

Article

ETHICore: Ethical Compliance and Oversight Framework for Digital Forensic Readiness

Amr Adel , Ali Ahsan  and Claire Davison

School of Business and Information Systems, Torrens University Australia, 88 Wakefield St, Adelaide, SA 5000, Australia; al_ahsan1@yahoo.com (A.A.); claire.davison@torrens.edu.au (C.D.)

* Correspondence: amr.adel@torrens.edu.au

Abstract: How can organisations be forensically ready? As organisations are bound to be criticised in the digitally developing world, they must ensure that they are forensically ready. The readiness of digital forensics ensures compliance in an organisation's legal, regulatory, and operational structure. Several digital forensic investigative methods and duties are based on specific technological designs. The present study is the first to address the core principles of digital forensic studies, namely, reconnaissance, reliability, and relevance. It reassesses the investigative duties and establishes eight separate positions and their obligations in a digital forensics' investigation. A systematic literature review revealed a gap in the form of a missing comprehensive direction for establishing a digital forensic framework for ethical purposes. Digital forensic readiness refers to the ability of a business to collect and respond to digital evidence related to security incidents at low levels of cost and interruption to existing business operations. This study established a digital forensic framework through a systematic literature review to ensure that organisations are forensically ready to conduct an efficient forensic investigation and to cover ethical aspects. Furthermore, this study conducted a focus group evaluation through focus group discussions to provide insights into the framework. Lastly, a roadmap was provided for integrating the system seamlessly into zero-knowledge data collection technologies.

Keywords: digital forensics; forensic readiness; data ethics; digital forensic framework



Citation: Adel, A.; Ahsan, A.; Davison, C. ETHICore: Ethical Compliance and Oversight Framework for Digital Forensic Readiness. *Information* **2024**, *15*, 363. <https://doi.org/10.3390/info15060363>

Academic Editor: Jiguo Li

Received: 29 May 2024

Revised: 9 June 2024

Accepted: 19 June 2024

Published: 20 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

What is a digital forensics investigation and how does one work? This question has been asked numerous times, but [1] emphasised that no straightforward solution exists. He stated that digital forensics is a procedure, not a task, and that it is a collection of tasks and procedures in inquiry, rather than a singular method.

A variety of digital forensics research methods seem to exist. Before user information on a computer can be accepted as evidence, legal practitioners do not need to fully comprehend the techniques used to 'dissect' the hard disc. They simply need to understand if the information applies to the investigation and is irrefutable. As a result, they become engrossed in the specifics, oblivious to the core idea behind digital forensic investigative techniques. Some concentrate on the technological components of data collection, while others concentrate on the data management part of the inquiry [2].

Since many of these processes were created to address distinct technologies utilised in the examined device, new protocols must be devised whenever the target device's underpinning technology evolves.

The processes of [3] are some of the most commonly cited processes by researchers and technicians in the field. In digital forensics inquiries, they are the conventional methods.

Digital forensics investigations encompass a broad spectrum of activities designed to collect, analyse, and preserve digital evidence in a manner that maintains its integrity and admissibility in legal contexts [4]. The field has evolved significantly over the years,

driven by rapid technological advancements and the increasing complexity of digital environments. The core objective of digital forensics is to uncover and interpret electronic data in a way that reconstructs past events, making it crucial for resolving cybercrimes, internal investigations, and regulatory compliance issues [5]. However, despite progress, a standardized, universally accepted method for conducting digital forensics investigations remains elusive. This lack of a clear-cut approach underscores the need for frameworks that can adapt to diverse technological landscapes and investigative requirements [6].

One of the primary challenges in digital forensics is the dynamic nature of technology itself [7]. As new devices and platforms emerge, the methodologies for extracting and analysing data must also evolve. Traditional forensic methods, while effective for certain types of data, may not be applicable to newer technologies such as cloud computing, mobile devices, and IoT systems [8]. This continuous evolution necessitates a flexible and forward-looking approach to digital forensics. The processes are widely recognized and utilized; however, they often require adaptation and refinement to remain relevant. Moreover, the increasing volume of data and the sophistication of cyber threats demand more robust and comprehensive forensic techniques that can address both the technical and ethical dimensions of digital investigations [9].

