Data and Metadata. 2025; 4:1179
doi: 10.56294/dm20251179

ORIGINAL

A Supervisory Approach to Building Ethical Digital Forensic Frameworks through Participatory Action Research

Un Enfoque De Supervisión Para La Creación De Marcos Forenses Digitales Éticos Mediante La Investigación-Acción Participativa

Arizona Firdonsyah[1], Purwanto[1], Imam Riadi[2], Mahrus Ali[1], Ammar Fauzan[3]

[1]Diponegoro University, Doctoral of Information system department. Semarang, Indonesia.
[2]Ahmad Dahlan University, Department of Information system. Yogyakarta, Indonesia.
[3]STMIK PGRI Arungbinang, Department of Information Technology. Kebumen, Indonesia.

Cite as: Firdonsyah A, Purwanto, Riadi I, Ali M, Fauzan A. A Supervisory Approach to Building Ethical Digital Forensic Frameworks through Participatory Action Research. Data and Metadata. 2025; 4:1179. https://doi.org/10.56294/dm20251179

Submitted: 25-11-2024 **Revised:** 03-04-2025 **Accepted:** 13-09-2025 **Published:** 14-09-2025

Editor: Dr. Adrián Alejandro Vitón Castillo

Corresponding Author: Arizona Firdonsyah

ABSTRACT

Introduction: the integrity of digital forensic case handling plays a crucial role in safeguarding the public interest. Breaches in ethical compliance within the forensic process can undermine the credibility of investigations and erode public trust in their outcomes.
Method: the Participatory Action Research (PAR) approach. The research engaged stakeholders from both academic and professional sectors. Data collection was conducted through comprehensive literature reviews and structured stakeholder discussions to ensure the resulting framework reflects both theoretical and practical considerations.
Results: the study introduced the Supervisory Framework to Respect Ethics or we call it SUFREE, a model specifically designed to address ethical oversight in the digital forensic process, specific to conditions in Indonesia. The framework was developed through iterative consultation and validation involving relevant experts, aiming to ensure methodological robustness and applicability within the Indonesian setting.
Conclusions: the SUFREE framework offers a structured, ethics-focused supervisory model expected to enhance the quality, integrity, and professionalism of digital forensic practices in Indonesia, thereby contributing to improved public trust in forensic investigations.

Keywords: Digital Forensics Ethics; Ethics-oriented Forensics Framework; Supervisory Framewor; Forensic Integrity.

RESUMEN

Introducción: la integridad en la gestión de casos de análisis forense digital desempeña un papel crucial en la protección del interés público. Las infracciones en el cumplimiento ético dentro del proceso forense pueden socavar la credibilidad de las investigaciones y erosionar la confianza pública en sus resultados.
Método: adoptando el enfoque de Investigación-Acción Participativa (IAP), la investigación involucró a actores clave de los sectores académico y profesional. La recopilación de datos se realizó mediante revisiones exhaustivas de la literatura y debates estructurados con las partes interesadas para garantizar que el marco resultante reflejara consideraciones tanto teóricas como prácticas.
Resultados: el estudio introdujo el marco SUFREE (Marco de Supervisión para el Respeto a la Ética), un modelo diseñado específicamente para abordar la supervisión ética en el proceso forense digital. El marco se desarrolló mediante consultas y validación iterativas con la participación de expertos relevantes, con el objetivo de garantizar su solidez metodológica y su aplicabilidad en el contexto indonesio.

Conclusiones: el marco SUFREE ofrece un modelo de supervisión estructurado y centrado en la ética que se espera que mejore la calidad, la integridad y el profesionalismo de las prácticas forenses digitales en Indonesia, contribuyendo así a mejorar la confianza pública en las investigaciones forenses.

Palabras clave: Ética Forense Digital; Marco de Investigación Forense Orientado a la Ética; Marco de Supervisión; Integridad Forense.

INTRODUCTION

The rapid growth of digital technologies has fundamentally transformed both personal and organizational activities, but it has also created unprecedented opportunities for cybercrime and technology-enabled offenses. As digital evidence increasingly becomes central in criminal investigations, the integrity, reliability, and admissibility of such evidence are often contested in legal proceedings. These challenges underscore the critical role of digital forensics as a specialized discipline within the broader forensic sciences, tasked with ensuring that digital evidence is collected, preserved, and analyzed in a manner that meets scientific and legal standards.

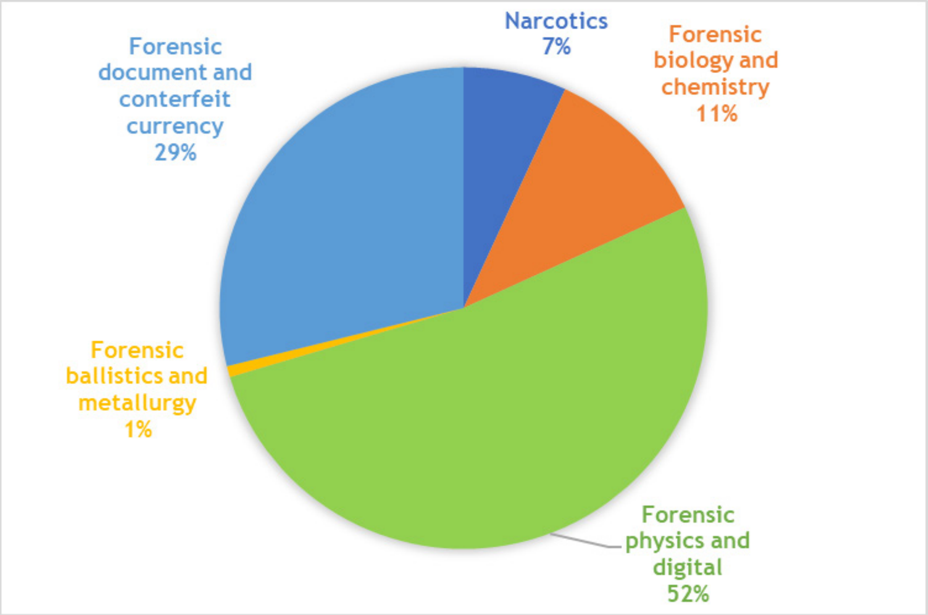

Figure 1. Forensic evidence by type produced in the period January 2022 to September 2024 at the Metro Jaya Police[1]

According to the Metro Jaya Regional Police, between 2022 and September 2024 a total of 170 712 crime cases were recorded, of which 96 456 were investigated using forensic scientific methods.[1] Compared to the total cases that used scientific forensic techniques, 52 % were related to digital evidence as depicted in figure 1. The Metro Jaya Regional Police is located in the capital of Indonesia, which is the area with the largest population nationally, so this data can be an accurate representation of the handling of cases with digital evidence in Indonesia.

