JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2024, VOL 7, NO 3

Supervision-Based Digital Forensics Framework to Respect Ethics using Participatory Action Research Method

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

[1,2]Doctoral Program of Information System, Postgraduate School, Universitas Diponegoro, Semarang, Indonesia
[3]Department Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: arizona@unisayogya.ac.id

Abstract: The handling of digital forensic cases significantly impacts the public interest. A lack of integrity in the digital forensic process, often caused by non-adherence to ethical codes, can result in a loss of trust in investigation outcomes. This research aims to identify, analyze, and evaluate existing digital forensic frameworks. While many countries have developed standard frameworks tailored to their specific needs, a notable gap exists in Indonesia, which requires attention from both academics and practitioners in the field of digital forensics. This study employed the Participatory Action Research (PAR) method, engaging stakeholders from both industry and academia. The result is the SUFREE framework (Supervisory Framework to Respect Ethics) which were developed through literature reviews and stakeholder discussions. The new framework is expected to enhance the quality and professionalism of Indonesian digital forensics

Keywords: digital forensics, framework, ethics, investigation

1. Introduction

Digital forensics is a new discipline. The field of digital forensics emerged as a response to crimes in the United States during the 1980s regarding unauthorized modifications to computer devices. The practice of forensic science in general has a long history so that it can be considered valid and reliable in criminal cases. An example of this forensic practice is the study of fingerprints. This study began in 1686 and was used to identify a person, and then in 1882 began to be used in the disclosure of criminal cases [1]. Studies on digital forensics conducted by several researchers reinforce the opinion that digital forensics is still far from perfection, especially in the application of frameworks [2]. Topics in the field of digital forensics based on studies that have been conducted still require improvisation in the forensic process to analyze digital evidence. The facts of studies that have been studied by researchers in various countries lead to recommendations for improving digital forensic frameworks [3]. Digital forensics practitioners and academics are paying particular attention to scientific validation in digital forensics, and the crisis in this field has been recognized by the world's standardization organizations [4]. Scientists and researchers have responded by demanding expert accreditation and discussing the lack of regulations for reliability testing and the danger of bias caused by framework errors and ethical violations by practitioners [5]. The Indonesian government has made efforts to standardize these practitioners with the existence of expert certification for digital forensic investigators and analysts, but there is no specific regulation regarding validation testing of digital forensic processes.

As technology continues to evolve, the potential for digital crime increases. Social networking platforms and financial technology are ideal places for criminals to commit digital crimes. Crimes that occur on social media platforms also have the potential to lead to the fintech domain. Social engineering on social networks and crimes on fintech applications committed by criminals are one of the modus operandi that researchers are concerned about [6]. Digital crime will get worse if the handling of digital forensic investigations is not done properly. Studies that have been conducted by several researcher’s state that the poor results of digital evidence analysis in social networking cases are caused by negligence in the process of collecting digital evidence [6]. Poor digital evidence

disclosure results can occur due to inappropriate framework implementation and lack of data management.

The readiness and maturity of digital forensics in organizations is related to risk mitigation measures for information technology infrastructure. Studies on organizational security state that the level of forensic readiness affects the risk of exploitation crimes [7]. In fact, a deep learning technique can also be used in identifying and classifying attacks to recognize readiness in digital forensics. The level of maturity and readiness of the forensic process according to Ariffin and Ahmad needs to be tested using the COBIT framework and integrated with certain indicators [8]. The framework for testing the level of maturity of digital forensics is considered the effective tool to measure the readiness of forensic capabilities in an organization [9]. Discussions about the importance of ethics in the field of digital forensics in America began in 2016 at the American Academic of Forensic Science (AAFS) conference. The discussion led to an agreement on the necessity of standardized professional code of ethics in the field of digital forensics. Seigfried-Spellar, Rogers, and Crimmins recommended that the development of the code of ethics should be based on seven values: consistency, respect of individuals, autonomy, integrity, justice, utility, and competence [10].

Digital forensics has a major influence on the public interest. Studies related to digital forensics suggest that monitoring the results of digital forensic investigations is very important because it will affect public trust. Trust in the digital forensic investigation process has been under the spotlight of many parties, including academics and researchers. Neale in an article written according to the results of his research states that there is an issue of trust in the reliability of case disclosure using digital forensics, in the form of an inverse relationship to the trustworthiness of the digital forensic process, namely the more the process is trusted, the less confidence in the reliability of the results [11]. Opinions regarding reliability and security in the field of digital forensics are heavily influenced by aspects of trust. Parties involved in investigating cases related to digital devices need to increase their level of scepticism in the digital forensics process. NIST issued a publication on how the trust aspect affects security in a company [12]. The 'trust' in this architecture refers to how the framework ensures that violations are prevented, whether due to human error or intentional ethical breaches.

The conditions that have been criticized by researchers about the code of ethics and trust in the field of digital forensics are inseparable from many results of digital forensic investigations that are not ideal. These results occur due to many factors, ranging from improperly implemented investigation frameworks, fraud on the part of those conducting the investigation, and parties who intervene in the investigation. Incorrect implementation of the framework and fraud on the results of digital forensic work can result in poor execution of a decision [13].

In the current research, Sufree framework is proposed as a standard framework which is suitable for digital forensics investigation process in Indonesia. There are 5 parts in this article. Section 1 presents the importance of digital forensics science and the development of issues in digital forensics. Section 2 presents several references related to the research. Section 3 describes PAR method used to conduct the research. Section 4 presents the results based on PAR research method. The final results of the research are summarized in section 5.

2. Related Works

The importance of maintaining the integrity of evidence and the digital forensic process has led many researchers to propose a framework aiming at improving the process. Frameworks are usually proposed based on different aspects depending on the researcher's point of view.