In this study, the ETHICore framework presents a pioneering effort to bridge the gap between technical proficiency and ethical compliance in digital forensic readiness. By reassessing investigative duties and establishing clear roles and responsibilities, the framework aims to streamline forensic processes while adhering to ethical standards. The focus on ethical considerations is particularly pertinent, given the potential for privacy violations and misuse of digital evidence. Through a systematic literature review and focus group discussions, the ETHICore study provides a well-rounded and practical roadmap for organizations to achieve forensic readiness. The integration with zero-knowledge data collection technologies further enhances the framework's applicability, ensuring that forensic investigations can be conducted with minimal disruption to business operations and maximum protection of sensitive data. This comprehensive approach not only enhances the efficacy of digital forensics but also aligns it with contemporary ethical and legal standards.

Although the extended model in [10] has expanded digital forensics techniques to encompass a broader scope and region, one key issue is still to be resolved. That issue is the disconnect between the technological elements of digital forensics and the legal system [11]. Losavio and Adams discovered that a significant gap still exists between technical experts and legal professionals. Although an increasing number of technical experts and legal professionals recognise the importance of learning about digital evidence and digital forensics procedures, they also believe that the technical methods and expertise are tough to acquire and execute.

The authors of [12] mentioned that for an organisation to optimise its ability to gather reliable digital evidence while reducing costs, it must establish a digital forensic framework. The literature defines digital forensic readiness as the conditions of the business for encompassing the digital processes and forensic collection of evidence. For an organisation to be forensically ready, it must ensure readiness in operational as well as infrastructural aspects (Dominic Savio, 2016). An operational framework is focused on the individuals involved in digital forensics, whereas an infrastructural framework is focused on processes for ensuring that organisational data are properly stored.

The authors of [13] highlighted that elements must be organised, policed, and controlled to improve forensic frameworks in Industry 5.0. Such a framework must be remembered as a holistic practice along organisational dimensions and integrated into the organisation's forensic preparation. This study aimed to develop a comprehensive framework that can act as a detailed roadmap for forensic investigators to provide credible evidence through several steps. These steps include various technical and nontechnical layers that assist in identifying different sources of information. The aim of establishing these different layers is to gather intelligence and answer questions that will open the door to new perceptions. Figure 1 explains how the research was conducted, from the

definition of the problem to the establishment of the framework. The completed framework is presented in the report of the findings.

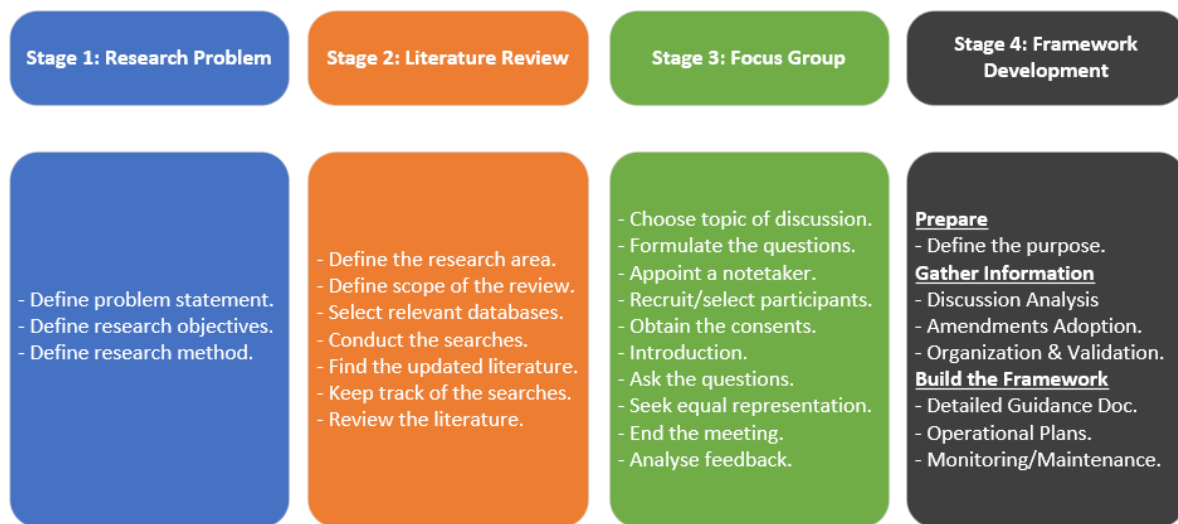


Figure 1. Research guidelines.

