International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 10, October, 2025, pp. 2061-2068
Journal homepage: http://iieta.org/journals/ijsse

Evaluating the SUFREE Framework for Ethical Digital Forensics in Indonesia

Arizona Firdonsyah[1*], Purwanto Purwanto[2], Imam Riadi[3]

[1] Department of Information Technology, Universitas 'Aisyiyah, Yogyakarta 55292, Indonesia
[2] Doctoral Program in Information Systems, Universitas Diponegoro, Semarang 50241, Indonesia
[3] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia

Corresponding Author Email: arizona@unisayogya.ac.id

https://doi.org/10.18280/ijsse.151009

Received: 23 August 2025
Revised: 11 October 2025
Accepted: 22 October 2025
Available online: 31 October 2025

Keywords:
digital forensics, ethical framework, cybercrime investigation, evaluation, data integrity

ABSTRACT

The increasing complexity of digital crimes requires digital forensic investigations to be conducted not only with technical rigor but also under clear and accountable ethical governance, particularly in context-sensitive environments such as Indonesia. To address this need, the Supervisory Framework to Respect Ethics (SUFREE) was developed as an ethics-oriented supervisory framework for digital forensic processes using a Participatory Action Research (PAR) approach that involved relevant institutional stakeholders. This study aims to evaluate the effectiveness of SUFREE in guiding ethical digital forensic practice. A multi-criteria vector evaluation method is applied across five key phases of the framework: evidence identification accuracy, integrity of data preservation, quality of evidence examination, validity of analysis results, and completeness of investigation documentation. The evaluation is conducted on a real cyber incident involving an academic information system at a private Indonesian university, with monitoring and validation scores provided by expert evaluators. Normalization and weighted aggregation techniques are used to compute an overall effectiveness score. The results show that SUFREE achieves a final score of 0.763 (76.3%), which falls into the "Effective" category according to the predefined criteria, indicating that the framework provides structured support for embedding ethical principles into digital forensic workflows. However, this evaluation is limited to a single institutional case with two expert evaluators, so the findings should be interpreted as preliminary evidence rather than population-level generalization.

1. INTRODUCTION

The rapid evolution of information and communication technology has significantly increased the incidence of cybercrimes, necessitating the development of robust and ethical digital forensic methodologies. Digital forensics serves a critical role in uncovering evidence of cybercrimes, yet improper handling or unethical practices can undermine the integrity of investigations and erode public trust [1]. Ethical violations, such as mishandling evidence, violating privacy rights, and bias in analysis, have been increasingly reported in digital forensic practices worldwide [2]. These violations not only threaten the admissibility of digital evidence in court but also raise concerns about the professional accountability and transparency of digital forensic practitioners. As digital forensics often involves accessing highly sensitive data—such as personal communications, financial records, or private images—investigators must balance the need for evidence collection with respect for individual rights and legal constraints. Furthermore, the absence of clear ethical guidelines can lead to inconsistencies in how digital evidence is preserved, analyzed, and interpreted across different cases or jurisdictions. This reinforces the urgent need for standardized ethical frameworks that can guide practitioners through complex decision-making processes, ensuring that digital investigations remain both legally sound and morally responsible.

The current state of digital forensic capability in numerous institutions is marked by ad hoc procedures, inconsistent documentation, and the absence of a unified digital forensic policy framework [3]. This lack of preparedness not only hampers the efficiency of incident response but also undermines the admissibility and reliability of digital evidence in legal proceedings [4, 5]. Organizational shortcomings in governance, standard operating procedures, and chain of custody protocols reflect a broader issue of insufficient integration between digital forensic readiness, information security practices, and legal compliance. Without a systematic approach that aligns digital forensic processes with institutional objectives and regulatory mandates, the ability to respond effectively to security breaches and maintain evidentiary integrity remains severely compromised [6].

Although several ethical frameworks for digital forensics have been proposed internationally, such as PRECEPT and other region-specific guidelines, these models are often tailored to particular legal systems or specific categories of cases [7]. These frameworks have largely been developed for mature law-enforcement settings and specific legal environments. Their assumptions regarding institutional structure, regulatory clarity, and resource availability do not fully align with the conditions faced by Indonesian organisations such as universities and semi-formal investigative units. Consequently, their direct applicability in the Indonesian context is limited, as variations in legal frameworks, cultural norms, and institutional readiness require localized adaptation.