Montasari, et al. proposed The Integrated Computer Forensics Investigation Process Model (ICFIPM). ICFIPM is a forensic investigation process framework or model specifically designed to collect digital evidence from various sources such as computers, networks and mobile devices. This model focuses on the collection, analysis, and interpretation of digital evidence with the goal of identifying and collecting significant digital evidence [14].

ICFIPM demands a thorough, organized, and all-encompassing forensic investigation approach for gathering, analyzing, and interpreting digital evidence. ICFIPM enables investigators to conduct the process with precision, proper documentation, and high standards, ensuring compliance with legal procedures.

Horsman explained his framework, namely Framework for Reliable Experimental Design (FRED) that is the framework or model used to design and conduct reliable and reproducible experiments [15]. The goal of FRED is to optimize the reliability of experimental results through careful and structured planning. FRED can be used to ensure that the experiments carried out have high reliability and trustworthiness, so that the experimental results can be used as a basis for decision making.

Granja and Rafael proposed PREDECI (Practical Research into Digital Evidence and Cybercrime Investigation). This framework is a digital forensics framework designed to assist cybercrime investigations [16]. PREDECI is a significant tool for law enforcement, enabling cybercrime investigations to be conducted in a structured and systematic manner, guaranteeing the efficient and effective collection of evidence.

Ferguson, et al. described in their work about digital framework called PRECEPT. PRECEPT (Process for Recording and Executing Computer Forensic Examinations and Techniques) is a digital forensics framework used to guide and record the digital forensic examination process [17]. PRECEPT helps law enforcement and digital forensic professionals in planning, implementing, documenting and presenting the results of digital forensic examinations in a structured and systematic manner.

Horsman in another research proposed new framework called PPDPP (Preparation, Collection, Analysis, Presentation, and Preservation). The digital forensic framework was designed to assist the cybercrime investigation process [18]. PPDPP is very useful for law enforcement and digital forensics professionals in carrying out cybercrime investigations in a structured and systematic manner, making it possible to collect evidence effectively and efficiently.

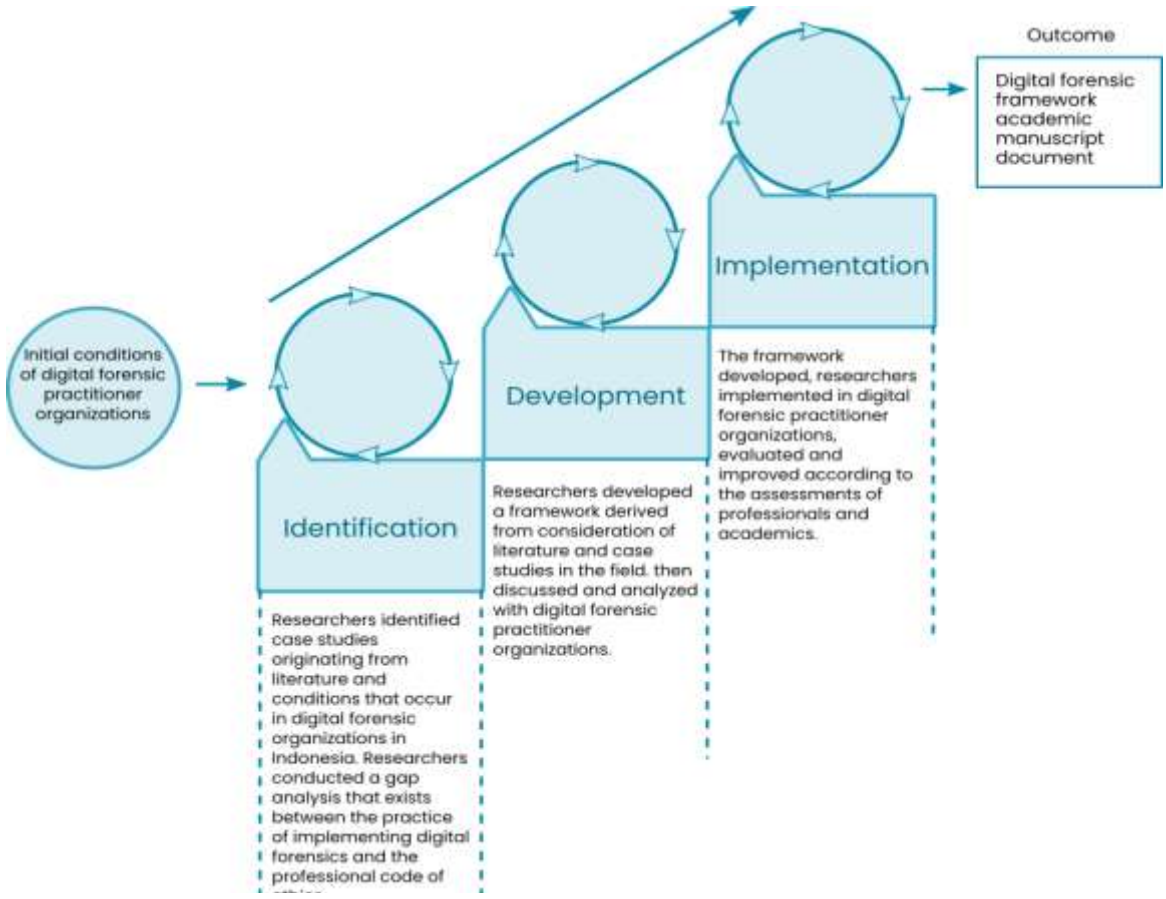

Figure 1. PAR Stages for Developing the Academic Paper Document of the Digital Forensics Framework

3. Method

This research used observation method followed by participatory action research (PAR) as the analysis stage [19]. Observation was carried out to analyze the symptoms and causes of digital forensic practitioners committing ethical violations, while the PAR method was used to analyze the cycles which occur in the field. This design method is based on social practice action research which aims to get improvement from a cyclical process so that systematic steps can be found [20]. PAR is a research method that emphasizes action practices carried out by a group of people with the aim of improving the ongoing cycle. PAR research is predominantly qualitative in nature, although quantitative methods can be used for measurement.