Digital forensics is a newer segment within the wider field of forensic sciences. Its origins can be traced to the 1980s in the United States, arising as a reaction to illegal actions involving unapproved modifications to computer systems and devices. While the field of digital forensics is quite recent, the area of forensic science has a rich historical background, offering recognized validity and reliability in criminal inquiries. A significant instance is fingerprint analysis, initially investigated in 1686 as a technique for recognizing individuals, and formally utilized in 1882 as an investigative resource to resolve criminal cases.[2] A growing body of scholarly work in the domain of digital forensics substantiates the view that, despite its advancements, the discipline has yet to achieve methodological maturity, with persistent shortcomings particularly evident in the operationalization and consistent application of established frameworks across diverse investigative contexts.[3] Extant literature in the domain of digital forensics demonstrates that, notwithstanding notable progress, the discipline continues to necessitate methodological refinement, particularly in enhancing procedural mechanisms for the acquisition, examination, and analysis of digital evidence. Comparative insights derived from empirical investigations conducted across multiple jurisdictions further converge on the recommendation that existing digital forensic frameworks require systematic improvement to ensure greater reliability, consistency, and applicability in diverse investigative contexts.[4]

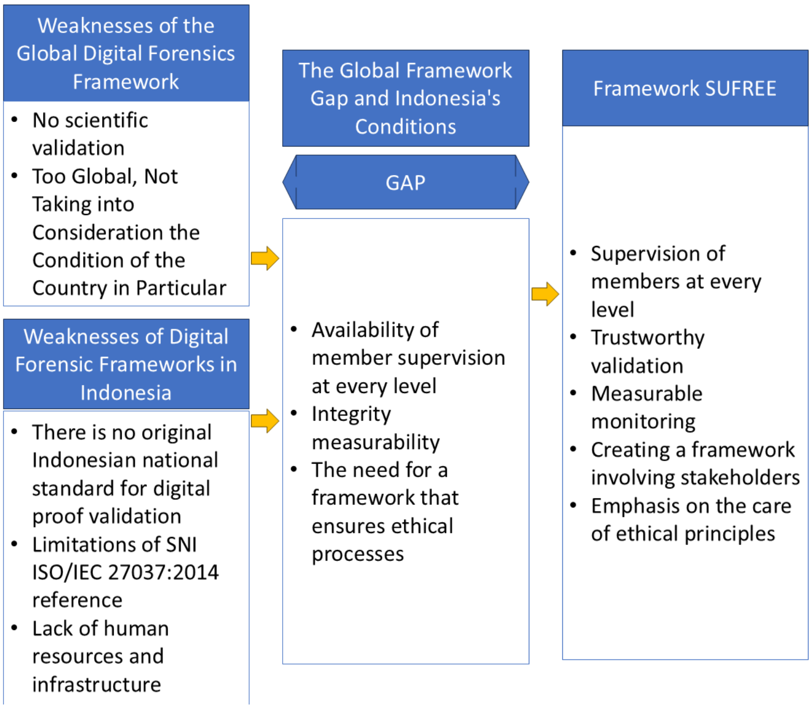
Weaknesses of the Global Digital Forensics Framework
• No scientific validation
• Too Global, Not Taking into Consideration the Condition of the Country in Particular
Weaknesses of Digital Forensic Frameworks in Indonesia
• There is no original Indonesian national standard for digital proof validation
• Limitations of SNI ISO/IEC 27037:2014 reference
• Lack of human resources and infrastructure
The Global Framework Gap and Indonesia's Conditions
GAP
• Availability of member supervision at every level
• Integrity measurability
• The need for a framework that ensures ethical processes
Framework SUFREE
• Supervision of members at every level
• Trustworthy validation
• Measurable monitoring
• Creating a framework involving stakeholders
• Emphasis on the care of ethical principles

Figure 2. Research Gap

As seen in figure 2, the Indonesian framework faces challenges such as the lack of an indigenous national standard for digital evidence validation, the limited applicability of SNI ISO/IEC 27037:2014 or other standards, and insufficient human resources and infrastructure to support large-scale forensic practices. The above research gap is the result of literature studies on digital forensic framework models, namely many forensic digital frameworks developed without strict scientific validation, thus raising doubts in terms of reliability. Then, international frameworks tend to be "one-size-fits-all" and don't always fit local needs. A study by Feby Thealma & Yova Rudelviani states that in Indonesia, standards used in digital forensics, such as ISO/IEC 27037 and SNI ISO/IEC 17025:2017, do not contain specific ethical aspects.(5) Edwin Setiawan & Hartiwiningsih also highlighted in their article that the regulatory challenges and the need for national standardization in digital forensic practices in Indonesia.(6) The challenges mentioned are also compounded by the lack of certified digital forensics examiner who can ensure the validity of the results.(1) Their involvement in an investigation can ensure that ethical principles can be implemented. Therefore, three points of gap research, namely supervision, integrity, and the need for a framework that ensures ethical processes are the basis for making a SUFREE framework.

Within the digital forensics community, both practitioners and academics have increasingly emphasized the critical importance of scientific validation, with the current crisis in the discipline formally acknowledged by leading international standardization bodies.(7) Researchers highlight the importance of expert accreditation and the current gap in regulations for reliability testing, while also stressing the risks of bias due to flawed systems and ethical violations.(8) While the Indonesian government has undertaken initiatives to professionalize the field through the implementation of certification schemes for digital forensic investigators and analysts, there remains a regulatory vacuum concerning the systematic validation and verification of digital forensic processes. As technological advancements accelerate, the scope and sophistication of digital crimes have expanded correspondingly, with social networking platforms and financial technology (fintech) applications emerging as prominent targets for illicit activities. Offenses initiated within social media environments frequently extend into the fintech domain, often facilitated through social engineering tactics and exploitation of vulnerabilities in digital financial services.(9) Such threats are exacerbated when digital forensic investigations are conducted ineffectively, a concern supported by prior research indicating that substandard outcomes in the analysis of digital evidence from social networking cases frequently stem from procedural negligence during evidence acquisition. These deficiencies are further compounded by inappropriate framework implementation and inadequate data management, undermining both investigative accuracy and judicial reliability.