As the figure demonstrates, in Stage 1, the problem, research objective, and method for achieving that objective were clearly defined. In Stage 2, the research area and scope were defined, and the literature was reviewed using relevant databases, such as Google Scholar, Scopus, Science Direct, and Springer Link. In this stage, it was also crucial to define the areas for improvement and future research directions. Once all the relevant literature had been reviewed, Stage 3 involved evaluating the initial design of the framework and obtaining more details regarding what could be considered highly beneficial for such investigations in critical infrastructures. Furthermore, feedback was collected from experts and qualitatively analysed. Lastly, in Stage 4, the detailed Feasible Forensic Framework was established and adopted for operation.

The remainder of this paper is organised as follows. The Section 2 identifies the research methodology, providing credible insights into how the research was conducted. The Section 3 presents the current state of play through the existing literature, which supported the initial design of the research. The Sections 4 and 5 present the results and analysis of feedback from the focus groups with experts, who were selected to conduct a thematic evaluation of the initial research design and obtain their input. The Sections 6 and 7 present the discussion, which describes how the experts' feedback was used to build the Feasible Forensic Framework. The Section 8 provides the conclusion, and summarises the research contributions.

2. Research Methodology

The research methodology employed in this study was qualitative research based on two stages. Stage 1 was a literature review, which was based on a conceptual framework for describing the organisational forensic framework and the facts that contribute to it. This research approach brought together the research on the selected topic systematically. Evidence was obtained through the qualitative study and drawn from a previous study [14]. A preliminary literature review was conducted to define the concept of digital forensics and its relationships with the framework. The data were gathered from various sources, including Google Scholar, Scopus, Web of Science, and IEEE. Those libraries offered peer-reviewed journal articles related to the selected research topic, which helped the researcher to gather the required evidence for the research. A mixture of reliability and significance guarantees the validity of an investigation. The keywords considered were 'digital forensic', 'forensic readiness', 'digital evidence', and 'organisational and digital forensic'. A total of

70 articles published between 2016 and 2023 were considered. Figure 2 shows the selection criteria process for conducting the systematic literature review (SLR).

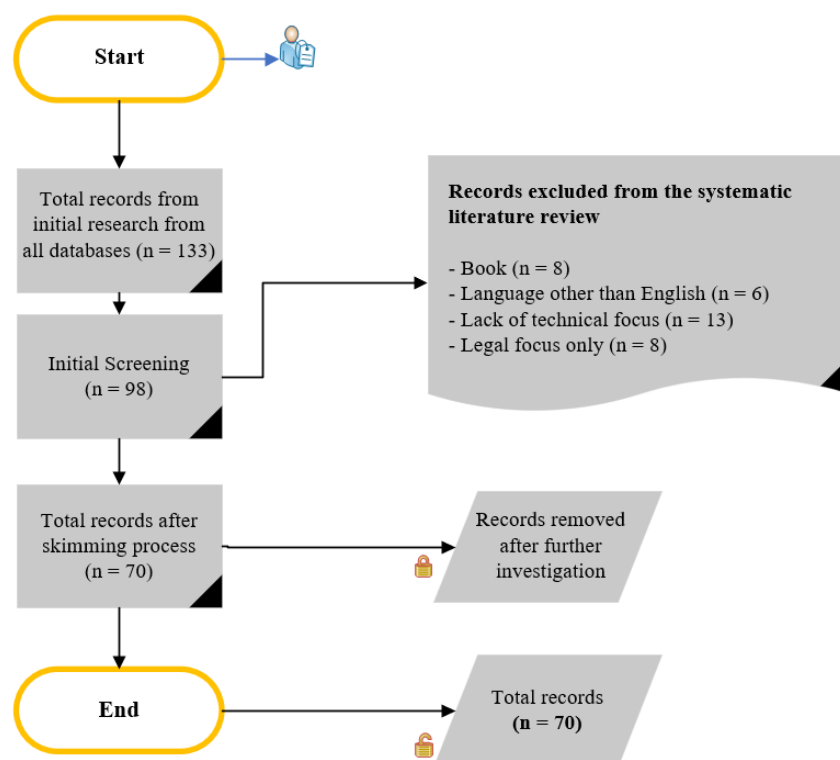


Figure 2. SLR selection criteria process.

A content analysis was conducted to determine whether the articles contributed to the field of digital forensics. This research tool is used to determine the presence of specific themes and keywords in obtained qualitative data [15]. Through this approach, the researcher quantified and analysed the meanings and relationships of the words and concepts. Through the systematic literature review, the preliminary study helped the researcher to understand the digital forensic framework for ensuring that organisations are forensically ready [16]. The outcomes of the research study are summarised as follows.