PAR method is very rare and even very difficult to find in research which as a STEM science basis. Based on what Gaskins, Guy, and Arthur stated in their article, this method is not well understood and accepted in the field of engineering, because this field implement methodology changing in a slow manner [21]. However, their ideas mentioning that the method is very beautiful, impactful, and powerful are brilliant. PAR method can be used to motivate participants to create new things which are necessary in the problems that they and the researchers focus on.

As shown in Figure 1, action research cycle was iterative until ideal conditions were achieved. This model relies on the participation of participants so that the expected final results are in accordance with the real conditions in the field. The PAR method in this research has three major stages with several cyclical phases. Each stage describes how the research team consisting of academics, practitioners, and organizations digital forensics is involved in the identification, development, and implementation of solutions to the problems raised in this research.

The three major stages of the research steps are Identification, Development, and Implementation that can be detailed into five phases namely Identification, Analysis, Evaluation, Development, and Testing. These steps are described in Table 1. The results of this research will then be presented in dissemination to practitioner organizations and academics.

Table 1. Details of research steps

Steps	Description
Identification	Jointly identify various cases of ethical violations in digital forensics
Analysis	Conduct joint analysis of knowledge gaps and practices of ethical violations in digital forensics
Evaluation	Evaluate various framework models related to ethical violations in digital forensics
Development	Jointly develop a new framework for ethical violations in digital forensics
Testing	Examine framework documents related to ethical violations in digital forensics

Participatory Action Research (PAR) is a research methodology that involves active participation from stakeholders in identifying, analyzing, evaluating, developing, and testing a framework or solution to address a particular issue or problem [22]. In the context of developing a digital forensics framework, PAR entails engaging various stakeholders such as digital forensics experts, law enforcement agencies, cybersecurity professionals, and potentially even representatives from the legal sector or private industry.

The process typically begins with the identification phase, where stakeholders collaborate to identify key challenges, requirements, and objectives for the digital forensics' framework. This may involve conducting surveys, interviews, or focus group discussions to gather insights and perspectives from diverse stakeholders. Once the challenges and objectives are identified, the analysis phase involves a detailed examination of existing digital forensics methodologies, tools, and practices. This

analysis helps identify gaps, limitations, and opportunities for improvement in current approaches to digital forensics. In the evaluation phase, stakeholders assess potential solutions and methodologies proposed for the framework. This may include evaluating the feasibility, effectiveness, and scalability of different approaches, as well as considering factors such as cost, resource requirements, and legal implications.

Based on the findings from the evaluation phase, the development phase involves designing and refining the digital forensics framework. This may involve creating workflows, protocols, guidelines, and standards for conducting digital investigations, as well as developing or adapting tools and technologies to support the framework.

Finally, the testing phase involves validating the effectiveness and reliability of the developed framework through practical testing and validation exercises. This may include conducting simulated forensic investigations, running test cases on real-world data sets, and soliciting feedback from stakeholders to identify areas for further refinement and improvement.

4. Result and discussion

4.1 Identify the digital forensics framework

Based on FGDs and interviews conducted by researchers, expert participants' understanding of the digital forensic framework is that it refers to a systematic approach used to investigate cyber events or incidents with several objectives with the output of presenting digital evidence effectively. There were three expert participants who were asked for information in this study. The participants came from academia who have been pursuing the field of digital forensics for more than five years. They were considered, by the researchers, as stakeholders who contribute to the formation of forensic digital framework by actively involving it.

The first expert explained that a digital forensic framework could provide a structured approach to investigate crimes or incidents and ensure that digital evidence could be effectively collected, analyzed, and presented. The second expert explained that the purpose of investigating was to collect digital evidence effectively, analyze the evidence collected, and document digital evidence. The third expert explained that the forensic digital framework was used as a tool in an organization or state institution. Some digital forensics frameworks had similarities such as the use of terms at their stages but differ in the technical details in them. The establishment of the framework was carried out with the aim of supporting the process of data collection and interpretation of electronic evidence. Based on the forum group discussion (FGD) conducted in April 2024, expert participants said that the stages of preparing the framework began with initial identification. Some experts determined it with an assessment to understand the incidence of the case to be analyzed.

The existence of this framework is to assist forensors or digital forensics professionals in developing a structured methodology to support the identification process of data collection and interpretation of electronic evidence. The preparation of the digital forensic framework goes through several stages, namely: identification, planning, evidence collection, analysis and interpretation of documentation and maintaining the integrity of the evidence or maintaining the authenticity of the evidence. Digital evidence must be obtained legally and verified for validity by computer science and information technology experts to be valid in criminal trials [23,24]. Therefore, validation steps from experts are important to carry out in the investigation process.

Regarding the identification of digital frameworks, the participants mentioned that there are several frameworks that may be familiar to forensors, such as: National Institute of Standards Technology. (NIST), National Institute of Justice (NIJ), International Digital Investigation Framework (IDIF), Scientific Working Group on Digital Evidence (SWDGE), Association of Chief Police Officers (ACPO) and ISO. The existence of these frameworks is very helpful in ensuring that the procedures used by forensors are in accordance with the standards made so that there is no abuse or deviation in the proof process until the last stage, namely the proof of digital evidence. Furthermore, in the view of the participants, each framework had a difference. The most obvious difference between the major

digital forensics frameworks was in their use. In general, each of these frameworks has a different purpose, for example in the use for forensic analysis on mobile devices and network devices [23]. This has shown a difference in the purpose of use so that the framework must be different.