The readiness and maturity of organizational digital forensics capabilities are intrinsically linked to broader risk mitigation strategies for information technology infrastructures. Empirical studies highlight that forensic readiness levels directly influence susceptibility to cyber exploitation.(10) Advanced techniques, including deep learning algorithms, have been applied to detect and classify cyberattacks, thereby supporting the assessment of forensic preparedness. According to Ariffin and Ahmad, evaluating forensic process maturity through the

COBIT framework, supplemented with tailored performance indicators, represents an effective means of measuring organizational investigative capability.[11,12]

Ethical considerations have also emerged as a critical dimension in digital forensics. At the 2016 American Academy of Forensic Sciences (AAFS) conference in the United States, the need for a standardized professional code of ethics drew attention. Seigfried-Spellar, Rogers, and Crimmins recommended grounding the code in seven essential values: respect for individuals, consistency, integrity, autonomy, utility, justice, and competence.[13] The ethical foundation is closely intertwined with the issue of trust, which significantly shapes perceptions of reliability within forensic investigations. Studies emphasize that public trust in digital forensic outcomes is contingent on the perceived integrity of the investigative process, with some findings, such as those reported by Neale[14], suggesting an inverse correlation between trust in process and confidence in investigative results. This dynamic underscores the importance of maintaining professional skepticism and rigorous oversight, a stance echoed by the National Institute of Standards and Technology, which links organizational security to the structural embedding of trust safeguards.[15]

The need to protect the integrity of digital evidence and the forensic process has led many scholars to create frameworks that improve procedural rigor and investigative reliability. Such frameworks are typically conceptualized from varying perspectives, reflecting the specific priorities and methodological orientations of their proponents. Montasari et al.[16] for instance, developed the Integrated Computer Forensics Investigation Process Model (ICFIPM), which provides a structured approach to gathering digital evidence from various sources such as computers, networks, and mobile devices. The ICFIPM emphasizes systematic procedures for evidence collection, analysis, and interpretation, with the overarching objective of ensuring that significant digital evidence is accurately identified and preserved. By mandating meticulous documentation and adherence to high procedural standards, the model ensures legal compliance and reinforces the evidentiary value of forensic findings. Because it combines many elements, these models tend to be complex and difficult to adopt directly by small institutions/investigators with limited resources. It requires trained human resources and strict documentation procedures, which are not always available.

In a related effort, Horsman proposed FRED (Framework for Reliable Experimental Design), which focuses on optimizing the reliability and reproducibility of experimental outcomes through structured and methodical planning.[17] By embedding principles of rigorous design, FRED enhances the trustworthiness of experimental results, thereby strengthening their utility as a basis for informed decision-making in forensic and investigative contexts. This framework has limitations in terms of technical capabilities compared to other digital forensic frameworks. FREDs are less flexible in accommodating different types of complex or difficult forensic investigations.

Similarly, Granja and Rafael developed PREDECI (Practical Research into Digital Evidence and Cybercrime Investigation), a digital forensic system intended to facilitate cybercrime inquiries.[18] PREDECI provides law enforcement agencies with a structured and systematic approach to evidence acquisition, ensuring investigative efficiency and effectiveness while safeguarding evidentiary integrity. This framework takes longer to conduct a thorough forensic investigation compared to some other digital forensic frameworks. PREDECI is also less flexible in accommodating various types of complex or difficult forensic investigations.

Ferguson et al., in their work, described PRECEPT and PRECEPT-4 (Process for Recording and Executing Computer Forensic Examinations and Techniques), a model intended to structure, document, and guide digital forensic examinations.[19,20] PRECEPT offers a procedural roadmap for planning, implementing, documenting, and presenting forensic analyses, thereby enabling both investigators and legal practitioners to conduct and communicate their work in a consistent and methodologically sound manner. Investigators still need operational guidance (tools, SOPs, or algorithms) that are not covered by this framework. This framework emphasizes the importance of ethics, but does not provide a quantitative method/audit standard to measure the extent to which investigators have followed these principles.

Persistent shortcomings in digital forensic practice—ranging from flawed framework implementation to investigator misconduct and undue external interference—have drawn sustained criticism from scholars. These factors collectively compromise the validity of forensic findings and risk precipitating erroneous judicial decisions.[21] Addressing these systemic issues, the present study introduces the SUFREE framework, an ethics-oriented supervisory model specifically designed to standardize digital forensic investigation processes within the Indonesian context.

Participatory Action Research (PAR) is employed in this study as the primary methodological foundation for developing an ethical digital forensic framework. Unlike conventional top-down approaches that often produce rigid models detached from field realities, PAR emphasizes collaboration, iteration, and active involvement of practices throughout the research process. Its unique value lies in enabling certified digital forensic experts, academics, and relevant stakeholders to jointly validate, monitor, and refine each stage of the framework. By adopting PAR, this study ensures that the proposed framework is not only theoretically robust but also contextually grounded, ethically responsive, and practically applicable across diverse investigative scenarios.

This participatory and action-based methodology therefore constitutes a key innovation that distinguishes the present work from existing studies in the field.

METHOD

This study employed an observational approach, followed by the application of Participatory Action Research as the primary development approach.(22) The observation stage was conducted to examine the manifestations and underlying causes of ethical breaches committed by digital forensic practitioners, whereas the PAR approach was utilized to analyze the iterative cycles occurring in real-world practice. Rooted in the principles of social practice action research, this methodological design seeks to achieve continuous improvement through a cyclical process, thereby enabling the identification of systematic and replicable procedural steps.(23) PAR, as a research paradigm, emphasizes collaborative action undertaken by a group with the explicit goal of enhancing ongoing practices. While predominantly qualitative in orientation, PAR also accommodates the integration of quantitative techniques to support measurement and validation.