Stage 2 involved focus group discussions. This approach is employed to help researchers gather more information from various sources in a short period of time regarding complex topics where opinions are conditional. A recruitment process was established to select eligible experts for five focus group discussions, which were aimed at elaborating, testing, and obtaining feedback on how the framework should be developed further to meet organisational requirements and ensure that the forensic capabilities are fully supporting infrastructures. The process was designed so that experts could provide their input through a focused discussion, thereby identifying areas for improvement. To select experts for the focus group, we established a comprehensive scoring system that evaluates candidates based on their academic qualifications, professional experience, research contributions, and technical expertise [13,17]. Experts with a master's or PhD degree in digital forensics or related fields were awarded 4 and 6 points, respectively. Those with a minimum of 5 years of experience received 4 points, while those with over 10 years were given 6 points. Candidates with a proven track record of high-quality research published in peer-reviewed journals and professional certifications in forensics received 3 and 2 points, respectively. Additionally, technical experience in digital investigative tools and a strong industry portfolio with proven resolved cases were each awarded 3 points. To ensure high standards, each expert required a minimum score of 13 to be eligible to contribute to this study. This scoring system ensures a balanced and thorough evaluation, selecting experts with both

theoretical knowledge and practical, real-world experience in digital forensics. Table 1 demonstrates the criteria and their scores.

Table 1. Expert criteria scoring system.

Criteria	Score
Master's degree in digital forensics or related fields	04
PhD degree in digital forensics or related fields	06
Minimum of 5 years of experience	04
Minimum of 10 years of experience	06
Proven track record of high-quality research published in peer-reviewed journals	03
Professional certificates in forensics or related fields	02
Technical experience in digital investigative tools	03
Strong industry portfolio—proven resolved cases	03

3. Current State of Play: Review of Current Digital Forensics Models and Frameworks

The authors of [18] define digital forensic readiness (DFR) as a proactive measure designed to ensure organizations are prepared to effectively respond to digital incidents by having appropriate policies, procedures, and technologies in place. This readiness involves the capability to collect, preserve, and analyse digital evidence in a timely and cost-effective manner to support investigations and legal proceedings. They addressed a significant gap in the field of digital forensics, highlighting the importance of preparedness in handling digital incidents. The authors extend the digital forensic readiness commonalities framework (DFRCF) and propose a digital forensics maturity model (DFMM) that allows organizations to assess their forensic readiness and security incident responses. The methodology, which incorporates feedback from forensic practitioners and academics, enhances the practical relevance of the proposed models. However, the study's focus on participants with a forensic background may limit the generalizability of its findings. Additionally, while the top-down design approach is comprehensive, further empirical validation across diverse organizational contexts would strengthen the model's robustness and applicability.

The authors of [19] define a blockchain-based lawful evidence management scheme called LEChain for digital forensics, aiming to control the entire chain of evidence with transparency, unforgeability, and verifiability. LEChain employs short randomizable signatures to authenticate witness identities, fine-grained access control through ciphertext-policy attribute-based encryption (CP-ABE) for evidence management, and a secure voting method to protect juror privacy. The scheme leverages a consortium blockchain to store all evidence transactions, ensuring a transparent, immutable, and auditable supervision of the evidence. It introduces a novel approach to address significant privacy issues in digital forensics, including witness and juror privacy, which are often overlooked in existing frameworks. By proposing a stronger security model that considers the possibility of corrupt investigators, the authors provide a comprehensive solution for lawful evidence management. The practical implementation of LEChain, evaluated using an Ethereum test network, demonstrates its feasibility and efficiency in terms of the computational cost, communication overhead, and network latency.

The authors in [20] address the growing need for advanced digital forensics investigation frameworks (DFIFs) in the context of the Fourth Industrial Revolution, which has increased cybercrime rates due to the proliferation of interconnected digital devices. The authors surveyed recent trends in cybercrime and associated cyber forensics, emphasizing the importance of preserving evidence integrity throughout the investigative process for effective legal prosecution. They conduct a comparative analysis of various DFIFs by mapping processes and outputs from different phases of previously proposed frameworks, aiming to optimize the digital forensic investigation process. The paper offers valuable insights and structured approaches for enhancing forensic investigations, though it could benefit from empirical validation and quantitative analysis to support its findings.