Prayudi argues that the framework has not yet depicted the interaction between humans, digital evidence, and processes, so it needs a business model approach [25]. This explanation is in line with Casey's opinion that digital forensics has a human component, rules, and tools [26]. Two participants argued that a framework built to prioritize ethics should be able to describe the relationship between technical officers or police officers and certified digital forensic experts. They said that the standardization of the use of tools in the digital forensic framework needs to be explained

Table 3. Framework identification aspects

Aspects	**Explanation**
Definition	A systematic approach to cyber investigations with the aim of effectively presenting digital evidence
Objective	Assist forensics in developing a structured methodology for the identification, data collection and interpretation of electronic evidence
Stages	1. Identification 2. Collection 3. Examination 4. Analysis and interpretation 5. Documentation
Known Frameworks	NIST, NIJ, IDIF, SWDGE, ACPO, ISO
Framework Benefits	Ensure forensic procedures are standardized, preventing evidentiary irregularities
Framework Differences	1. Intended use (forensic analysis of mobile devices vs. networks) 2. Programming language (depending on the type of analysis) 3. Category (commercial vs. open source)
Framework Equation	Provides a basic work structure as a step-by-step tool in digital forensic work, including rules and rules for using digital forensic tools

In addition to the differences between frameworks, the field findings of this research show that there are similarities between all frameworks. In general, the similarity between frameworks is that they provide a basic work structure that is a tool that guides step by step in carrying out digital forensic work. The basic work structure includes rules and regulations in using digital forensic tools. An explanation of the identification of digital forensic frameworks can be seen in Table 3.

Considering the identification above, the researchers discussed with experts about the suitability of these frameworks for conditions in Indonesia. According to the experts, the framework can be

applied in Indonesia and the procedures have also been used in real cases undertaken by digital forensors. However, the participants also mentioned the importance of Indonesia having its own framework that is in accordance with the unique social, cultural, legal and regulatory environment in Indonesia.

4.2 Analysis of elements and sub-elements of various digital forensic frameworks

Field findings from interviews with participants stated that the earliest elements of the digital forensics' framework are identification and planning. In identification, it can be traced about the category of cybercrime committed, whether it is about system misuse or certain security violations. Meanwhile in planning, preparation can be made for the necessary resources, the need for time used. After identification and planning, the next step is evidence collection. The process of collecting this evidence usually includes identifying security and recording relevant digital evidence.

Various digital forensic frameworks adopt varied approaches in defining the elements and sub-elements that support the digital forensic investigation process [27]. Different digital forensic frameworks exhibit diverse methodologies for deciphering elements and sub-elements, which impacts the effectiveness and integrity of the digital forensic investigation process [28]. Based on interviews with three expert sources, core elements such as identification, preservation, inspection, analysis, and documentation were the main components found in most frameworks. The framework for digital forensics must have well-documented stages to maintain the credibility of the investigation results [29]. The process of proper preservation and validation of each sub-element greatly affects the success of the investigation and the receipt of evidence in court [16]. The first expert participant explained the importance of validation at each stage of the investigation to ensure that data integrity is maintained. The second expert participant highlighted the monitoring role of certified forensic experts in conducting applied technical performance assessments. The participants explained the importance of statistical assessment to each step to improve the quality of the analysis results. Validation acts as a safeguard, confirming that the evidence remains unaltered and reliable from its collection to its final analysis, which is crucial for maintaining trust in the forensic process

4.3 Evaluation of various digital forensic frameworks

The evaluation stage is a crucial step in the development of Sufree's forensic digital framework. A comprehensive evaluation will identify the shortcomings, strengths, and effectiveness of this framework. Thus, continuous improvements and improvements can be made.

Regarding the evaluation of the digital forensic framework, the participants in this research mentioned the need for a framework which did not only explain the handling of digital evidence but also needs to cover the entire handling of digital forensics, starting from human resources to evidence and the applications used, then how to present and how to preserve it. In the view of the participants, a framework was needed adapting the uniqueness and conditions existing in Indonesia.

Expert participants evaluated one of the frameworks frequently used in Indonesia, namely ISO/IEC 27037. In this framework there is still a lack of preparation. ISO/IEC 27037 only refers to the earliest elements of identification, but there is no preparation [30,31]. Whereas in this preparation there are important elements related to the forensor subject (the first handling assistant for digital evidence, digital evidence founder, digital evidence specialist and others) which must be ensured to have adequate competence as evidenced by the certification of expertise. Participants made recommendations if a digital forensic framework did require planning, but that was not the most important thing. The new digital forensics framework must be able to have mechanisms to maintain the integrity of the evidence and the integrity of the process.

As in table 4, the participants saw the importance of training and developing human resources who really master or are ready to face threats or cyber-attacks. In addition to competence, the number

of digital forensors is still not optimal in numbers, including the distribution of resources which was still minor in Indonesia in which there were still very few numbers of certified digital forensor. The number of digital forensic experts in Indonesia continued to grow but remains limited compared to the increasing demand for cybercrime investigations [32,33]. Another evaluation material was about the lack of infrastructure to conduct research and innovation [34]. According to the participants, the lack of infrastructure hindered the development of the digital forensics' world.

