Framework for Digital Forensic Ethical Violations: A Systematic Literature Review

Arizona Firdonsyah1*, Purwanto Purwanto2, and Imam Riadi3

1Doctorate Program of Information System, School of Postgraduate Studies, Universitas Diponegoro, Semarang, Indonesia
2Doctorate Program of Information System, School of Postgraduate Studies, Universitas Diponegoro, Semarang, Indonesia
3Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Abstract. Handling digital forensic cases plays a critical role in maintaining public interest and trust. However, the lack of an ethical code in digital forensics work processes can compromise the integrity and reliability of inspection results. This study aims to address this issue by conducting a systematic literature review (SLR) to explore existing standards for digital forensic frameworks. This study uses SLR techniques to identify and map various digital forensic investigation processes described in the literature. While there are some topics that address digital forensic frameworks in this review, we find it to be overwhelmingly focused on testing or evaluating digital forensic investigations. Unfortunately, the reviewed frameworks often neglected the code of ethics validation process, leaving the potential for ethical violations in the field of digital forensics. Integrating ethical considerations into existing frameworks is essential to ensure the credibility and reliability of digital forensic investigations. This study highlights the need to establish comprehensive policies and standards that include not only technical aspects but also ethical practices. In this way, digital forensics professionals can effectively maintain professional ethics, mitigate ethical violations, and restore public confidence in their findings. Future research should focus on the development and implementation of robust ethical frameworks in the field of digital forensics.

1 Introduction

Digital forensics is a relatively new scientific field. This scientific field was born in the 1980s in the wake of crimes related to the unauthorized modification of computer equipment in the United States. The practice of forensic science in general has a long history of being considered valid and reliable in criminal cases. For example, the study of fingerprints began in 1686 and was used for identification in 1882 and then used in uncovering criminal cases in 1892 [1]. Research of digital forensic science conducted by several researchers confirm that digital forensics is still far from perfection, both in terms of procedures and efforts to
validate digital evidence [2]. Based on the studies that have been carried out, several topics in the field of digital forensics still require improvisation in the forensic process to analyze digital evidence [3]. Research facts that have been studied by researchers in various countries narrow down to recommendations for improving the digital forensic process.

Digital forensic practitioners and academics show special concern for scientific validation in digital forensics, while the crisis in this field has been recognized by the world's standardization organizations [4-5]. In response, some scientists are demanding accreditation of experts and discussing the absence of regulations for testing reliability and the danger of bias caused by practitioners [6].

Increasingly developing technology, on the other hand, raises the potential for digital crime. Social networking platforms and financial technology are ideal places for criminals to carry out their actions. Crimes that occur on social media platforms also have the potential to lead to the fintech domain. Social engineering on social networks and fintech carried out by criminals is one of the modus operandi that researchers are concerned about [7]. This problem will be exacerbated if the handling of digital forensic investigations is not carried out properly. Studies that have been carried out by several researchers state that the poor results of disclosing digital evidence in social networking cases are caused by negligence in storing significant forensic artifacts in the process of forensic collection and analysis [8]. This can happen due to inappropriate storage formats and lack of data management.

The readiness and maturity of digital forensics in organizations are related to risk mitigation measures for information technology infrastructure. Studies on organizational security state that the level of forensic readiness influences the risk of exploitation crimes [9]. 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 [10]. The digital forensic maturity level testing framework is considered appropriate as a tool for measuring the readiness of forensic capabilities in an organization [11].

Discussion on the importance of ethics in digital forensics in America began in 2016 at the American Academic of Forensic Science (AAFS) conference where academics, practitioners, and vendors from the digital forensics field discussed the need for a professional code of ethics in digital forensics [12]. The discussion resulted in an agreement that there is a need for a uniform professional code of ethics in the field of digital forensics. Seigfried-Spellar, Rogers, and Crimmins recommend that the development of the code of ethics must be based on seven values: consistency, respect of individuals, autonomy, integrity, justice, utility, and competence.

Digital forensics has a major impact on the public interest. Based on research related to digital forensics, monitoring of digital forensic investigation’s results are very important because it will affect public trust. Trust in the digital forensic investigation process is under the spotlight of many parties, including academics and researchers. Neale in an article written from the results of the research captures the issue of trust in the reliability of case disclosures using digital forensics [13]. There is an inverse relationship to the trustworthiness of the digital forensic process that Neale revealed, that is, the more we trust the process, the less trust the reliability of the results will have.

