective incident response. In addition, integrating forensic tools into existing network infrastructures and adapting to rapidly evolving attack techniques remain significant technical challenges (Rahman et al., 2024). Addressing these challenges requires cybersecurity solutions that combine efficient forensic analysis, automated threat detection, and scalable analytical techniques suitable for real-world operational environments.

**Research Gap and Contribution**

The current literature reveals three important research gaps. First, digital forensics, intrusion detection, and machine learning have largely been investigated as separate research domains, with relatively limited efforts to integrate these approaches into a unified cybersecurity framework. Second, previous studies have primarily evaluated technical performance, including attack detection and forensic investigation capabilities, while giving comparatively little attention to user-centered outcomes such as perceived security and trust. Third, empirical evidence demonstrating the combined application of digital forensic analysis, machine learning-based threat detection, and user trust assessment within a single evaluation framework remains limited.

To address these gaps, this study proposes an integrated framework combining digital forensic analysis, machine learning-based intrusion detection, and user trust evaluation. The study evaluates

both objective cybersecurity performance and subjective user perceptions following system implementation. By integrating technical and human-centered perspectives, the proposed framework seeks to provide a more comprehensive assessment of the contribution of digital forensics to modern network security.

## Method

### Research Design

As shown in Figure 1, this study employed a quantitative field-experimental design to evaluate the effectiveness of integrating digital forensics into a network security system. The research consisted of three complementary components: (1) technical evaluation of a network intrusion detection system (IDS), (2) machine learning-based threat classification, and (3) user trust assessment following system implementation. This design enabled both objective evaluation of cybersecurity performance and subjective assessment of users' perceptions of security and trust.

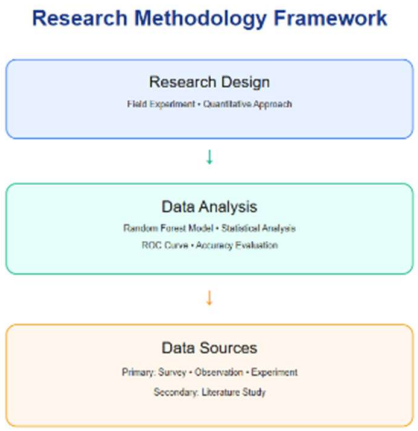


**Figure 1**. Research Method

### Network Traffic Dataset

A dataset comprising 5,000 simulated network traffic log records was used to develop and evaluate the threat detection model. The dataset included both normal network activity and malicious traffic representing common cyberattack scenarios, including denial-of-service (DoS) attacks, brute-force login attempts, unauthorized intrusion activities, and other anomalous network behaviors. Relevant features were extracted from the network logs, including IP address behavior, packet size, request frequency, connection duration, and anomaly indicators. These features were selected to characterize network behavior and distinguish normal from malicious traffic.

### Machine Learning Model

Threat classification was performed using the Random Forest algorithm because of its robustness in handling high-dimensional cybersecurity data and its strong classification performance. The dataset was randomly divided into training (80%) and testing (20%) subsets. Model development and evaluation were implemented using Python with the Scikit-learn library. To improve model reliability and reduce sampling bias, stratified cross-validation was applied during model training. Model performance was evaluated using several classification metrics, including accuracy, confusion matrix, receiver operating characteristic (ROC) curve, and the area under the ROC curve (ROC-AUC).

**Experimental Procedure**

The experimental evaluation compared two network security configurations:

- a conventional intrusion detection system (baseline IDS), and
- an intrusion detection system integrated with digital forensic analysis.

Both configurations were exposed to the same network traffic scenarios containing normal activity and simulated cyberattacks. System performance was evaluated by comparing attack detection accuracy, detection time, and overall classification performance.

**User Trust Assessment**

Following system implementation, a survey involving 100 respondents was conducted to evaluate users' perceptions of the proposed security system. User trust was measured using a structured questionnaire consisting of ten Likert-scale items assessing three constructs:

- perceived security,
- perceived system reliability, and
- overall trust in the digital system.

Responses were aggregated to obtain an overall trust score for subsequent statistical analysis.

**Data Analysis**

Technical performance of the intrusion detection system was evaluated using detection accuracy, detection time, confusion matrix analysis, and ROC-AUC. Comparative analyses were conducted between the baseline IDS and the forensic-enhanced IDS. Survey data were analyzed using descriptive statistics to summarize users' perceptions. Where appropriate, inferential statistical analyses were performed to examine changes in user trust following implementation of the proposed system. The combined technical and user-centered evaluations were used to assess the effectiveness of integrating digital forensics into network security.