Table 4. Evaluation results of digital forensic framework

Evaluation Aspect	**Disadvantages**	**Recommendation**
Framework Completeness	Less focus on presentation and preservation of evidence.	The framework needs to cover the entire handling of digital forensics, from human resources, evidence, applications, presentation, to preservation.
Suitability with Conditions in Indonesia	ISO/IEC 27037 focuses less on forensor preparation and competency.	The framework needs to adapt the uniqueness and conditions in Indonesia
Technology Development	Digital forensic tools are less sophisticated.	More sophisticated digital forensic tools are needed.
Government Regulation	Regulations are not up to date and cannot predict the future.	There is a need for regulations that are up to date and can predict the future of digital forensics.
Forensor Quality	Training and development of human resources is less than optimal.	Optimal training and development of human resources as well as equitable distribution of forensor resources are needed.
Infrastructure	Lack of infrastructure for research and innovation.	Adequate infrastructures for research and innovation are needed.

Digital forensics in Indonesia faces rapid technological growth, followed by increasing digital security threats. In response, participants emphasized the need for policies which addressed forensic shortcomings and ensured investigations uphold ethical standard.

4.4 Developing a new framework in Indonesia

Regarding the development of a framework document in Indonesia, participants stated that it was important to ensure a comprehensive framework which covered several elements reflecting the specific needs and context in Indonesia. Based on the consensus of the participants in this study, there were four important aspects which had to be considered in building a framework to prevent ethical violations so that respect for ethics can be realized in digital forensic investigations, as can be seen in Figure 2.

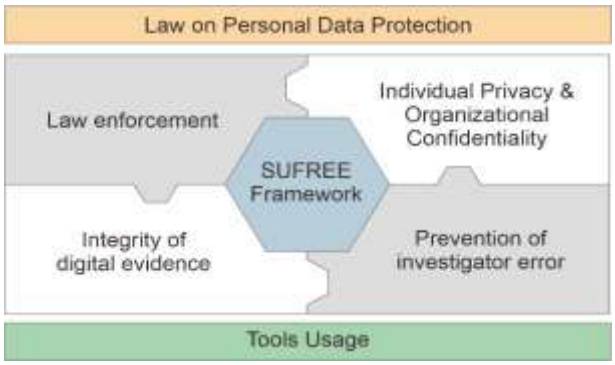

Figure 2. Aspects of the framework

Digital forensic procedures must comply with the requirements of legal authorities in the respective country's jurisdictions [35]. The lack of standard norms for the handling of digital evidence could hinder its acceptance in legal contexts, requiring collaboration between the legal and technology sectors [36]. Another thing that was also important to pay attention to in the preparation of this new framework document was the existence of a collaborative team consisting of the cyber community, academics, government, companies, law enforcement and other actors who can sit "together in one forum" to discuss new documents that are suitable for the Indonesian context.

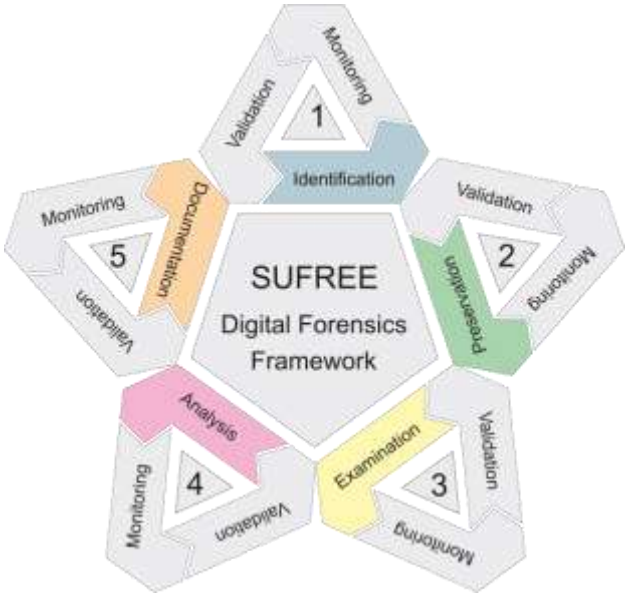

Figure 3. Supervisory framework to respect ethic (Sufree)

Figure 3 shows that Sufree (supervisory framework to respect ethic) consists of five major stages: identification, preservation, analysis, documentation and presentation. These five stages are inspired by the simple stages of The NIST procedure is proposed by NIST as the stage most often used by researchers. The NIST procedure is open to development that can be adapted to the circumstances of the organization [37]. The explanation for the steps especially validation and monitoring of each stage in the Sufree framework can be seen in Table 5.

Table 5. Validation and monitoring of each stage

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	Experts (supervisors) evaluate the use of inspection tools and techniques to ensure the accuracy of the analysis results.	Experts (supervisors) assess the efficiency and effectiveness of technical workers in the use of forensic tools and methodologies.

Analysis	Experts (supervisors) ensure that the results obtained are free from bias or errors.	Experts (supervisors) assess the correctness and consistency of the analysis results with the available data.
Documentation	Experts (supervisors) review documentation to ensure its completeness and conformity with standard procedures.	The expert (supervisor) assesses the completeness of the documentation.

Monitoring and validation are carried out by experts as a supervisory group consisting of practitioners who have been certified or have experience in the field of digital forensics is necessary to preserve the integrity of digital evidence and ethics that carried out by forensors. The context of certified experts was proposed because the participants realize that in Indonesia, a group of investigators need to work quickly while there are fewer certified practitioners and the ethics of digital forensics process were often left unsupervised. The validation and monitoring diagram of the Sufree framework were visualized as in Figure 4.