Prior literature also indicates that without context-sensitive supervisory mechanisms, ethical principles are often interpreted inconsistently and applied informally in real investigative practice. This situation creates a significant gap: the absence of a context-specific, standardized ethical framework that can ensure both legal compliance and moral accountability in digital forensic practices [8]. Addressing this gap is essential not only for improving investigative integrity but also for strengthening public confidence in digital forensic outcomes, particularly in cases involving sensitive personal or national security data.

Supervisory Framework to Respect Ethics (SUFREE) does not replace technical forensic models such as ICMP-Flood volumetric-based Distributed Denial of Service (DDoS) [9] or live forensic acquisition [10]; instead, it serves as an ethical and procedural supervisory layer that can be applied on top of existing forensic technical processes. The necessity for frameworks that embed ethical principles into digital forensic workflows has been emphasized by numerous scholars and international bodies [11]. The lack of standardized ethical frameworks in digital forensics can severely compromise the credibility of forensic findings in legal proceedings, ultimately eroding public confidence in investigative bodies. This concern stems from ethical challenges such as breaches of privacy and improper handling of evidence, which may jeopardize the admissibility and reliability of digital proof in court [12, 13]. However, most existing frameworks are contextually developed for specific regions or types of cases, and there remains a gap in frameworks tailored to the Indonesian environment.

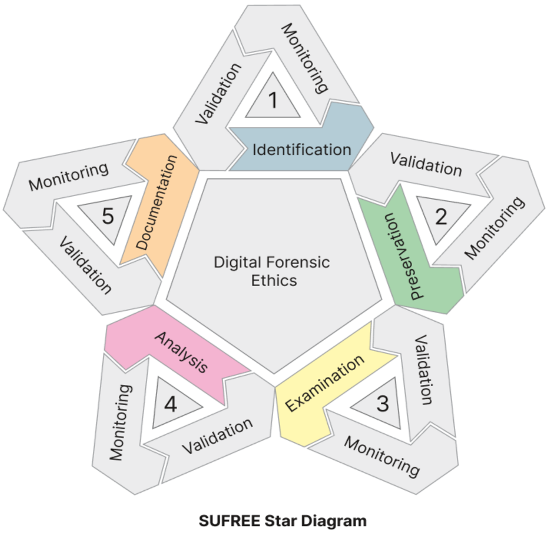

Figure 1. SUFREE digital forensics framework

To address this gap, the SUFREE, as seen in Figure 1, SUFREE was developed using a Participatory Action Research (PAR) approach [14]. PAR involves collaboration between researchers and stakeholders to ensure that solutions are grounded in practical realities [15]. SUFREE aims to enhance the reliability, integrity, and ethical standards of digital forensic investigations in Indonesia by providing structured procedures across all phases of forensic analysis [16]. The core group consisted of digital forensic practitioners selected by purposive sampling based on their involvement in incident handling and governance. The timeline of discussion of this framework was carried out for a total of three months, with three cycles as shown in Figure 2.

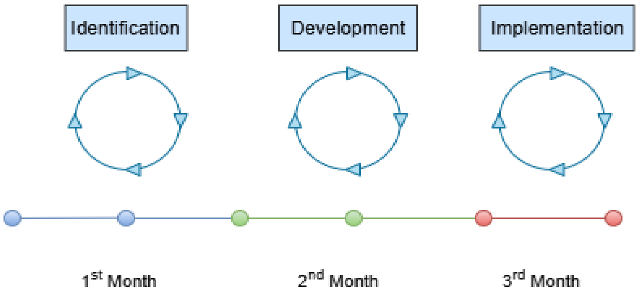

Figure 2. Framework development timeline

Through three PAR cycles of identification, development, and implementation, the stakeholders identified ethical and procedural gaps in existing practices, tested preliminary versions of SUFREE on past and hypothetical cases, and iteratively revised the phases and indicators until a shared, context-appropriate structure was obtained.

This study evaluates the effectiveness of the SUFREE framework to assess its implementation quality. Accordingly, this study addresses the gap by quantitatively evaluating SUFREE as an ethics-oriented supervisory framework in a real Indonesian university case, using a multi-criteria vector approach.

2. METHODOLOGY

In light of these challenges and the identified gap in ethical digital forensic practices, this study employs a structured methodological approach to develop, implement, and evaluate the SUFREE framework within the Indonesian context. The methodology is designed to ensure both technical rigor and the integration of ethical principles across all phases of the forensic process. The following section outlines the methodological stages undertaken to design, refine, and assess SUFREE, ensuring that the resulting framework is operationally effective, ethically sound, and aligned with national legal and regulatory requirements.