The authors of [21] propose a proactive digital forensic readiness (DFR) framework to mitigate ransomware attacks on Windows operating systems. The framework leverages the Windows Registry and volatile memory to trace ransomware activity, aiming to collect digital footprints that could potentially decrypt affected systems. Evaluated against the ISO/IEC 27043 standard [21], the framework shows promise in harnessing system information before and during an attack. However, practical validation and consideration of its applicability in diverse scenarios are needed. Despite these challenges, the framework represents a significant advancement in ransomware defence through digital forensic readiness.

The authors of [22] propose an innovative framework called Internet-of-Forensics (IoF). This framework addresses the critical need for transparency and security in digital forensics within the Internet of Things (IoT) paradigm, characterized by its heterogeneity and cross-border legal challenges. IoF leverages consortium blockchain to ensure a secure chain of custody through a case chain mechanism, encompassing all stakeholders such as heterogeneous devices and cloud service providers. By employing blockchain-based evidence management, the framework enhances the transparency of forensic investigations and addresses cross-border legalization issues through a decentralized consensus model. Additionally, programmable lattice-based cryptographic primitives reduce complexities and benefit power-aware devices, enhancing the framework's novelty and efficiency. IoF is designed to be generic and versatile, suitable for use by security operation centres, cyber-forensic investigators, and for managing man-made crime evidence. The experimental results demonstrate IoF's efficiency in terms of complexity, time consumption, memory and CPU utilization, gas consumption, and energy analysis, proving its superiority over existing state-of-the-art frameworks.

The authors of [23] propose the D4I framework for reviewing and investigating cyber attacks, addressing the critical need for robust cyber attack investigation in the context of Industry 4.0 digitalization efforts. The D4I framework aims to enhance the examination and analysis phases of digital forensics, which are often insufficiently detailed, thus limiting their effectiveness. The framework categorizes digital artifacts and maps them to the Cyber Kill Chain steps of attacks, providing a structured approach to investigation. Additionally, it offers detailed instructional steps for the examination and analysis phases, improving the depth and thoroughness of cyber attack investigations. The paper demonstrates the framework's applicability with a case study on a spear phishing attack, showcasing its potential to support effective damage mitigation and the development of future prevention strategies. While the framework leverages intelligent tools and processes, it acknowledges that these tools are less effective against novel attack mechanisms, highlighting the importance of the comprehensive and structured approach provided by D4I.

The authors of [24] present a fog-based digital forensics investigation framework for IoT systems. The proliferation of IoT devices necessitates the development of efficient digital forensic techniques to address computer-related crimes involving these devices. Traditional forensic data acquisition methods focusing on computing hardware and operating systems may not be suitable for IoT devices due to their unique characteristics and constraints. The FoBI framework aims to tackle these challenges by leveraging fog computing to facilitate forensic investigations of IoT devices. The paper details the architecture, use cases, and implementation of FoBI, demonstrating how it can improve the digital forensics process for IoT systems. By addressing key challenges such as determining relevant data types for collection and effectively leveraging traces from IoT devices, FoBI offers a comprehensive approach to enhancing digital forensics in the context of IoT.

The authors of [25] propose the Framework for Reliable Experimental Design (FRED) in the paper "Framework for Reliable Experimental Design (FRED): A Research Framework to Ensure the Dependable Interpretation of Digital Data for Digital Forensics", aimed at enhancing the reliability and robustness of digital forensic research. Recognizing the critical need for factual accuracy in digital forensic analysis, especially with the impending requirement for ISO/IEC 17025 accreditation, FRED provides a structured approach

to planning, implementing, and analysing investigatory research [25]. The framework emphasizes procedures for reverse-engineering digital data structures and extracting and interpreting digital content, ensuring findings are dependable and accurate. Designed as a resource for both industry and academic professionals in digital forensics, FRED supports the development of best practices and contributes to the credibility and reliability of digital forensic investigations.

The authors of [26] present a framework for IoT forensics in their paper “IoT Forensic: A Digital Investigation Framework for IoT Systems”. The paper addresses the growing security issues, threats, and attacks associated with IoT devices, highlighting the necessity for a robust forensic methodology to investigate IoT-related crimes. The challenges posed by IoT for forensic investigators include the vast variety of information, the blurring lines between private and public networks, and the complexity added by the integration of numerous objects of forensic interest. The proposed framework aims to support digital investigations of IoT devices by systematically tackling these challenges. The authors emphasize various steps crucial for conducting digital forensics in the context of IoT, aiming to provide a structured approach to address the unique difficulties presented by the IoT ecosystem. This framework is essential for developing effective forensic methodologies to keep pace with the evolving landscape of IoT-related security threats.