PAR was not chosen merely as an innovative approach, but as an essential strategy to address two persistent problems in digital forensic practice: recurring ethical breaches in evidence handling, and limited practitioner engagement with top-down frameworks, which often leads to poor adoption. By embedding participation, iteration, and collaborative decision-making, PAR enabled the active involvement of certified digital forensic experts, law enforcement officers, and academics to ensure that the framework is both ethically robust and contextually relevant to the Indonesian environment. According to the observations of Gaskins et al.(24), this methodological approach has yet to gain broad understanding and acceptance within the engineering field, primarily due to the slow pace at which methodological changes are adopted in this domain. Nevertheless, their characterization of PAR as a method that is elegant, impactful, and highly influential underscores its potential value. The approach can inspire participants to generate innovative solutions that address both their own concerns and the focal issues of the research team.

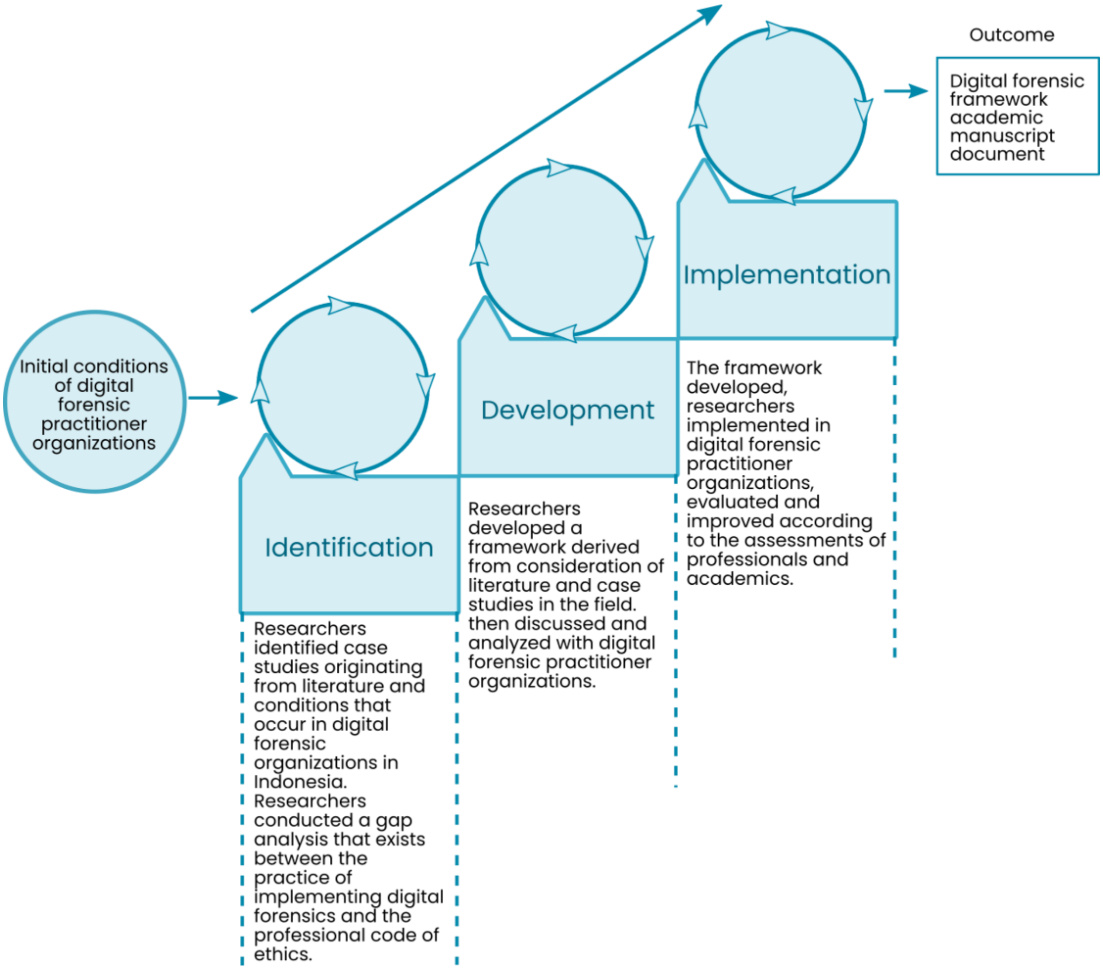
Outcome
Digital forensic framework academic manuscript document
Initial conditions of digital forensic practitioner organizations
Identification
Development
Implementation
Researchers identified case studies originating from literature and conditions that occur in digital forensic organizations in Indonesia. Researchers conducted a gap analysis that exists between the practice of implementing digital forensics and the professional code of ethics.
Researchers developed a framework derived from consideration of literature and case studies in the field. then discussed and analyzed with digital forensic practitioner organizations.
The framework developed, researchers implemented in digital forensic practitioner organizations, evaluated and improved according to the assessments of professionals and academics.

Figure 3. The PAR method for designing a digital forensic framework

As illustrated in figure 3, the action research process follows an iterative cycle that continues until optimal conditions are achieved. This model places significant emphasis on active participant involvement, ensuring that the final outcomes align closely with the realities observed in the field.

Iterative cycles and data collection techniques

PAR was conducted in three iterative cycles:

1. Identification Phase
   - Conducted via structured interviews with all participants.
   - Responses were recorded, transcribed, and thematically coded.

2. Development Phase
   - A series of two focus group discussions (FGDs) were organized with mixed participants (law enforcement, academics, practitioners).
   - Topics included: validation mechanisms, supervisory structures, and weaknesses of existing frameworks.
   - Each FGD lasted 2 hours, facilitated by the research team, and recorded for analysis.

3. Implementation and Testing Phase
   - Draft versions of the SUFREE framework were tested against two case-based scenarios simulating real-world investigations (The source of the case comes from the Cyber Security Incident Response Team from 'Aisyiyah University of Yogyakarta).
   - Feedback was collected via Likert-scale surveys and open-ended expert critiques.
   - The results of the calculation from the survey are processed using AHP to obtain performance conclusions
   - Framework was revised after each cycle based on participant input.

As a collaborative research approach, PAR ensures stakeholder participation in identifying problems, analyzing them, evaluating strategies, and creating and testing frameworks or solutions aimed at specific challenges.[25] Iterations are carried out on each cycle at least one to three times. In this research, during the development and implementation phases, the iteration can be up to two times to ensure the results of each discussion and assessment.

Participants and recruitment

A total of 5 participants were involved across three PAR cycles. They consisted of:

- 4 certified digital forensic examiners, and
- 1 academics specializing in digital forensics.