## Results and Discussion

**Network Security Performance**

Figure 2 illustrates the conceptual architecture of the proposed digital forensic framework. The network consists of multiple client devices connected to a centralized server, where network traffic is monitored and analyzed. The digital forensic component collects communication logs and network traces from connected devices to support the identification of suspicious activities and potential cyberattacks. This architecture demonstrates how forensic monitoring can be incorporated into a network security environment to facilitate continuous traffic analysis.

The experimental evaluation suggests that integrating digital forensic techniques improved the operational performance of the intrusion detection system. Compared with the baseline system, the average detection time decreased from 7 seconds to 5 seconds. The authors also report that the attack detection rate increased from 80% to 95%. These findings suggest that forensic monitoring may enhance the ability of the security system to identify malicious activities more rapidly. However, the manuscript should clearly describe how the reported detection rate was calculated and how it differs from the machine learning classification metrics presented later.


**Figure 2.** Network Connected

**Machine Learning Classification Performance**

The machine learning component was evaluated using a Random Forest classifier. Figure 3 presents the receiver operating characteristic (ROC) curve, which achieved an area under the curve (AUC) of 0.80. An AUC of 0.80 indicates good discrimination between normal and malicious network traffic, suggesting that the classifier is capable of distinguishing attack patterns with reasonable accuracy.

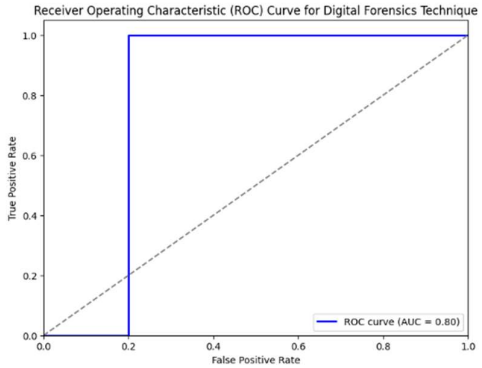


**Figure 3**. Receiver Operating Characteristic (ROC) curve

The corresponding confusion matrix is presented in Figure 4. Among the 5,000 classified observations, the model correctly identified 3,000 normal traffic instances (true negatives) and 800 malicious instances (true positives). However, 500 normal observations were incorrectly classified as attacks (false positives), while 700 attack instances were incorrectly classified as normal traffic (false negatives).

These results indicate that although the classifier demonstrates satisfactory predictive performance, classification errors remain. In particular, the relatively large number of false negatives indicates that some malicious activities were not detected. In practical cybersecurity applications, missed attacks may pose greater risks than false alarms because they allow malicious activities to remain unnoticed. Therefore, further optimization of feature extraction, model selection, or hyperparameter tuning may improve the robustness of the proposed classification model.

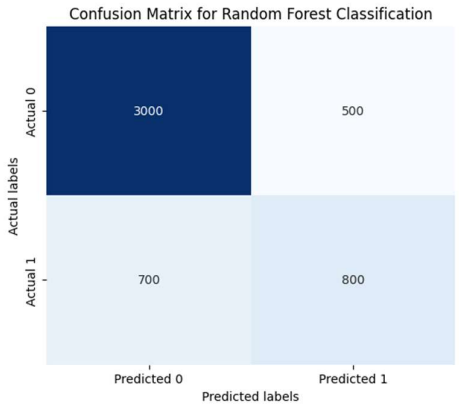


**Figure 4.** Confusion Matrix for Random Forest Classification

### User Trust Evaluation

To complement the technical evaluation, a survey involving 100 respondents was conducted to assess users' perceptions of the proposed security system. The average trust score increased from 6.8 before implementation to 8.5 after implementation, indicating that respondents perceived the forensic-enhanced security system as more secure and trustworthy. This finding is consistent with previous studies showing that perceived security and system reliability are important determinants of user trust in digital technologies. Improved threat detection and more transparent security mechanisms may strengthen users' confidence that their data and digital activities are adequately protected.

### Discussion

The results suggest that integrating digital forensic monitoring with machine learning-based threat classification has the potential to improve both technical and user-centered aspects of network security. The reduction in detection time indicates that forensic monitoring may support more timely identification of suspicious network activities, while the Random Forest classifier demonstrated reasonable capability for distinguishing malicious from normal traffic.