The authors of [27] introduce the Digital Evidence Reporting and Decision Support (DERDS) framework. This framework addresses the critical need for reliable investigative decision-making in digital forensics, recognizing that this competency is often assumed rather than formally taught. Given the complexity of digital investigations, the lack of formalized decision-making models poses a significant issue, leading to scrutiny regarding the quality and validity of evidence produced by digital forensics practitioners. The DERDS framework is designed to assist practitioners in evaluating the reliability of their inferences, assumptions, and conclusions related to evidential findings. By outlining the stages of decision-making, the framework helps practitioners assess the accuracy of their findings and recognize when content may be deemed unsafe to report. This structured approach aims to enhance the credibility and reliability of digital forensic investigations.

4. Navigating Technical and Ethical Complexities in Digital Forensics

With the increasing complexity and frequency of digital crimes, the need for robust digital forensic investigation frameworks and readiness measures has become critical [28–30]. This discussion explores the technical and ethical issues and challenges faced in digital forensic investigations and readiness. Figure 3 illustrates the technical and ethical issues in digital forensics.

a. Technical Issues and Challenges

Data Volume and Complexity

One of the primary technical challenges in digital forensics is the sheer volume and complexity of data that need to be processed [31–36]. Modern digital environments generate vast amounts of data from various sources such as computers, mobile devices, cloud services, and Internet of Things (IoT) devices. Managing and analysing these data to extract relevant evidence requires significant computational resources and advanced analytical tools. The complexity is further compounded by the diverse formats and encryption methods used, which can hinder the accessibility and readability of potential evidence.

Rapid Technological Evolution

The rapid pace of technological advancement presents another significant challenge [37–39]. New technologies and devices are continuously being developed, each with unique characteristics and security features. Forensic tools and methodologies must constantly evolve to keep up with these changes, requiring ongoing research and development. Additionally, proprietary technologies and closed systems can limit the ability of forensic investigators to access and analyse data, as manufacturers may not provide the necessary support or tools.



Figure 3. Mindmap of technical and ethical issues in digital forensics.

Data Integrity and Chain of Custody

Ensuring the integrity of digital evidence is crucial for its admissibility in court. Any alteration or contamination of evidence can render it inadmissible. Maintaining a secure chain of custody—documenting every step of the evidence handling process from collection to presentation—is essential to demonstrate that the evidence has not been tampered with. This process can be technically challenging, especially when dealing with digital evidence that can be easily modified or corrupted [40–48].

Encryption and Anti-Forensic Techniques

The use of encryption and anti-forensic techniques by criminals poses a significant obstacle to digital forensic investigations. Encryption can make it extremely difficult to access the contents of digital devices and communications. Anti-forensic techniques, such as data obfuscation, steganography, and secure deletion methods, are designed to hinder forensic analysis by erasing or masking digital traces [49–54]. Overcoming these barriers requires sophisticated decryption tools and methods to detect and counteract anti-forensic measures.

Resource Constraints

Digital forensic investigations can be resource-intensive, requiring specialized hardware, software, and skilled personnel. Many organizations, particularly smaller ones, may lack the necessary resources to conduct thorough forensic investigations [55–59]. This can lead to delays in evidence processing and analysis, potentially compromising the investigation's outcomes. Additionally, the cost of acquiring and maintaining forensic tools and training personnel can be prohibitive.

b. Ethical Issues and Challenges

Privacy Concerns

Digital forensic investigations often involve accessing sensitive personal information, raising significant privacy concerns. Investigators must balance the need to gather evidence with the obligation to respect individuals' privacy rights [56,60–66]. Unauthorized access to personal data can lead to legal and ethical ramifications. Ensuring that investigations are conducted in compliance with privacy laws and regulations is essential to maintain public trust and avoid legal consequences.

Bias and Objectivity

Maintaining objectivity and avoiding bias is a critical ethical issue in digital forensics. Investigators must ensure that their findings are based solely on the evidence and not influenced by external factors such as personal beliefs, organizational pressures, or biases against specific individuals or groups [67–69]. Bias can lead to wrongful accusations and undermine the credibility of the investigation. Implementing standardized procedures and peer reviews can help mitigate the risk of bias.