The evaluation methodology of the SUFREE framework follows a structured sequence as seen in Figure 3.

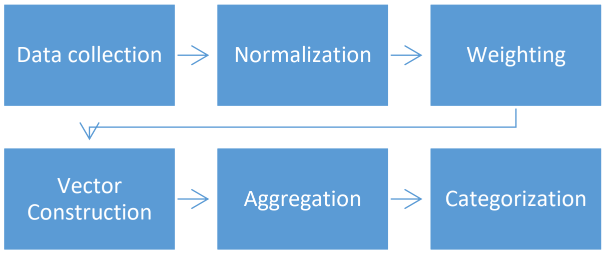

Figure 3. Evaluation method with multi-criteria vector weighting

1. **Data Collection:** Collection of monitoring and validation scores from the five key phases of the SUFREE framework implementation.
2. **Normalization:** Applying Min-Max normalization to the collected scores.
3. **Weighting:** Assigning criteria weights based on expert judgment.
4. **Vector Construction:** Constructing the score vector and weight vector.
5. **Aggregation:** Calculating the final score using the dot product formula.
6. **Categorization:** Classifying the total score based on predefined effectiveness categories.

2.1 Evaluation method: Multi-criteria vector approach

Multi-criteria evaluation often employs a hierarchical structure to organize criteria, allowing for a clear representation of relationships among different properties of the system [17]. In digital forensic frameworks, evaluation must consider multiple critical factors simultaneously, including accuracy, integrity, quality, validity, and documentation completeness [18]. The multi-criteria vector method provides a structured approach to quantitatively assess these dimensions, enabling consistent comparison and comprehensive judgment.

The steps in multi-criteria vector evaluation are as follows:

- **Normalization:** Each raw score is normalized to a range between 0 and 1 using the Min-Max normalization:

$$N_i = \frac{X_i - X_{min}}{X_{max} - X_{min}} \quad (1)$$

where, N_i is the normalized score, X_i is the original score, X_{min} and X_{max} are the minimum and maximum possible scores.

- **Vector Representation:** Normalized scores are represented as a vector:

$$\mathrm{s} = [\mathrm{s}_1, \mathrm{s}_2, \mathrm{s}_3, \dots, \mathrm{s}_\mathrm{n}] \in [0,1]^\mathrm{n} \quad (2)$$

where, n is the number of evaluation criteria.

- **Weight Assignment:** Each criterion is assigned a weight based on its relative importance:

$$\mathrm{S} = [\mathrm{s}_1, \mathrm{s}_2, \mathrm{s}_3, \mathrm{s}_4, \mathrm{s}_5] \quad (3)$$

- s_1: Digital evidence identification accuracy score;
- s_2: Data preservation integrity score;
- s_3: Evidence examination quality score;
- s_4: Validity score of the analysis results;
- s_5: Completeness of investigation documentation score.

- **Aggregation:** The final evaluation score is obtained by calculating the dot product of the weight vector and the score vector:

$$e = [e_1, e_2, e_3, \dots, e_n] \text{ with } \sum e_i = 1 \quad (4)$$

2.2 Categorization

- **Categorization:** The total score is mapped to evaluation categories to determine effectiveness.

The following section applies this evaluation procedure to a real institutional case and reports the resulting scores.

Table 1. Score categorization

Score Range (%)	Category	Description
≥ 85%	Highly Effective	The framework meets almost all aspects of evaluation. The implementation is very good and consistent.
70% – 84.99%	Effective	The framework is quite good; most aspects are in place, but can still be improved.
50% – 69.99%	Quite Effective	The framework still has many shortcomings in some important indicators. It needs improvement.
30% – 49.99%	Less Effective	The framework lacks many indicators and can lead to bias or inaccuracy.
< 30%	Ineffective	The framework fails to meet almost all indicators. It cannot be used as a reference in the investigation.

The categories listed in Table 1 follow the principles used in ISO/IEC 25010:2011 on system and software quality evaluation [19]. The quality standards of the evaluation framework set a score ≥ 85% as a highly effective category, which means that almost all aspects are well met and implementation is consistent. Frameworks with a score of 70%–84.99% are categorized as effective because most aspects are compliant even though they still need improvement. A score of 50%–69.99% shows that the framework is quite effective but still has many shortcomings in important indicators. A score of 30%–49.99% indicates that the framework is less effective because it does not meet many indicators and therefore risks causing bias. Scores below 30% are categorized as ineffective, because almost all indicators fail to meet and the framework cannot be used as a reference in investigations.