From the user perspective, the higher trust scores suggest that respondents perceived the enhanced security measures positively. Although the survey results indicate improved confidence in the system, they represent subjective perceptions rather than direct evidence that digital forensics alone caused the observed increase in trust.

Overall, the findings provide preliminary evidence that combining digital forensic analysis with machine learning may contribute to stronger network security and improved user confidence. Nevertheless, further validation using larger datasets, real-world network environments, and more rigorous statistical evaluation is necessary to confirm the effectiveness and generalizability of the proposed framework.

## Conclusion

This study investigated the integration of digital forensic techniques with machine learning-based threat detection to strengthen network security while examining users' perceptions of trust in the proposed system. The findings suggest that incorporating digital forensic analysis into a network security framework has the potential to improve operational performance by reducing attack detection time and enhancing the identification of suspicious network activities. The machine learning component, implemented using a Random Forest classifier, demonstrated good classification performance with an ROC-AUC of 0.80, indicating its potential for distinguishing between normal and malicious network traffic. In addition, the user survey indicated higher perceived trust following

implementation of the proposed system, suggesting that improved security measures may positively influence users' confidence in digital technologies.

Despite these encouraging findings, several limitations should be acknowledged. The machine learning model was evaluated using a simulated network traffic dataset, which may not fully represent the complexity and variability of real-world network environments. Furthermore, the user trust assessment was based on self-reported perceptions from a relatively limited sample and therefore does not establish a causal relationship between digital forensic implementation and user trust. Future studies should validate the proposed framework using real-world network traffic, evaluate its performance across more diverse cyberattack scenarios, compare alternative machine learning algorithms, and investigate the long-term effects of enhanced security mechanisms on user trust and technology adoption.

## Declaration of Conflict of Interest

The authors declare that there are no potential conflicts of interest related to this article's research, writing, and/or publication.

## References


Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Abu Alghanam, O. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability, 15*(13), 9908. https://doi.org/10.3390/su15139908

Alotaibi, R., & Alghamdi, A. (2022). The impact of perceived security and perceived trust on the use of m-payment applications in Saudi Arabia. *International Journal on Advanced Science, Engineering and Information Technology, 12*(6), 2398–2403. https://doi.org/10.18517/ijaseit.12.6.16540

Erdodi, L., Abraham, D., & Houmb, S. H. (2025). Improving detectability of advanced persistent threats (APT) by use of APT group digital fingerprints. *Information, 16*(9), 811. https://doi.org/10.3390/info16090811

Khan, A. A., Shaikh, A. A., Laghari, A. A., Dootio, M. A., Rind, M. M., & Awan, S. A. (2022). Digital forensics and cyber forensics investigation: Security challenges, limitations, open issues, and future direction. *International Journal of Electronic Security and Digital Forensics, 14*(2), 124–150. https://doi.org/10.1504/IJESDF.2022.121174

Malik, V., Khanna, A., Sharma, N., & Nalluri, S. (2024). Advanced persistent threats (APTs): Detection techniques and mitigation strategies. *International Journal of Global Innovations and Solutions (IJGIS)*. https://doi.org/10.21428/e90189c8.91e89a3e

Septya Mikayla, H., Kusyanti, A., & Trisnawan, P. H. (2024). Analisis forensik digital untuk investigasi kasus cyberbullying pada media sosial TikTok. *Jurnal Teknologi Informasi dan Ilmu Komputer, 11*(5), 1113–1124. https://doi.org/10.25126/jtiik.2024118017

Oyadeyi, O. O., Oyadeyi, O. A., & Bello, R. O. (2024). Cybercrime in the Asia-Pacific region: A case study of Commonwealth APAC countries. *Commonwealth Cyber Journal,* 130–160.

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan online dalam media sosial: Pentingnya perlindungan data pribadi di era digital (Studi kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia, 6*(1), 38–52. https://doi.org/10.35870/jpni.v6i1.1097

Rahman, R., & Akmal, G. L.(2024). Forensik Jaringan untuk Investigasi Kejahatan Cyber. *Jurnal Riset Sistem Informasi, 1*(3), 70-76

Roca, J. C., García, J. J., & de la Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96–113. https://doi.org/10.1108/09685220910963983