Legal and Jurisdictional Challenges

Digital forensics often involves cross-border investigations, which can complicate legal and jurisdictional issues. Different countries have varying laws and regulations regarding data privacy, evidence collection, and admissibility. Coordinating investigations across jurisdictions requires careful navigation of these legal frameworks to ensure that evidence is collected and handled lawfully [70–76]. Failure to adhere to legal requirements can result in evidence being excluded from legal proceedings.

Ethical Use of Technology

The use of advanced technologies in digital forensics, such as artificial intelligence (AI) and machine learning, raises ethical concerns regarding their application and potential misuse [77–84]. While these technologies can enhance the efficiency and accuracy of forensic investigations, they also carry risks of algorithmic bias, errors, and misuse. Ethical guidelines and oversight are necessary to ensure that these technologies are used responsibly and transparently.

Accountability and Transparency

Accountability and transparency are essential in digital forensic investigations to maintain public trust and uphold ethical standards. Investigators must be accountable for their actions and decisions throughout the investigation process [75–77]. The transparent documentation of procedures, findings, and decision-making processes helps ensure that investigations are conducted ethically and that the results are credible and trustworthy. A lack of transparency can lead to questions about the integrity of the investigation and its outcomes.

Table 2 compares the ETHICore framework with various digital forensic readiness frameworks, highlighting key criteria such as proactive preparedness, evidence integrity, privacy and security, scalability and efficiency, advanced analytical tools, empirical validation, legal and ethical considerations, and comprehensive documentation. ETHICore stands out for its comprehensive approach, consistently addressing each criterion. It aligns with other frameworks like LEChain and FRED in ensuring evidence integrity, matches the privacy and security strengths of LEChain and Internet-of-Forensics, and demonstrates high scalability and efficiency, similar to LEChain and Advanced DFIFs. Additionally, ETHICore incorporates advanced analytical tools, provides empirical validation, addresses legal and ethical considerations, and offers comprehensive documentation, positioning it as a robust and thorough framework in comparison to other existing frameworks.

Table 2. Comparison between our proposed framework and the current forensic frameworks. Partially covered (✓), fully covered (✓★), or not covered (x).

Criterion	Digital Forensic Readiness [18]	LEChain [19]	Advanced DFIFs [20]	Ransomware DFR [21]	Internet-of-Forensics [22]	D4I Framework [23]	FoBI Framework [24]	FRED [25]	IoT Forensic Framework [26]	DERDS Framework [27]	Our Proposed Framework: ETHICore
Proactive Preparedness	✓★	x	✓	✓★	x	✓	✓	x	x	x	✓★
Evidence Integrity	✓★	✓★	✓★	✓	✓★	✓★	✓	✓★	✓★	✓	✓★
Privacy and Security	x	✓★	x	x	✓★	x	x	x	x	✓	✓★
Scalability and Efficiency	✓	✓	✓	✓	✓★	✓	✓	x	x	x	✓★
Advanced Analytical Tools	x	x	✓	✓	✓	✓	✓	✓★	x	x	✓★
Empirical Validation	✓	✓	x	x	✓	✓	x	✓★	x	x	✓★
Legal and Ethical Considerations	x	✓	x	x	✓	✓	x	x	✓	✓★	✓★
Comprehensive Documentation	✓	✓	✓	x	✓	✓	x	✓★	x	✓★	✓★

5. Focus Group Discussions and Feedback on Technical Aspects and Ethical Principles: Results and Analysis

a. Data Examination Layer

Experts emphasize the crucial importance of maintaining privacy and preventing data breaches during forensic activities to preserve the integrity and credibility of digital forensics. Privacy concerns are paramount as they directly impact the trust stakeholders place in digital forensic processes (PK). Regular audits and compliance checks are advocated to ensure the authenticity of data and to maintain a transparent chain of custody. Such measures help verify the integrity of forensic practices and prevent any potential misuse of data during the investigation (NA, RR). Ethically, it is paramount that qualified individuals with proven experience lead the examination process. This ensures that the forensic procedures are conducted with the utmost competence and oversight. Additionally, meticulous documentation of all actions and findings must be maintained to ensure accountability and transparency. This documentation serves as a foundational component that supports the validity of the forensic findings in legal contexts.