3. EVALUATION RESULTS AND CASE STUDY CALCULATION

3.1 Case study

A private university's academic management information system in Indonesia experienced service interruptions and repetitive suspicious activity on e-learning servers and other integrated sub-applications. The university's IT team reported symptoms of performance degradation and the appearance of unusual consecutive error logs.

The university's cyber security incident response team (CSIRT) conducted a preliminary investigation using Wazuh's security monitoring device and Burp Suite analysis tool. In this process, several activities were found that indicated the occurrence of security breaches, which then became the basis for the start of digital forensic investigations.

There were at least five attacks on this case study, namely XSS, host header attack, sniffing, password guessing, and DDoS. The most dangerous attack is XSS because this attack takes advantage of the way browsers execute scripts from various sources without properly confirming where they come from, resulting in a serious threat to users [20].

Stages of Attack Discovery:

Identification:

- Digital evidence sources are collected from server logs, application databases, and system configurations.
- Burp Suite identifies some app URLs with cleartext password submissions, such as http://sim.unisayogya.ac.id/simptt-akademik/, indicating weak encryption of user data.

Inspection:

The log results from Wazuh show suspicious activity:

- Many HTTP requests to /old/wp-admin/install.php and /uploads/ALFA_DATA/alfacgiapi/perl.alfa from the same IP address.
- There was a spike in Web Server 400 Error Code at 03.00 – 03.25 WIB, May 19, 2023.
- Other attacks appear with very long URL patterns (URL Too Long), leading to possible overflow buffer exploits.

Analysis:

Five types of attacks were identified:

- **Cross-Site Scripting (XSS)**: Through vulnerable JavaScript libraries.
- **Host Header Attack**: Occurs because there is no X-Frame-Options setting.
- **Sniffing**: Cookies do not have Secure and SameSite security flags.
- **Password Guessing (Brute Force)**: Happens through the login page.
- **Distributed Denial of Service (DDoS)**: Distributed attacks aimed at central servers.

The attack discovery process began with a comprehensive reconnaissance analysis, where raw log data from multiple system components were correlated to identify anomalous patterns. This included the correlation of HTTP access logs, database query logs, and system-level event logs to establish a timeline of suspicious activities. The combination of Wazuh's real-time monitoring and Burp Suite's vulnerability scanning allowed the investigative team to pinpoint potential weaknesses exploited by the attacker. At this stage, prioritization of evidence sources was essential to ensure that the most volatile and perishable data, such as active network sessions and temporary cache files, were captured before they were overwritten or lost.

Following the initial identification, the preservation phase focused on creating forensically sound copies of critical evidence. Server images were generated using write-blocker techniques to ensure integrity, while cryptographic hash values (SHA-256) were computed and stored for each data set to maintain verifiable authenticity. This phase also involved isolating compromised systems from the production network to prevent further intrusion while maintaining system states for later analysis.

During the detailed inspection, investigators applied layered analysis by segregating evidence into network-level, application-level, and file-system-level indicators. This step revealed patterns such as repeated access attempts to deprecated web directories, anomalies in HTTP header structures, and the absence of security attributes in session cookies. Such findings were cross-referenced with known attack signatures and threat intelligence databases, enabling the classification of attack types and the identification of the probable intrusion vectors.

The attack classification and root cause analysis stage integrated findings from multiple sources to form a coherent attack narrative. For instance, the occurrence of long URL injection patterns pointed towards possible buffer overflow exploits, while abnormal host header values suggested an attempt to manipulate virtual host routing. Coupling these observations with system configuration reviews helped confirm misconfigurations such as missing X-Frame-Options headers that facilitated certain attack types. This systematic classification enabled a targeted mitigation strategy tailored to the vulnerabilities exploited.

Finally, a post-discovery validation process was conducted to ensure that the identified attack vectors were indeed responsible for the incident. Controlled simulation of the attacks in an isolated environment replicated the observed behavior, confirming the findings and strengthening the evidentiary value for potential legal proceedings. This validation phase also served to refine the SUFREE framework's procedural recommendations, ensuring that lessons learned from this case could be codified into future forensic readiness protocols. This incident provided a comprehensive context in which all five phases of SUFREE could be operationalized and evaluated.