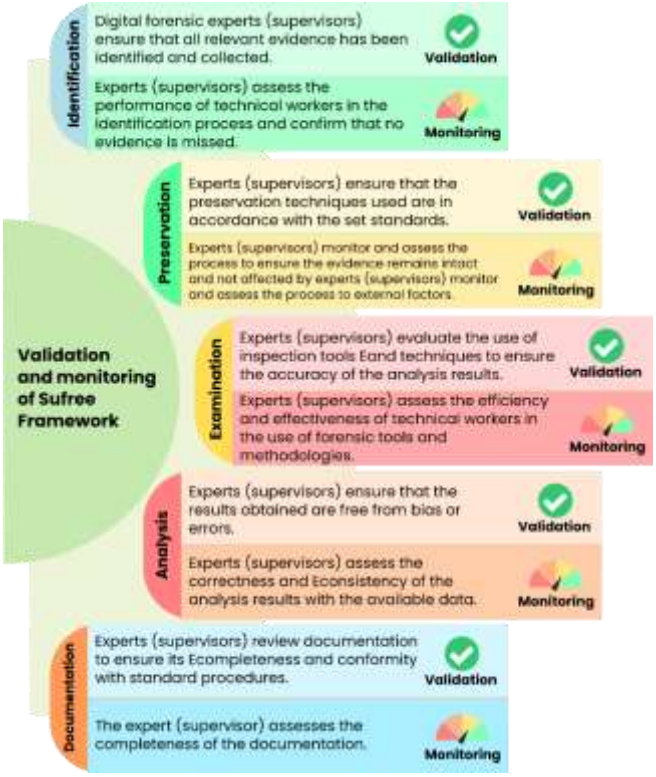

Figure 4. Validating and monitoring of Sufree Framework

SUFREE's digital forensics framework explains that the monitoring and validation process carried out by supervisors to technicians plays an important role in maintaining the integrity and quality of each stage of the investigation. At each step of Identification, Preservation, Inspection, Analysis, and Documentation, supervisors who are certified digital forensic experts are responsible for technical validation and monitoring of technician performance. The validation and monitoring process is illustrated in Figure 5.

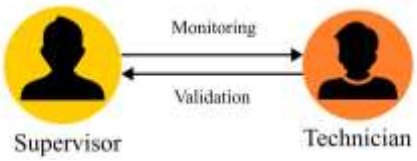

Figure 5. Validation and monitoring mechanism

The validation process involves checking the engineer's work to ensure that all actions taken are in accordance with the standard operating procedures (SOPs) and methodologies that have been set. Supervisors verify that digital evidence has been correctly identified, preservation techniques are applied appropriately, examination tools are used effectively, analysis is carried out without bias, and the entire process is fully documented.

Table 6. Monitoring Criteria at each stage

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 used at each stage are different. There are three criteria that have been agreed upon by the researchers at each stage as shown in Table 6. Monitoring in the Sufree framework uses the AHP method assessment process that can evaluate technicians according to criteria objectively. AHP is a commonly used decision-making tool for solving MCDM problems and is useful in a variety of real-time applications.

Figure 6. Hierarchy of AHP for monitoring assessment

In the development of the SUFREE (Supervisory Framework to Respect Ethics) framework for digital forensic investigations, monitoring the performance of technical workers is a key element that requires in-depth analysis. To carry out this monitoring, the Analytic Hierarchy Process (AHP) approach needs to be carried out with criteria arranged in a hierarchical hierarchy, as seen in figure 6. This AHP hierarchy helps determine the weight and priority of each stage in the digital forensic process based on the main goal of the framework, which is to ensure objective and comprehensive monitoring and validation of technical worker performance.

The weighting process with three criteria is carried out through the calculation of the comparison matrix with the formula Eq. (1):

$$A = \begin{bmatrix} 1 & a_{12} & a_{13} \\ 1/a_{12} & 1 & a_{23} \\ 1/a_{13} & 1/a_{23} & 1 \end{bmatrix} \qquad \text{Eq. (1)}$$

Explanation:

A = weight of criterion A

a_{12} = Weight of criterion 1 versus criterion 2

a_{13} = Weight of criterion 1 versus criterion 3

a_{23} = Weight of criterion 2 versus criterion 3

The AHP method can be used for performance appraisal in a variety of contexts, including project management, risk assessment, and strategic decision-making [38]. AHP helps break down complex problems into simpler elements, which are then systematically analyzed.

Table 7. Weighting criteria for each objective stage

Objective stage	**Index**	**Monitoring Criteria**	**Weight**
Identification (I)	CI.1	Accuracy	0.686
	CI.2	Completeness	0.292
	CI.3	Speed	0.117
Preservation (P)	CP.1	Data Integrity	0.686
	CP.2	Security	0.292
	CP.3	Speed	0.117
Examination (E)	CE.1	Accuracy of Tool Use	0.686
	CE.2	Efficiency	0.292
	CE.3	Completeness of Results	0.117
Analysis (A)	CA.1	Accuracy of Analysis	0.686
	CA.2	Reliability of Results	0.292
	CA.3	Objectivity	0.117

Documentation (D)	CD.1	Completeness	0.686
	CD.2	Consistency	0.292
	CD.3	Timeliness	0.117

The AHP assessment criteria for monitoring each stage vary. Table 7 is an explanation of the criteria and weighting of each objective stage. An overview of the monitoring assessment with AHP can be visualized in Figure 7. This AHP calculation method is a relevant option to measure the competence of technical officers in the field while still being supervised by a certified supervisor.