This means that all parties involved in law enforcement in cases related to digital devices must increase their level of skepticism in the digital forensic investigation process. NIST also issues publications on how aspects of trust affects security in a company [14]. They publish the Zero Trust (ZT) architecture to be implemented in companies to change the traditional security paradigm. Based on the above phenomenon, the paradigm of reliability and security in the context of cyber security is heavily influenced by aspects of trust. The condition that has been criticized by researchers regarding trust is inseparable from the many results of digital forensic investigations that are in doubt. This can occur due to many factors, ranging from investigative procedures that are not carried out properly to fraud on
the part of those who intervene. Erroneous execution of procedures and fraud on the results of digital forensic work can result in poor execution of a decision. Based on the background above, there are a number of problems where technology that is currently growing has led to an increase in the potential for digital crime. With the increasing potential for digital crime, it is necessary to monitor violations in the digital world, one of which is through digital forensic analysis. However, there are various problems encountered in digital forensics, such as:

- Procedures and validation of digital evidence that are still weak
- A lack of scientific validation in the world of digital forensics, accreditation of experts and discussing the absence of regulations for testing reliability and the danger of bias caused by practitioners
- Excessive improvisation due to the lack of standardization
- Poor results of disclosing digital evidence in social networking cases were caused by negligence in storing significant forensic artifacts in the digital forensic collection and analysis process
- There is still a weak level of skepticism in the digital forensic investigation process
- There are many results of digital forensic investigations that are in doubt due to many factors, such as investigative procedures that are not carried out properly to fraud on the part of those who intervene, incorrect execution of procedures and fraud on the results of digital forensic work which can result in poor execution of a decision.

2 Method

The presentation of this manuscript was carried out using the Systematic Literature Review (SLR) method, which is a systematic literature review aimed at identifying, evaluating, and interpreting the findings of primary studies. Referring to Kitchenham's guidelines regarding systematic literature reviews conducted in the field of software engineering [15], the review process is divided into three stages, namely planning, conducting, and reporting just like shown on Figure 1.

![Fig 1. SLR Research Method](https://doi.org/10.1051/e3sconf/202344801003)

The planning stage is a process of defining the research scope and data sources used to collect literature. In this research, literature sources has been taken from ScienceDirect, Google Scholar, and ProQuest.

At the conducting stage, bibliometric analysis was conducted using Vosviewer with grouping of keywords and visualization of research topics from data sources. The results of processing this analysis then obtained several article titles that discussed frameworks and ethical violations in the field of digital forensics. The collected literature is then reviewed based on the abstract and content.
3 Research Discussion

Bibliometric techniques were carried out to identify the topic and area of this research. Based on a bibliometric study on the topic of frameworks in digital forensics, there can be found many connections between digital forensics and the latest technologies keywords. Several technologies that intersect with the keywords digital forensics include the internet of things, cloud computing, security, big data, and others. Research topics in the digital forensic area can be seen in Table 1.

<table>
<thead>
<tr>
<th>Keywords</th>
<th>occurrences</th>
<th>total link strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>digital forensics</td>
<td>71</td>
<td>297</td>
</tr>
<tr>
<td>cloud computing</td>
<td>20</td>
<td>112</td>
</tr>
<tr>
<td>cloud forensics</td>
<td>17</td>
<td>69</td>
</tr>
<tr>
<td>internet of things</td>
<td>9</td>
<td>55</td>
</tr>
<tr>
<td>Security</td>
<td>10</td>
<td>46</td>
</tr>
<tr>
<td>digital evidence</td>
<td>9</td>
<td>39</td>
</tr>
<tr>
<td>Blockchain</td>
<td>9</td>
<td>36</td>
</tr>
<tr>
<td>big data</td>
<td>4</td>
<td>33</td>
</tr>
<tr>
<td>Forensics</td>
<td>9</td>
<td>33</td>
</tr>
<tr>
<td>IoT</td>
<td>6</td>
<td>32</td>
</tr>
<tr>
<td>Investigation</td>
<td>7</td>
<td>31</td>
</tr>
<tr>
<td>digital forensic readiness</td>
<td>8</td>
<td>30</td>
</tr>
<tr>
<td>Survey</td>
<td>3</td>
<td>30</td>
</tr>
<tr>
<td>deep learning</td>
<td>7</td>
<td>28</td>
</tr>
<tr>
<td>image forensics</td>
<td>8</td>
<td>28</td>
</tr>
<tr>
<td>camera model identification</td>
<td>7</td>
<td>27</td>
</tr>
<tr>
<td>non-repudiation</td>
<td>2</td>
<td>27</td>
</tr>
<tr>
<td>Privacy</td>
<td>5</td>
<td>27</td>
</tr>
<tr>
<td>nuisance parameters</td>
<td>6</td>
<td>25</td>
</tr>
<tr>
<td>hypothesis testing</td>
<td>6</td>
<td>24</td>
</tr>
</tbody>
</table>