3.2 Implementation of the SUFREE digital forensic framework

The SUFREE framework is prepared in five main stages, namely identification, preservation, examination, analysis, and documentation. To facilitate systematic and mathematical modeling, all of these stages can be represented in the form of process vectors, where each element represents a single phase of forensic digital investigation. These representations not only reflect linear workflows, but also allow for the integration of quantitative assessment components such as technical performance scores and ethical validation in a structured and measurable structure. Formally, the stages in SUFREE can be expressed in line vectors as shown in Eq. (5).

$$\mathrm{T} = [\mathrm{T}_1, \mathrm{T}_2, \mathrm{T}_3, \mathrm{T}_4, \mathrm{T}_5] = [\mathrm{I}, \mathrm{P}, \mathrm{E}, \mathrm{A}, \mathrm{D}] \tag{5}$$

where,

- T_1 = I: Identification Accuracy;
- T_2 = P: Preservation Integrity;
- T_3 = E: Examination Quality;
- T_4 = A: Validity of the Analysis;
- T_5 = D: Completeness of Documentation.

Each T_i element is a single process that can be analyzed based on two main components: the monitoring value (M_i) and the validation status (V_i). Monitoring scores are obtained through the Analytic Hierarchy Process (AHP) method based on three technical performance criteria at each stage, while validation is determined by certified supervisors as a form of supervision of the ethics and integrity of the procedure.

Weights are given to each component of the score to reflect the preferences or relative importance of each dimension. Weights are assigned to each stage using the expert judgement approach, leveraging the experience and knowledge of seasoned digital forensic practitioners. This method is especially relevant in contexts where empirical data are limited, or where situational complexity demands informed professional discretion.

The determination of weights for each stage in the SUFREE framework is carried out by an expert judgement approach, which is a method based on subjective assessment from experts who have competence and direct experience in the field of digital forensics. This approach is commonly used in multi-criteria-based system evaluations, especially when quantitative data are not fully available or when the complexity of the context demands professional intuition-based adjustments.

Table 2. Evaluation indicator weights

Evaluation Indicator	Weight (e_i)
I – Identification Accuracy	0.15
P – Preservation Integrity	0.25
E – Quality Inspection	0.15
A – Validity of the Analysis	0.25
D – Completeness of Documentation	0.2

These evaluation indicator weights in Table 2 reflect the relative importance of each stage in the context of ethical and accountable digital forensic implementation. The preservation and analysis stages received the highest weight (0.25) because they were considered the most critical in ensuring the integrity and validity of digital evidence. Meanwhile, the identification and examination stage received a lower weight (0.15) because it was assessed as an initial and operational stage that still depended on the quality of input and the context of the case. The documentation stage is given a medium weight (0.20) because of its very important role in supporting the transparency and legitimacy of investigation procedures.

Thus, the final score of SUFREE, which represents the level of success and ethical compliance of the digital forensic process, is obtained from Eq. (6).

$$\text{SUFREE\_score} = \mathrm{e} \cdot \mathrm{T}^{\mathrm{t}} = \sum_{i=1}^{5} (\mathrm{e_i} \times \mathrm{T_i}) \tag{6}$$

Through this structured approach, the SUFREE framework transforms the traditional forensic process into an ethically guided, performance-measurable, and court-ready methodology. This dual emphasis on technical excellence and ethical compliance strengthens both the credibility of investigative outcomes and the public's trust in digital forensic processes. Moreover, by integrating measurable performance metrics with formal ethical oversight, SUFREE ensures that each investigative phase not only achieves its technical objectives but also aligns with institutional mandates, legal frameworks, and professional codes of conduct. This synergy between operational efficiency and ethical integrity reduces the likelihood of procedural errors, strengthens the admissibility of evidence in legal proceedings, and enhances the ability of investigative teams to respond swiftly and effectively to evolving cyber threats.

In addition, the adoption of SUFREE provides organizations with a repeatable and auditable forensic methodology that can be adapted to a wide range of case complexities from routine data breaches to large-scale cybercrime investigations without sacrificing ethical safeguards. Its vector-based evaluation model enables continuous monitoring of investigative performance, allowing decision-makers to identify process gaps, allocate resources more strategically, and refine operational protocols based on empirical data. Over time, this capability fosters a culture of accountability and continuous improvement within digital forensic units, ensuring that the framework remains relevant and resilient in the face of rapidly changing technological and legal landscapes. Ultimately, SUFREE serves not only as a procedural guide but also as a governance instrument, bridging the gap between technical forensics, ethical responsibility, and organizational policy enforcement.