Participants were recruited through purposive sampling, targeting individuals with extensive forensic experience and ethical certification, as well as through formal invitations issued via professional networks and academic partnerships. All participants' identities are kept confidential in this publication regarding the personal data protection policy of the institution they originated from. No ethical clearance was made for this research however all participants provided informed consent and agreed to maintain confidentiality throughout the study.

Validation Procedures

Validation of the SUFREE framework involved expert judgment across three criteria from each stages of the framework:

1. Identification: accuracy, completness, speed.
2. Preservation: data integrity, security, and speed.
3. Examination: accuracy of tool use, efficency, completeness of results.
4. Analysis: accuracy of analysis, reliability of results, objectivity.
5. Documentation: completeness, consistency, accuracy of the conclusion.

Experts rated each criterion using a 5-point Likert scale, supplemented with qualitative commentary. The Likert-scale scores were then processed using the Analytical Hierarchy Process (AHP) to provide a weighted evaluation of each criterion. This allowed the study to capture not only the overall agreement but also the relative importance assigned by experts to different aspects of the framework.

RESULTS

In this study, five expert participants were engaged through focus group discussions (FGDs) and in-depth interviews, consisting of both practitioners and academics with more than five years of professional experience in digital forensics. Their dual perspectives as field investigators and researchers positioned them as critical stakeholders, contributing actively to the conceptualization and refinement of the framework.

The discussions revealed structural challenges in Indonesian forensic practice. The most pressing issue is the absence of a nationally endorsed standard, which forces reliance on international frameworks such as ISO/IEC 27037. While authoritative, these standards do not fully align with the local investigative and judicial context, leading to inconsistent practices and frequent disputes over the admissibility of evidence. In addition, the limited number of certified forensic professionals has created capacity gaps as cybercrime cases increase. Ethical shortcomings were also identified, ranging from lapses in evidence handling to weak supervision of the chain of custody.

Although established models such as NIJ, NIST, ACPO, IDIF, and PREDECI provide technical structure, expert consensus indicated that they lack integrated mechanisms for ethical oversight and are not adequately adaptable to Indonesia's institutional and regulatory environment. This shortcoming highlights that merely adopting international standards is insufficient to guarantee both procedural reliability and ethical accountability.

At the same time, the empirical findings of this study reveal commonalities across frameworks: all of them provide a core operational structure that offers step-by-step guidance for conducting digital forensic activities, supported by established rules for tool usage and evidence handling. However, expert participants stressed that Indonesia requires a dedicated framework tailored to its socio-cultural and legal landscape. Such a framework must retain the procedural rigor of existing models while embedding supervisory validation and ethical safeguards to ensure both reliability and admissibility in criminal justice processes. These insights formed the foundation for the development of the Supervisory Framework to Respect Ethics (SUFREE), the central contribution of this study.

Evaluation of digital forensic frameworks

Expert feedback specifically addressed ISO/IEC 27037, a widely adopted standard in Indonesia, noting that while it adequately addresses early-stage identification, it lacks a formalized preparation phase.(26,27) This preparatory stage is critical for ensuring the competence of key forensic actors—including first responders, evidence locators, and specialized forensic analysts—whose qualifications should be substantiated through recognized professional certifications. While participants acknowledged the importance of planning, they argued that the foremost priority of any new digital forensic framework should be the implementation of mechanisms capable of safeguarding both the integrity of the evidence and the investigative process.

As outlined in table 4, participants underscored the urgency of structured training and capacity-building initiatives to cultivate human resources that are both technically proficient and operationally prepared to address emerging cyber threats. Despite incremental growth in the number of certified digital forensic professionals in Indonesia, their availability remains insufficient to meet the escalating demand for cybercrime investigations.(28,29) This shortage is compounded by the uneven geographical distribution of experts across the country. Additionally, participants identified inadequate research and innovation infrastructure as a significant constraint, limiting the advancement and modernization of digital forensic practices.(30)

Table 4. Assessment outcomes of the digital forensic framework

Evaluation Aspect	Disadvantages	Recommendation
Framework Completeness	Reduced emphasis on the presentation and safeguarding of evidence.	The framework must encompass all aspects of digital forensics management, including human resources, evidence, tools, presentation, and preservation.
Suitability with Conditions in Indonesia	ISO/IEC 27037 places less emphasis on preparing forensic experts and their competencies.	The framework must be tailored to accommodate the distinct characteristics and circumstances specific to Indonesia.
Technology Development	Digital forensic tools are comparatively less advanced.	There is a need for more advanced digital forensic tools.
Government Regulation	Regulations are deemed outdated and are not equipped to foresee future advancements.	Regulations that are current and capable of anticipating future developments in digital forensics are required.
Forensor Quality	The training and development of human resources are considered suboptimal.	Optimal training and development of human resources, along with the equitable distribution of forensic resources, are required.
Infrastructure	Infrastructure for research and innovation is lacking.	Sufficient infrastructure for research and innovation is required.

While table 4 outlines the assessment outcomes across key dimensions, several critical weaknesses of existing frameworks warrant deeper reflection highlighted by experts. First, the limited attention to evidence presentation and safeguarding indicates that most frameworks remain overly focused on technical acquisition and analysis, neglecting the communicative and legal dimensions that are essential for admissibility in court. Second, the dependency on ISO/IEC 27037 highlights a structural misalignment with Indonesia's socio-legal context, as the standard does not sufficiently prepare practitioners for context-specific challenges nor integrate competency-based certification schemes. Third, the underdevelopment of forensic tools and infrastructure, coupled with outdated regulatory provisions, demonstrates a systemic lag in responding to rapidly evolving cyber threats. Finally, the lack of structured pathways for human resource development suggests that ethical oversights are not merely procedural gaps but reflect deeper institutional shortcomings. These limitations collectively reinforce the necessity of a new approach—one that embeds supervisory oversight and ethical validation as core mechanisms, as operationalized in the SUFREE framework.

In the Indonesian context, the digital forensics domain is confronted with the dual challenge of accelerating technological advancements and the escalating sophistication of cyber threats. To address these dynamics, expert participants underscored the necessity for policy interventions that not only mitigate existing forensic gaps but also ensure that investigative practices consistently adhere to stringent ethical standards. These insights provided a critical foundation for formulating a contextually relevant and ethically robust forensic framework subsequently realized in the development of the SUFREE (Supervisory Framework to Respect Ethics) model, designed to align with Indonesia's socio-cultural, legal, and regulatory landscape. Through the consensus established in this study, four critical aspects were determined to be essential for the development of a framework designed to prevent ethical violations, thus ensuring that ethical standards are maintained in digital forensic investigations, as depicted in figure 4.