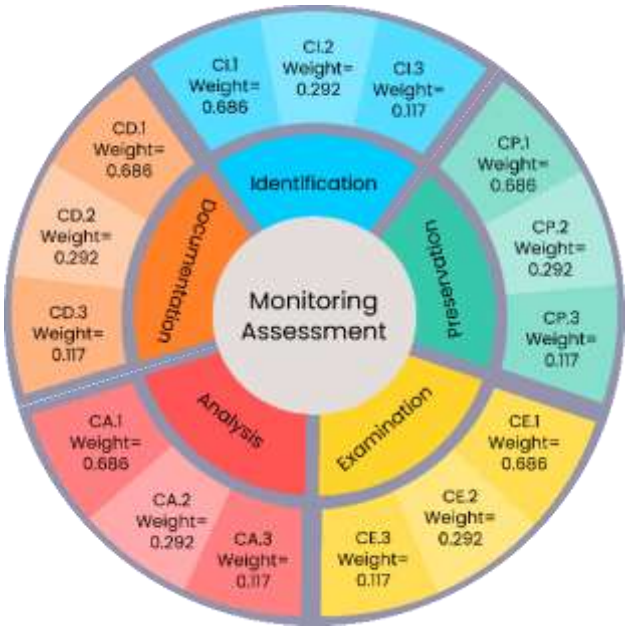

Figure 7. Monitoring assessment diagram

To test the validity of the calculation from the monitoring, the calculation of the paired matrix needs to be done with the formula Eq. (2). Validity calculations can only be done using datasets that have been tested with monitoring assessment, which are not simulated in this paper.

$$CR = CI / RI \qquad \text{Eq. (2)}$$

Explanation:
CR = consistency ratio
CI = consistency index
RI = random index

This calculation is a yardstick which can overcome the severity from simple administrative errors to the loss of important information during the examination process, and the loss of evidence [39]. These efforts are made so that when this framework is implemented, the evaluation of subjective handling can also be avoided.

5. Conclusion

This research discusses digital forensic frameworks, starting from identification, analysis of elements and sub-elements, to evaluation of existing frameworks. The findings of this research show several things: first, there are various digital forensic frameworks used globally. Each framework has advantages and disadvantages, as well as differences in intended use, programming language, and commercial/open-source category. Second, existing digital forensic frameworks can be applied in

Indonesia. However, there needs to be a framework specifically created for Indonesia to suit the country's unique social, cultural, legal, and regulatory environment. Third, important elements in the digital forensic framework include: identification, preservation, examination, analysis, and documentation. Fourth, the evaluation of existing digital forensic frameworks shows several shortcomings, such as: lack of focus on human resources, application, presentation, and preservation of evidence; lack of preparation and competence of forensors; and lack of sophisticated tools and up to date regulations. Fifth, there is a need to develop a new framework to prevent ethics violation. This new framework should be comprehensive, address the specific needs and context in Indonesia, and comply with applicable regulations/laws.

Based on the research findings above, it can be concluded that a comprehensive digital forensic framework that is suitable for the Indonesian context is very important to support an effective and efficient digital forensic investigation process. The development of a new framework is expected to improve the quality of investigation process and far from ethics violation.

References

[1] Ashley DuVal, "History of Forensic Psychology," https://forensicpsych.umwblogs.org. [Online]. Available: https://forensicpsych.umwblogs.org/research/criminal-justice/fingerprint-analysis/

[2] H. Arshad, A. Bin Jantan, and O. I. Abiodun, "Digital forensics: Review of issues in scientific validation of digital evidence," *Journal of Information Processing Systems*, vol. 14, no. 2, pp. 346–376, 2018, doi: 10.3745/JIPS.03.0095.

[3] A. Krivchenkov, B. Misnevs, and D. Pavlyuk, *Intelligent methods in digital forensics: State of the art*, vol. 68. Springer International Publishing, 2019. doi: 10.1007/978-3-030-12450-2_26.

[4] N. Hughes and U. Karabiyik, "Towards reliable digital forensics investigations through measurement science," *WIREs Forensic Science*, vol. 2, no. 4, pp. 1–11, 2020, doi: 10.1002/wfs2.1367.

[5] H. Henseler and S. van Loenhout, "Educating judges, prosecutors and lawyers in the use of digital forensic experts," *DFRWS 2018 EU - Proceedings of the 5th Annual DFRWS Europe*, vol. 24, pp. S76–S82, 2016, doi: 10.1016/j.diin.2018.01.010.

[6] H. Arshad, A. Jantan, and E. Omolara, "Evidence collection and forensics on social networks: Research challenges and directions," *Digit Investig*, vol. 28, pp. 126–138, 2019, doi: 10.1016/j.diin.2019.02.001.

[7] O. J. Ayangbekun, O. F. Bankole, and B. A. Saka, "Analysis of security mechanisms in Nigeria E-banking platform," *International Journal of Electrical and Computer Engineering*, vol. 4, no. 6, pp. 837–847, 2014, doi: 10.11591/ijece.v4i6.6857.

[8] K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," *Comput Secur*, vol. 105, 2021.

[9] F. Bankole, A. Taiwo, and I. Claims, "An extended digital forensic readiness and maturity model," *Forensic Science International: Digital Investigation*, vol. 40, 2022.

[10] K. C. Seigfried-Spellar, M. Rogers, and D. M. Crimmins, "Development of A Professional Code of Ethics in Digital Forensics," *Annual ADFSL Conference on Digital Forensics, Security and Law*, vol. 9, no. c, p. 15, 2017.

[11] C. Neale, I. Kennedy, B. Price, Y. Yu, and B. Nuseibeh, "The case for Zero Trust Digital Forensics," *Forensic Science International: Digital Investigation*, vol. 40, p. 301352, 2022, doi: 10.1016/j.fsidi.2022.301352.

[12] NIST, "Zero Trust Architecture," *Controlling Privacy and the Use of Data Assets*, pp. 127–134, 2022, doi: 10.1201/9781003189664-11.