3.3 Evaluators and assessment procedure

The evaluation involved two expert evaluators who are experienced in digital forensics and information security governance. These evaluators assessed each phase of SUFREE using predefined indicators and weightings derived from the multi-criteria vector approach. While two evaluators are sufficient for an initial exploratory assessment, the study acknowledges that the small number of evaluators limits statistical generalization and may introduce expert bias. Nonetheless, their involvement provides early insight into the practical interpretation of SUFREE's ethical principles in an actual investigative setting.

3.4 Case study selection and context

The case study used in this evaluation was an actual cyber incident involving unauthorized access and data manipulation within an academic information system at a private Indonesian university. This case was intentionally selected based on three considerations. First, the incident represents a typical and recurring challenge faced by higher-education institutions in Indonesia, where digital forensic capability often varies and formal ethical guidelines remain limited. Second, the institution involved had previously adopted preliminary components of the SUFREE framework, making it a suitable pilot environment for assessing its practical applicability. Third, the incident provided access to complete artefacts, logs, and administrative documentation required for an ethical forensic investigation, ensuring that the full five phases of SUFREE could be meaningfully evaluated.

4. DISCUSSION

The evaluation results indicate that the SUFREE framework demonstrates an effective level of supervisory control over digital forensic processes. The relatively high scores in identification accuracy and documentation completeness underscore the critical role of precise evidence acquisition and systematic reporting in ensuring the reliability and admissibility of digital evidence within judicial contexts. These findings reaffirm the notion that the early stages of a forensic investigation, particularly those concerning accurate identification of evidence sources, are foundational to the integrity of subsequent analytical and interpretative processes. The comprehensive nature of documentation, as mandated within SUFREE, not only preserves the chain-of-custody but also establishes a transparent procedural narrative that can withstand both legal scrutiny and academic review.

To gain a comprehensive understanding of the level of effectiveness of the implementation of the SUFREE framework, a quantitative evaluation process was carried out on all stages that have been designed in the framework. This evaluation involves the participation of two expert respondents from the national digital forensic practitioner environment, with a standardized criteria-based assessment approach in the form of a structured evaluation instrument. Each responder was asked to score on five main stages in the framework, namely identification, preservation, examination, analysis, and documentation, based on predetermined success indicators. The assessment is carried out independently to ensure the objectivity of the results. The following table presents the results of the evaluation provided by each respondent, which is the basis for calculating the overall framework performance score aggregate. The calculation SUFREE_score can be seen in Table 3 based on the values given by two respondents who are digital forensic practitioners.

Table 3. Evaluation results of the SUFREE framework

Evaluation Indicators	x_i		s_i	e_i	e_i*s_i
	R1	**R2**			
I - Identification Accuracy	80	75	0.8	0.15	0.117
P - Preservation Integrity	70	70	0.7	0.25	0.175
E - Quality Inspection	85	80	0.85	0.15	0.124
A - Validity of the Analysis	75	75	0.75	0.25	0.188
D - Completeness of Doc.	80	80	0.8	0.2	0.16
Total					0.763

Table 3 presents the evaluation results of the SUFREE framework across the five phases: Identification Accuracy (I), Preservation Integrity (P), Examination Quality (E), Validity of the Analysis (A), and Completeness of Documentation (D). The scores assigned by the two evaluators range from 70 to 85, indicating a generally moderate-to-high level of effectiveness across all phases. Differences between raters are minimal and primarily observed in the Identification and Examination phases, reflecting expected variations in expert judgment. The consistency observed is comparable with prior studies emphasizing the subjective nature of expert-based assessments in socio-technical evaluations [16].

When normalized and weighted according to the scheme in Table 2, the phases contribute unequally to the final score. Validity of the Analysis (A) yields the highest weighted contribution (0.188), followed by Preservation Integrity (P) (0.175) and Completeness of Documentation (D) (0.160). These results align with multi-criteria decision-making principles, which assign greater influence to ethically critical activities within forensic processes [13, 16].

The overall SUFREE effectiveness score, derived using the vector aggregation model e. T^t is 0.763 (76.3%). According to the threshold ranges in Table 1, this value falls within the effective category, consistent with classification approaches widely applied in system and process quality evaluations [20]. Although the result indicates that SUFREE provides a structured ethical supervisory layer, it also underscores specific areas, particularly preservation procedures and analytical validation, where further refinement is required. These findings offer an empirical basis for prioritizing enhancements in subsequent iterations of the framework and for extending validation across broader institutional settings.