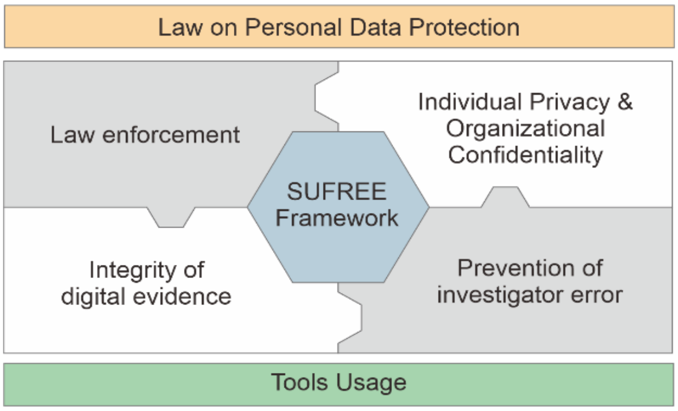
Law on Personal Data Protection
Law enforcement
Individual Privacy & Organizational Confidentiality
SUFREE Framework
Integrity of digital evidence
Prevention of investigator error
Tools Usage

Figure 4. Essential components of the framework

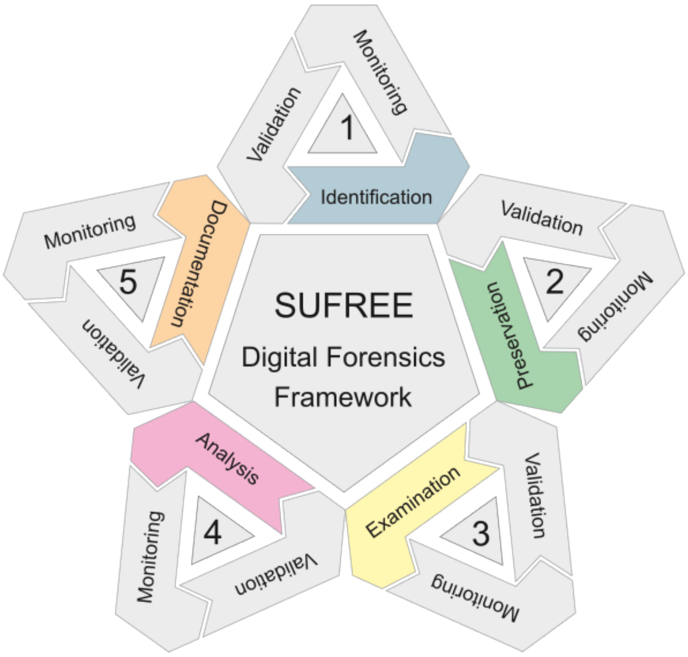

Figure 5. SUFREE star diagram

Digital forensic practices are requiredto adhere to the legal mandates and procedural standards applicable within the jurisdiction of the respective country.[31] The absence of universally accepted norms governing the management and preservation of digital evidence poses challenges to its admissibility in judicial proceedings, thereby necessitating a synergistic collaboration between the legal and technological domains.(32) In formulating the proposed framework document, it is imperative to establish an interdisciplinary consortium comprising representatives from the cyber community, academia, governmental bodies, industry stakeholders, law enforcement agencies, and other relevant actors. The consortium should be established as a single platform for discussing and adapting the framework's provisions to Indonesia's social, legal, and technological conditions.

It is shown in figure 5 that SUFREE includes five core phases, namely identification, preservation, analysis, documentation, and presentation. These phases are derived from the simplified procedural model proposed by the National Institute of Standards and Technology (NIST), which represents one of the most widely adopted methodologies among researchers. The NIST framework remains adaptable, allowing for modifications to suit the specific operational contexts of different organizations.(33) A detailed description of the SUFREE stages, with particular emphasis on the validation and monitoring processes integrated into each phase, is presented in table 5.

Table 5. Validation and monitoring for every stages

Stages	Validation	Monitoring
Identification	Digital forensic experts (supervisors) ensure that all relevant evidence has been identified and collected.	Experts (supervisors) assess the performance of technical workers in the identification process and confirm that no evidence is missed.
Preservation	Experts (supervisors) ensure that the preservation techniques used are in accordance with the set standards.	Experts (supervisors) monitor and assess the process to ensure the evidence remains intact and not affected by external factors.
Examination	The evaluation of inspection tools and techniques is conducted by experts (supervisors) to guarantee accurate analysis outcomes.	Experts (supervisors) are responsible for assessing the efficiency and effectiveness of technical workers in applying forensic tools and methodologies.
Analysis	The results are verified by experts (supervisors) to ensure the absence of bias or mistakes.	It is assessed by experts (supervisors) whether the analysis results are correct and consistent with the available data.
Documentation	The documentation is reviewed by experts (supervisors) to ensure its completeness and conformity with standard procedures.	The completeness of the documentation is assessed by the expert (supervisor).

Monitoring and validation in the SUFREE framework are carried out by a supervisory panel consisting of certified professionals with expertise in digital forensics. This process is required to protect the integrity of digital evidence and to maintain ethical standards in forensic practice. The inclusion of certified experts is particularly relevant in the Indonesian context, where investigative teams are often required to operate under time constraints, while the availability of certified practitioners remains limited, resulting in instances where ethical oversight of the digital forensic process is lacking.

In the SUFREE digital forensics framework, monitoring and validation are carried out by supervisory personnel to safeguard integrity and ensure quality at every stage of the investigation. Certified experts are assigned to validate techniques and monitor the performance of forensic technicians throughout the phases of Identification, Preservation, Examination, Analysis, and Documentation. This structured oversight is illustrated in figure 6.

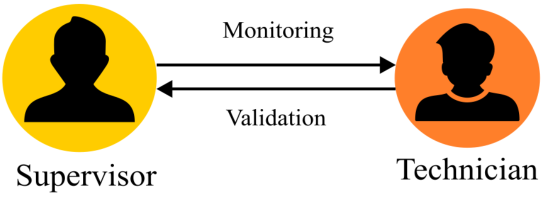

Figure 6. Validation and monitoring mechanism

The validation process is carried out through a comprehensive review of the engineer's work to ensure alignment with established standard operating procedures (SOPs) and predefined methodologies. This process involves verification by the supervisor that digital evidence is correctly identified, preservation techniques are properly applied, examination tools are effectively used, analyses are conducted objectively without bias, and documentation is completed in full.