The bibliometric map visualization that underlies this research can be seen in Figure 2. The goal is to identify the journals most strongly associated with one particular keyword through a bibliographic link [16]. This bibliometric map can be interpreted as a message that discussions about digital forensic processes that are applied throughout the world need to be continuously developed and discussed.
Digital forensic studies always intersect with cybersecurity. In digital forensics the concept of the information security triangle is also used as a benchmark for the digital forensic processes that are carried out. The information security triangle shown in Figure 3 shows that data integrity, confidentiality, and availability are priorities that must be maintained in the digital forensic process.

**Fig 2. Visualization of Bibliometric Map for Digital Forensics Frameworks Topics**

**Fig 3. Information Security Triad [17]**

Integrity is one of the core principles of information security which means accuracy and completeness of information. Security audit efforts to maintain the integrity of the digital forensic process are important to do [18]. So that the element of data integrity is one thing
that needs to be prioritized when developing a code of ethics in handling digital forensics [19].

Data breaches occur due to poor implementation and lack of full control over privacy from the private sector or the government. Data integrity, which is a security priority, is compromised in the digital forensics process. There needs to be a clear digital forensic code of ethics and an organization that oversees it [20].

3.1 Framework Identification

The discussion in the article written by Bankole, Taiwo, and Claims [11] focuses on measuring frameworks for digital forensic processes in general. They expanded on the DFR Commonalities Framework (DFRCF) and leveraged its structure to design a digital forensic maturity assessment model (DFMM) that can validate the work of forensic practitioners and academics with semi-structured interviews. This framework is used in the assessment of digital forensic handling. Assessment of the forensic framework can determine whether the framework is effective or not. The assessment framework developed can be used as a reference in making code of ethics council policies in the digital forensics field.

Measurement of this framework is inseparable from the value of integrity that must be possessed in the digital forensic process. Tian and Wang explained that the element of data integrity is one of the core of information security [18]. They formulated a system model and a security model for a valid audit on data integrity verification based on the forensic process audit concept. This is in line with research conducted by Balogun and Zuva that data integrity is a subject that needs to be identified when developing a code of ethics in digital forensics so that an assessment of the framework discussed at the outset becomes important [19].

There are several studies that try to present a new digital forensic framework related to codes of ethics and personal data protection. Ferguson, Renaud, Wilford, and Irons [21] developed a framework based on respect for privacy in the digital forensic investigation process. The framework, called PRECEpt: Privacy-respecting ethical framework, provides a basic balance between the requirements and expectations of digital forensic investigators on the one hand and the rights of individuals and organizations on the other. Graeme Horsman [22] in the following year proposed a set of ten Privacy-Preserving Data Processing Principles (PPDPP) for consideration in the data extraction and examination process that separates personal data from verifiable data. Two of the many examples of reference sources illustrate that establishing a new framework by understanding the confidentiality of personal data is not impossible. This is a small practice of a professional code of ethics that needs to be carried out by digital forensic investigators. Sungmi Park, Nikolay Akayev, Yunsik Jang, Jisoo Hwang, Donghyun Kim, Wooneun Yu, Hyunwoo Shin, Changhee Han, Jonghyun Kim [20] consider it necessary to have a clear digital forensics code of ethics and an organization to oversee it.