From a methodological standpoint, the adoption of the multi-criteria vector evaluation model provides a rigorous, quantifiable mechanism for assessing performance across multiple forensic dimensions. By normalizing, weighting, and aggregating scores through a vector-based approach, the framework allows evaluators to generate an objective composite measure of effectiveness while retaining the granularity to identify specific process strengths and weaknesses. This mathematical structuring aligns well with quality management principles and systems engineering methodologies, making SUFREE adaptable for integration into broader institutional audit and compliance systems. Furthermore, the reliance on expert judgement for weight determination ensures that the evaluation reflects practical realities rather than purely theoretical constructs, thereby enhancing contextual relevance.

The results of this study support the hypothesis that the incorporation of the PAR approach in the development of the framework provides an advantage in terms of contextual alignment, namely the ability to adapt to evolving ethical and institutional dynamics. Thus, the framework is not only built on international theories but is also firmly rooted in local practices and conditions identified through participatory action processes.

5. CONCLUSIONS

The evaluation results place SUFREE within the "Effective" category, with an overall score of 0.763. While this indicates an adequate level of ethical supervision across the investigative phases in the examined case, a more critical reading is required when positioning SUFREE within the broader landscape of digital forensic frameworks. In parallel, a range of process-oriented models and guidelines, such as generic digital forensic process frameworks and investigative standards discussed in previous studies [7, 12, 13], focus on structuring technical activities, defining stages of investigation, and safeguarding evidentiary integrity.

Despite their contributions, these frameworks generally share two limitations in the context of this study. First, they are predominantly designed for mature law-enforcement or highly regulated environments, assuming clear legal mandates, stable institutional capacity, and specialised investigative units. Second, they rarely provide an operational, quantitative mechanism for monitoring and evaluating how ethical principles and process requirements are implemented in practice across the full lifecycle of an investigation, particularly in non–law-enforcement organisations such as universities. As a result, the application of such frameworks in Indonesian institutional settings often remains informal and uneven, with ethical principles interpreted ad hoc, and supervisory oversight is weakly institutionalized.

SUFREE addresses this gap by introducing a supervisory layer that embeds explicit ethical checkpoints into each investigative phase and links them to measurable indicators. Rather than solely articulating what investigators ought to do, SUFREE specifies how compliance with ethical and procedural expectations can be documented, scored, and aggregated using a multi-criteria vector approach. The weighted contributions in the evaluation highlight that phases related to analytical validity and preservation integrity exert the strongest influence on the final score, which is consistent with the emphasis on evidentiary robustness and analytical accountability in prior frameworks.

These findings must also be interpreted in light of the study's methodological constraints. The evaluation is based on a single case within one university and relies on the judgments of two expert evaluators, which limits statistical generalisation and introduces the possibility of expert bias—an issue already acknowledged in socio-technical evaluation literature [16]. Nevertheless, within these constraints, the results provide valuable preliminary evidence that SUFREE can serve as a practical supervisory framework that operationalises ethical oversight in digital forensics, particularly in institutional contexts where direct adoption of existing law-enforcement–centric frameworks is problematic. The evaluation also delineates concrete areas for improvement, suggesting that future work should focus on refining preservation and analysis controls, expanding the framework's implementation to multiple institutions, and conducting larger-scale assessments to strengthen the robustness and external validity of SUFREE as an ethics-oriented supervisory mechanism.

5.1 Limitations

This study has several important limitations that should be acknowledged to properly contextualize the findings. First, the evaluation is based on a single case study conducted in one university environment, which limits the diversity of incident types and organizational contexts represented. Second, the assessment relies on two evaluators, which restricts the ability to measure inter-rater reliability and increases the potential for subjective bias in scoring. Third, the study uses expert judgment to derive the weighting and evaluation scores, which may be influenced by the professional background and prior experience of the evaluators. Fourth, because the institution involved had partial familiarity with SUFREE, the results may not directly reflect how the framework would perform in less-prepared environments.

Despite these limitations, the primary purpose of this paper is not to provide population-level generalizations, but to demonstrate the use of a structured evaluation method for assessing the SUFREE framework in a realistic setting. Accordingly, this exploratory study serves as a foundational step toward broader validation, which future research can strengthen through multi-site evaluations, larger assessor groups, and more diverse case types.

REFERENCES

[1] Carrier, B., Spafford, E.H. (2003). Getting physical with the investigative process. International Journal of Digital Evidence, 2(2): 1-20. https://pdfs.semanticscholar.org/915b/524318e2f0689b586ba7ae89ea39e9b22ce3.pdf.