Table 6. Criteria for monitoring in every stages

Stages	Monitoring criteria
Identification	Accuracy
	Completeness
	Speed
Preservation	Data Integrity
	Security
	Speed
Examination	Accuracy of Tool Use
	Efficiency
	Completeness of Results
Analysis	Accuracy of Analysis
	Reliability of Results
	Objectivity
Documentation	Completeness
	Consistency
	Accuracy of the conclusion

The criteria applied at each stage vary, with three agreed-upon criteria established by the researchers for every phase, as presented in Table 6. Within the SUFREE framework, monitoring is conducted using the Analytical Hierarchy Process (AHP) to objectively assess technicians based on these criteria. AHP serves as a widely adopted decision-making approach for addressing multi-criteria decision-making (MCDM) problems and is applicable to various real-time contexts.[34]

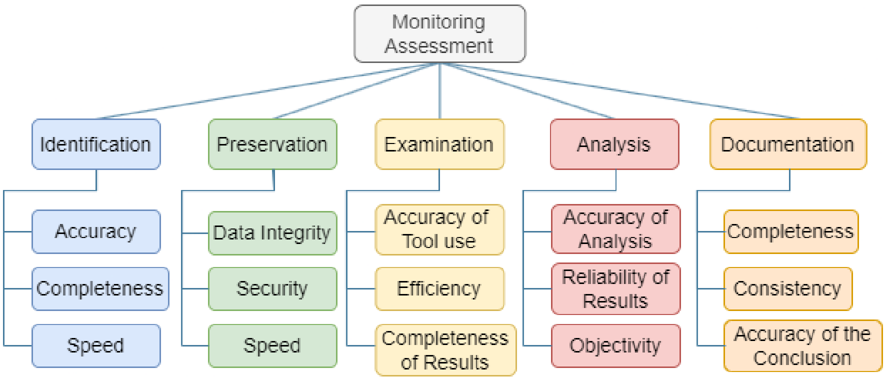

Figure 7. Hierarcy of AHP for monitoring assessment

The enhancement of the SUFREE (Supervisory Framework to Respect Ethics) framework for digital forensic investigations necessitates that the systematic monitoring of technical personnel performance be subjected to rigorous assessment. This monitoring process is operationalized through the application of the Analytic Hierarchy Process (AHP), wherein the evaluation criteria are structured within a multi-level hierarchical model, as illustrated in figure 7. The hierarchical arrangement within the AHP facilitates the determination of relative weights and priorities for each stage of the digital forensic workflow, aligning with the overarching objective of the framework—namely, to ensure an objective, transparent, and comprehensive mechanism for monitoring and validating the performance of technical practitioners.

Beyond the procedural validation and monitoring, the SUFREE framework is theoretically anchored in established ethical principles within digital forensics. The supervisory mechanism is designed not only to verify technical compliance but also to embed ethical accountability grounded in broader normative theories. Drawing on Seigfried-Spellar et al.[13], the framework incorporates values of integrity, justice, competence, and respect for individuals, ensuring that every procedural step aligns with ethical obligations toward fairness and transparency. This approach resonates with professional accountability theory, where oversight mechanisms serve as safeguards against bias and misconduct, and with deontological ethics, which emphasize the duty to follow established ethical rules regardless of outcome. By embedding these values into supervisory validation, SUFREE advances beyond conventional procedural frameworks and positions itself as an ethically responsive model tailored to Indonesia's socio-legal context.

CONCLUSIONS

This study set out to address the persistent challenges of ethical breaches, weak supervisory oversight, and limited adoption of existing digital forensic frameworks in Indonesia. The research introduced SUFREE (Supervisory Framework to Respect Ethics) as a novel contribution, characterized by its supervisory layer that embeds continuous validation and monitoring by certified forensic experts at every stage of investigation. By employing a participatory action research (PAR) approach, the framework was co-developed and refined collaboratively with practitioners, law enforcement officers, and academics, ensuring that it is both scientifically robust and contextually grounded.

Three key contributions emerge from this study. First, SUFREE advances the field by operationalizing ethics into measurable supervisory mechanisms, thereby bridging the long-standing gap between theory and practice in digital forensics. Second, the integration of multi-criteria evaluation using Likert scales and Analytical Hierarchy Process (AHP) provides an innovative means of weighting any criteria of the stages in the framework. Third, the study demonstrates the value of PAR as an essential methodological strategy, not merely an alternative, for building frameworks that are contextually relevant and practically embraced by stakeholders.

The broader implications of this work extend beyond Indonesia. SUFREE illustrates how ethical supervision can be systematically embedded into forensic processes, offering a transferable model for other jurisdictions facing similar gaps in standards, practitioner certification, and accountability. For policymakers, the findings highlight the urgent need to institutionalize supervisory mechanisms and expand certification programs to ensure the credibility of digital evidence in court. For practitioners, SUFREE provides a structured pathway for ethically sound investigations. For the research community, the study underscores the importance of participatory methodologies and opens avenues for testing the framework across diverse case types and integrating it with emerging forensic technologies such as cloud forensics, IoT forensics, and AI-driven tools.

In sum, SUFREE represents a significant step forward in strengthening the ethical and methodological foundations of digital forensic investigations. By embedding supervision, validation, and participatory engagement into the heart of forensic practice, the framework not only addresses pressing national needs but also contributes to the global discourse on forensic integrity and ethical accountability.

BIBLIOGRAPHIC REFERENCES

1. Bakhtiar HS, Ilyas A, Kholiq A, Bakhtiar HS. The utilisation of scientific crime investigation methods and forensic evidence in the criminal investigation process in Indonesia. Egypt J Forensic Sci. 2025;15(1). https://doi.org/10.1186/s41935-025-00456-y

2. Ashley DuVal. History of Forensic Psychology. https://forensicpsych.umwblogs.org. 2014. https://forensicpsych.umwblogs.org/research/criminal-justice/fingerprint-analysis/

3. Arshad H, Jantan A Bin, Abiodun OI. Digital forensics: Review of issues in scientific validation of digital evidence. J Inf Process Syst. 2018;14(2):346–76.