3.2 Review of Digital Forensics Frameworks

All frameworks reviewed in this research are evaluated based on their strengths and weaknesses, so that they can be compared and become a reference in the development of new frameworks. Comparison of the advantages and disadvantages of the framework can be seen in Table 2.
<table>
<thead>
<tr>
<th>Frameworks</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| ICFIPM     | • ICFIPM combines several internationally recognized forensic investigation methods and techniques in one model, thus providing comprehensive guidelines for conducting forensic investigations on computer devices.  
• ICFIPM emphasizes the involvement of forensic experts in the early stages of investigation, thereby minimizing potential damage or modifications to digital evidence.  
• ICFIPM includes a detailed and systematic analysis phase, thus enabling forensic experts to identify and obtain relevant digital evidence more effectively. | • ICFIPM may be too complex to be used by novice forensic experts or by users inexperienced in forensic investigations.  
• ICFIPM requires sufficient time and resources to conduct a thorough forensic investigation using the methods described in this model. |
| FRED       | • FRED is designed to be easy to use and can be operated by forensic experts who do not have an extensive technical background in IT.  
• FRED uses a structured and systematic process for collecting and analyzing digital evidence, thereby minimizing the risk of damage or modification to digital evidence.  
• FRED includes innovative technologies and can support different types of devices used in forensic investigations. | • FRED may be too limited in terms of technical capabilities compared to other digital forensics frameworks.  
• FRED may lack flexibility in accommodating different types of complex or difficult forensic investigations. |
| PREDECI    | • PREDECI adopts a systematic and structured approach in collecting, analyzing, and presenting digital evidence, thereby minimizing the potential for errors or loss of digital evidence.  
• PREDECI includes practical guidance that can assist forensic experts in determining forensic investigation strategies and steps appropriate to the situation at hand.  
• PREDECI includes a verification and validation process to ensure the authenticity and integrity of digital evidence. | • PREDECI may take longer to conduct a thorough forensic investigation compared to some other digital forensics frameworks.  
• PREDECI may lack flexibility in accommodating different types of complex or difficult forensic investigations. |
<p>| PRECEPT    | • PRECEPT adopts a systematic and structured approach in collecting, analyzing, and presenting digital evidence, thereby minimizing the | • PRECEPT may take longer to conduct a thorough forensic investigation compared to some other digital forensics frameworks. |</p>
<table>
<thead>
<tr>
<th>Frameworks</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRECEPT</td>
<td>• PRECEPT includes practical guidance that can assist forensic experts in determining forensic investigation strategies and steps appropriate to the situation at hand. • PRECEPT emphasizes the importance of ethics and privacy in conducting forensic investigations.</td>
<td>• PRECEPT may lack flexibility in accommodating many types of complex or difficult forensic investigations.</td>
</tr>
<tr>
<td>PPDPP</td>
<td>• PPDPP provides innovative solutions in integrating privacy principles in forensic investigations. • PPDPP can help forensic experts to retrieve and process data in a more secure and ethical way, so as not to harm the privacy of data owners. • PPDPP also provides practical guidance for forensic experts in applying privacy principles in forensic investigations.</td>
<td>• PPDPP may require greater time and effort to apply privacy principles in forensic investigations, which may compromise the efficiency and productivity of forensic experts. • PPDPP may require more in-depth technical knowledge in terms of privacy and data processing, which may be a challenge for forensic experts who do not have a strong technical background.</td>
</tr>
</tbody>
</table>

Through this research, we emphasize the importance of adopting a comprehensive ethical framework in the practice of digital forensics to ensure the credibility and reliability of our findings. While some of these frameworks have made great strides in developing digital forensic investigative techniques, significant gaps exist in validating professional ethics. Therefore, to restore public trust and avoid ethical violations in this area, there is a need to strengthen existing ethical frameworks and ensure that their use is properly integrated at all stages of digital forensic investigations. More effort is needed. Integrating technical and ethical aspects into a digital forensics framework is an important step forward in preserving the integrity and quality of future digital forensics work.

Most of the articles reviewed show that digital forensic handling techniques and models need to be scientifically tested in order to find the right formulations in real cases. If PRECEPT, PDPP, and PREDECI are truly valid digital forensics techniques, they must undergo these crucial assessment procedures to be regarded as dependable instruments for digital investigations. It is essential for researchers and practitioner to release their work and expose it to examination by the broader community to guarantee that the techniques are robust, reliable, and efficient. The majority of these techniques necessitate a significant amount of time during the procedure, and it is necessary to evaluate whether this will pose a hindrance or not. Additionally, the adaptability of the FRED, PREDECI, PRECEPT approaches may hinder their implementation, and a thorough examination is required to assess this.

4 Conclusion

The literature review of this research refers to digital forensic frameworks that have been written by academics and practitioners around the world in scientific references. Elements and sub-elements of the digital forensic framework are identified and evaluated to critique.
the content of the existing digital forensic framework. Validation of ethics in digital forensic processes has not been found in these studies.

Most of the articles reviewed show that digital forensic handling techniques and models need to be documented and scientifically tested in order to find the right formulations in real cases. These facts indicate that the research topic regarding framework formation is an interesting topic for researchers and academics. Several frameworks were born from cases that occurred in the area of origin of the researchers and the policies that apply there. Case studies, policies, the point of view of researchers determine the characteristics of the elements embedded in the digital forensic framework.

References