[2] Firdonsyah, A., Purwanto, P., Riadi, I. (2023). Framework for digital forensic ethical violations: A systematic literature review. E3S Web of Conferences, 448: 01003. https://doi.org/10.1051/e3sconf/202344801003

[3] Smit, N.M., Morgan, R.M., Lagnado, D.A. (2018). A systematic analysis of misleading evidence in unsafe rulings in England and Wales. Science & Justice, 58(2): 128-137. https://doi.org/10.1016/j.scijus.2017.09.005

[4] Thakar, A.A., Kumar, K., Patel, B. (2021). Next generation digital forensic investigation model (NGDFIM) - Enhanced, time reducing and comprehensive framework. Journal of Physics: Conference Series, 1767: 012054. https://doi.org/10.1088/1742-6596/1767/1/012054

[5] Jones, A., Vidalis, S. (2019). Rethinking digital forensics. Annals of Emerging Technologies in Computing, 3(2): 41-53. https://doi.org/10.33166/AETiC.2019.02.005

[6] Adel, A. (2022). A conceptual framework to improve cyber forensic administration in industry 5.0: Qualitative study approach. Forensic Sciences, 2(1): 111-129. https://doi.org/10.3390/forensicsci2010009

[7] Ferguson, R.I., Renaud, K., Wilford, S., Irons, A. (2020). PRECEPT: A framework for ethical digital forensics investigations. Journal of Intellectual Capital, 21(2): 257-290. https://doi.org/10.1108/JIC-05-2019-0097

[8] Tan, T.C.C., Ruighaver, A.B., Ahmad, A. (2010). Information security governance: When compliance becomes more important than security. In IFIP Advances in Information and Communication Technology, pp. 55-67. https://doi.org/10.1007/978-3-642-15257-3_6

[9] Yudhana, A., Riadi, I., Suharti, S. (2022). Network forensics against volumetric-based distributed denial of service attacks on cloud and the edge computing. International Journal of Safety and Security Engineering, 12(5): 577-588. https://doi.org/10.18280/ijsse.120505

[10] Herman, Yudhana, A., Sarjimin. (2023). Live forensic environment with parallel data acquisition for investigating private mode browsing. International Journal of Safety and Security Engineering, 13(3): 577-585. https://doi.org/10.18280/ijsse.130320

[11] Quick, D., Choo, K.K.R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. Future Generation Computer Systems, 78: 558-567. https://doi.org/10.1016/j.future.2016.12.032

[12] Aleke, N.T., Trigui, M. (2025). Legal and ethical challenges in digital forensics investigations. In Digital Forensics in the Age of AI, pp. 147-176. https://doi.org/10.4018/979-8-3373-0857-9.ch006

[13] Mandayam, R. (2025). Ethical considerations in digital forensic. International Journal of Innovative Research in Engineering, Multidisciplinary & Physical Sciences, 13(1): 1-4. https://www.ijirmps.org/papers/2025/1/231831.pdf.

[14] Triantaphyllou, E. (2000). Multi-criteria Decision Making Methods: A Comparative Study. Springer New York, NY. https://doi.org/10.1007/978-1-4757-3157-6

[15] Deb, K. (2011). Multi-objective optimization using evolutionary algorithms: An introduction. In Multi-Objective Evolutionary Optimisation for Product Design and Manufacturing, pp. 3-34. https://doi.org/10.1007/978-0-85729-652-8_1

[16] Firdonsyah, A., Purwanto, P., Riadi, I. (2024). Supervision-based digital forensics framework to respect ethics using participatory action research method. Journal of International Crisis and Risk Communication Research, 7(3): 124-140. https://doi.org/10.63278/jicrcr.vi.2291

[17] Voronin, A., Savchenko, A. (2023). Evaluation of complex systems: Multicriteria approach. International Scientific and Technical Journal "Problems of Control and Informatics", 67(6): 83-89. https://doi.org/10.34229/1028-0979-2022-6-7

[18] Han, J., Kamber, M., Pei, J. (2012). Data Mining: Concepts and Techniques (3rd ed.). Morgan Kaufmann/Elsevier. https://homes.di.unimi.it/ceselli/IM/slides/03Preprocessing.pdf.

[19] ISO/IEC 25010:2011. (2011). Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models. https://www.iso.org/standard/35733.html.

[20] Herman, Riadi, I., Rafiq, I.A. (2022). Forensic mobile analysis on social media using national institute standard of technology method. International Journal of Safety and Security Engineering, 12(6): 707-713. https://doi.org/10.18280/ijsse.120606