4. Krivchenkov A, Misnevs B, Pavlyuk D. Intelligent methods in digital forensics: State of the art. Vol. 68, Lecture Notes in Networks and Systems. Springer International Publishing; 2019. 274–284 p. Available from: http://dx.doi.org/10.1007/978-3-030-12450-2_26

5. Farhan NM, Setiaji B. Indonesian Journal of Computer Science. Indones J Comput Sci. 2023. http://ijcs.stmikindonesia.ac.id/ijcs/index.php/ijcs/article/view/3135

6. Setiawan E, Hartiwiningsih H. Optimizing the use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia. Int J Law, Crime Justice. 2025;2(2):73–86.

7. Hughes N, Karabiyik U. Towards reliable digital forensics investigations through measurement science. WIREs Forensic Sci. 2020;2(4):1–11.

8. Henseler H, van Loenhout S. Educating judges, prosecutors and lawyers in the use of digital forensic experts. DFRWS 2018 EU - Proc 5th Annu DFRWS Eur. 2016;24:S76–82. http://dx.doi.org/10.1016/j.diin.2018.01.010

9. Arshad H, Jantan A, Omolara E. Evidence collection and forensics on social networks: Research challenges and directions. Digit Investig. 2019;28:126–38. https://doi.org/10.1016/j.diin.2019.02.001

10. Ayangbekun OJ, Bankole OF, Saka BA. Analysis of security mechanisms in Nigeria E-banking platform. Int J Electr Comput Eng. 2014;4(6):837–47.

11. Ariffin KAZ, Ahmad FH. Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Comput Secur. 2021;105:102237. https://doi.org/10.1016/j.cose.2021.102237

12. Bankole F, Taiwo A, Claims I. An extended digital forensic readiness and maturity model. Forensic Sci Int Digit Investig. 2022;40.

13. Seigfried-Spellar KC, Rogers M, Crimmins DM. Development of A Professional Code of Ethics in Digital Forensics. Annu ADFSL Conf Digit Forensics, Secur Law. 2017;9(c):15. https://commons.erau.edu/adfsl/2017/papers/12

14. Neale C, Kennedy I, Price B, Yu Y, Nuseibeh B. The case for Zero Trust Digital Forensics. Forensic Sci Int Digit Investig. 2022;40:301352. https://doi.org/10.1016/j.fsidi.2022.301352

15. NIST. Zero Trust Architecture. Control Priv Use Data Assets. 2022;127–34.

16. Montasari R, Peltola P, Evans D. Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. Commun Comput Inf Sci. 2015;534:83–95.

17. Horsman G. Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. Comput Secur. 2018. https://doi.org/10.1016/j.cose.2017.11.009

18. Granja FTM, Rafael GDR. Model for digital evidence preservation in criminal research institutions-PREDECI. Int J Electron Secur Digit Forensics. 2017;9(2):150–66.

19. Ferguson RI, Renaud K, Wilford S, Irons A. PRECEPT: a framework for ethical digital forensics investigations. J Intellect Cap. 2020;21(2):257–90.

20. Renaud K, Bongiovanni I, Wilford S, Irons A. PRECEPT-4-Justice: A bias-neutralising framework for digital forensics investigations. Sci Justice. 2021;61(5):477–92. Available from: https://doi.org/10.1016/j.scijus.2021.06.003

21. Kumar U, Gaud N, Joshi C. A Framework for Digital Forensic Investigation using Authentication Technique to maintain Evidence Integrity. Int J Comput Appl. 2016;154(6):1–3.

22. Buckles DJ, Chevalier JM. Participatory action research: Theory and methods for engaged inquiry. 2nd ed. Oxon: Routledge; 2019. 1–474 p.

23. Kember D. Action Learning and Action Research: Improving the Quality of Teaching and Learning. Vol. 9, Quality Assurance in Education. London: Kogan Page; 2000. 54–56 p.

24. Gaskins W, Guy B, Arthur B. Reflections on Implementing Participatory Action Research in Engineering. J Educ Dev. 2023;7(3):18.

25. Eelderink M, Vervoort JM, van Laerhoven F. Using participatory action research to operationalize critical systems thinking in social-ecological systems. Ecol Soc. 2020;25(1).

26. Faizal A, Luthfi A. Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis. J Inf Syst Informatics. 2024;6(2):701–18.

27. Sudyana D. Analysis and Evaluation Digital Forensic Investigation Framework Using Iso 27037:2012. Int J Cyber-Security Digit Forensics. 2019;8(1):1–14.

28. Nyman A, Rutberg S, Lilja M, Isaksson G. The Process of Using Participatory Action Research when Trying out an ICT Solution in Home-Based Rehabilitation. Int J Qual Methods. 2022;21:1–8.

29. Iman N, Susanto A, Inggi R. Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). J Telekomun dan Komput. 2020;9(3):186.

30. Ramadhani E, Hariyadi D, Nastiti FE. A Bibliometrics Analysis of Digital Forensics Research in Indonesia Based on Scopus Index: 2012-2021. In: 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA). 2022. p. 1–6.

31. Jordaan J. Ensuring the Legality of the Digital Forensics Process in South Africa. Int J Comput Appl. 2013;68(23):36–9.

32. A. Rakha N. Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Vol. 16, Mexican Law Review. 2024. 23–54 p.

33. Kent K, Chevalier S, Grance T, Dang H. Guide to Integrating Forensic Techniques into Incident Response. Vol. 800, The National Institute of Standards and Technology. 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

34. Cortinas BF, Contreras-Salinas J, López-Irarragorri F, De La Hoz Granadillo E. Multicriteria Methodology Based on Hierarchical Process Analysis (AHP) for the Selection and Evaluation of Companies in an Entrepreneurial Project Accelerator. In: MOL2NET'21, Conference on Molecular, Biomedical & Computational Science and Engineering, 7th ed. 2021.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Arizona Firdonsyah.
Data curation: Arizona Firdonsyah.
Formal analysis: Arizona Firdonsyah.
Research: Arizona Firdonsyah.
Methodology: Arizona Firdonsyah.
Project management: Arizona Firdonsyah.
Resources: Purwanto.
Software: Arizona Firdonsyah.
Supervision: Purwanto.
Validation: Imam Riadi.
Display: Ammar Fauzan.
Drafting - original draft: Mahrus Ali.
Writing - proofreading and editing: Ammar Fauzan.