[13] U. Kumar, N. Gaud, and C. Joshi, "A Framework for Digital Forensic Investigation using Authentication Technique to maintain Evidence Integrity," *International Journal of Computer Applications*, vol. 154, no. 6, pp. 1–3, 2016, doi: 10.5120/ijca2016912145.

[14] R. Montasari, P. Peltola, and D. Evans, "Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations," *Communications in Computer and Information Science*, vol. 534, pp. 83–95, 2015, doi: 10.1007/978-3-319-23276-8_8.

[15] G. Horsman, "Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics," *Comput Secur*, vol. 73, pp. 294–306, 2018, doi: 10.1016/j.cose.2017.11.009.

[16] F. T. M. Granja and G. D. R. Rafael, "Model for digital evidence preservation in criminal research institutions-PREDECI," *International Journal of Electronic Security and Digital Forensics*, vol. 9, no. 2, pp. 150–166, 2017, doi: 10.1504/IJESDF.2017.083989.

[17] R. I. Ferguson, K. Renaud, S. Wilford, and A. Irons, "PRECEPT: a framework for ethical digital forensics investigations," *Journal of Intellectual Capital*, vol. 21, no. 2, pp. 257–290, 2020, doi: 10.1108/JIC-05-2019-0097.

[18] G. Horsman, "Defining principles for preserving privacy in digital forensic examinations," *Forensic Science International: Digital Investigation*, vol. 40, Mar. 2022.

[19] D. J. Buckles and J. M. Chevalier, *Participatory action research: Theory and methods for engaged inquiry*, 2nd ed. Oxon: Routledge, 2019.

[20] D. Kember, *Action Learning and Action Research: Improving the Quality of Teaching and Learning*, vol. 9, no. 1. London: Kogan Page, 2000. doi: 10.1108/qae.2001.9.1.54.3.

[21] W. Gaskins, B. Guy, and B. Arthur, "Reflections on Implementing Participatory Action Research in Engineering," *Journal of Education and Development*, vol. 7, no. 3, p. 18, 2023, doi: 10.20849/jed.v7i3.1369.

[22] M. Eelderink, J. M. Vervoort, and F. van Laerhoven, "Using participatory action research to operationalize critical systems thinking in social-ecological systems," *Ecology and Society*, vol. 25, no. 1, 2020, doi: 10.5751/ES-11369-250116.

[23] A. F. Moussa, "Electronic evidence and its authenticity in forensic evidence," *Egyptian Journal of Forensic Sciences*, vol. 11, no. 1, 2021, doi: 10.1186/s41935-021-00234-6.

[24] R. A. Fahrezi Abdullah, "Digital Forensic Urgence in Analyzing Electronic Evidence for Evidence of Criminal Actions in Information and Electronic Transactions," *Journal of Development Research*, vol. 7, no. 2, p. Process, 2023, doi: 10.28926/jdr.v7i2.238.

[25] Y. Prayudi, A. Ashari, and T. K Priyambodo, "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia," *International Journal of Computer Network and Information Security*, vol. 7, no. 11, pp. 1–8, 2015, doi: 10.5815/ijcnis.2015.11.01.

[26] E. Casey, *Digital Evidance and Computer Crime. Forensic Science, Computers, and the Internet*. 2011.

[27] M. Ivanova and S. Stefanov, "Digital Forensics Investigation Models: Current State and Analysis," in *2023 8th International Conference on Smart and Sustainable Technologies (SpliTech)*, 2023, pp. 1–4. doi: 10.23919/SpliTech58164.2023.10193176.

[28] K. S. Singh, A. Irfan, and N. Dayal, "Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, 2019, pp. 584–590. doi: 10.1109/ISCON47742.2019.9036214.

[29] T. M. J. Abbas, "Studying the Documentation Process in Digital Forensic Investigation Frameworks/ Models," *Journal of Al-Nahrain University-Science*, vol. 18, no. 4, pp. 153–162, 2015, doi: 10.22401/jnus.18.4.21.

[30] A. FFaizal and A. Luthfi, "Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 701–718, 2024, doi: 10.51519/journalisi.v6i2.717.

[31] D. Sudyana, "Analysis and Evaluation Digital Forensic Investigation Framework Using Iso 27037:2012," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 1–14, 2019, doi: 10.17781/p002464.

[32] A. Nyman, S. Rutberg, M. Lilja, and G. Isaksson, "The Process of Using Participatory Action Research when Trying out an ICT Solution in Home-Based Rehabilitation," *International Journal of Qualitative Methods*, vol. 21, pp. 1–8, 2022, doi: 10.1177/16094069221084791.
[33] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)," *Jurnal Telekomunikasi dan Komputer*, vol. 9, no. 3, p. 186, 2020, doi: 10.22441/incomtech.v9i3.7210.
[34] E. Ramadhani, D. Hariyadi, and F. E. Nastiti, "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, pp. 1–6. doi: 10.1109/ICITDA55840.2022.9971449.
[35] J. Jordaan, "Ensuring the Legality of the Digital Forensics Process in South Africa," *International Journal of Computer Applications*, vol. 68, no. 23, pp. 36–39, 2013, doi: 10.5120/11722-7432.
[36] N. A. Rakha, *Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations*, vol. 16, no. 2. 2024. doi: 10.22201/iij.24485306e.2024.2.18892.
[37] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," The National Institute of Standards and Technology. Accessed: May 25, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
[38] B. F. Cortinas, J. Contreras-Salinas, F. López-Irarragorri, and E. De La Hoz Granadillo, "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.
[39] G. Horsman and A. Dodd, "Competence in digital forensics," *Forensic Science International: Digital Investigation*, vol. 48, no. November 2023, p. 301693, 2024.