b. Data Acquisition Layer

The acquisition of forensic data must adhere to stringent legal standards, emphasizing respect for individual privacy and limiting data access solely to what is relevant to the case. This approach ensures that the rights of individuals are safeguarded while enabling effective forensic investigations (PK, JS). There is also a noted need for equitable access to advanced forensic tools to avoid disparities in justice handling across different regions or institutions. This access is essential for ensuring that all forensic investigations can be conducted with the same level of thoroughness and accuracy, regardless of the investigators' geographical location or institutional affiliation (MH). Ethically, secure and reliable data storage platforms are necessary to preserve data integrity during this process (E5). Moreover, the well-being of investigators must be prioritized to ensure high-quality and ethical outcomes (E13). This involves creating a supportive work environment that considers the physical and psychological health of forensic professionals.

c. Forensic Preparation Layer

Setting clear, standardized procedures and providing comprehensive training in both technical and ethical standards are key to protecting privacy and maintaining data integrity during forensic preparations. These preparations involve rigorous internal audits and consistent application of best practices to safeguard sensitive information (NA, BC). Transparency with all parties involved in data handling processes is critical for building trust and ensuring adherence to ethical standards. Such transparency helps alleviate concerns about data misuse and fosters a collaborative atmosphere among stakeholders (JS). Ethically, it is crucial to maintain the confidentiality of the information, limiting access only to those directly involved in the case. Furthermore, implementing secure data storage solutions is essential for maintaining the integrity and confidentiality of the data collected.

d. Identification Layer

The use of privacy-enhancing technologies (PETs) during the identification phase of forensic investigations helps minimize the exposure of non-relevant personal data. These technologies are crucial for ensuring that only pertinent data are analysed, thereby protecting the privacy of individuals not directly related to the case (RR). Continuous training for forensic professionals ensures they are equipped to handle evidence ethically and competently. This training should cover the latest advancements in forensic technologies and ethical standards, ensuring that professionals remain current in their practices (BC). Relevant ethical principles highlight the need to exclude data irrelevant to the investigation from reports to maintain focus and integrity. This exclusion helps prevent the dilution of forensic findings and reduces the risk of privacy violations.

e. Motivation Layer

Ensuring equitable access to digital forensic tools is a significant ethical issue that needs addressing to prevent inequalities in justice. This access ensures that all forensic investigations, regardless of location, have the necessary tools to conduct thorough and accurate investigations (MH). Oversight and continuous review of forensic practices are necessary to adapt to rapid technological advancements and maintain ethical standards. This ongoing oversight ensures that forensic methods remain relevant and effective in the face of evolving digital landscapes (MG). Regular professional training for forensic investigators is crucial to ensure the quality and accuracy of forensic processes. This training helps maintain a high standard of professional practice and ethical conduct among forensic investigators.

f. Legal Advisory Layer

Clear legal frameworks should define permissible actions and safeguards during forensic investigations to protect individual rights and maintain ethical integrity. These frameworks are essential for guiding forensic professionals in their daily responsibilities and ensuring that their actions remain within legal bounds (BC, PK). Transparency about legal procedures and maintaining strict adherence to legal standards is essential to uphold the credibility of forensic investigations. This transparency helps stakeholders understand the legal basis for forensic activities and fosters trust in the outcomes of these investigations (NA). Investigations must be transparent and maintain high levels of confidentiality, integrity, and availability, ensuring lawful conduct and availability of valid evidence upon request. These principles are foundational to maintaining the legal admissibility of forensic evidence and the ethical integrity of the investigation process.

g. Security Layer

Implementing supervisory controls and security mechanisms to protect system information and prevent unauthorized access or data breaches is vital. These controls are crucial for safeguarding the integrity of forensic data and ensuring that it remains untampered throughout the investigative process (RR, BC). Maintaining comprehensive system logs with timestamps can help trace activities and safeguard against tampering or unauthorized access. These logs provide a verifiable record of all actions taken during the forensic process, adding an additional layer of security and accountability (MG). Ensuring data confidentiality and secure storage is essential to prevent leaks and unauthorized access, maintaining the integrity of the forensic process. These security measures are integral to protecting sensitive information from external threats and ensuring that forensic investigations can be conducted in a secure and controlled environment.

6. Report of Findings

After collecting and evaluating the perpetrator's data as well as the IP address data obtained from the network operators, the legal prosecution must consult with the investigation manager and the owners of the system on the goals of legal presentations (Why). The criminal counsel will be able to assess whether the matter may be brought to trial or dismissed based on the retrieved necessary details and analytical report, as well as when adequate proof has been gathered. Regarding the characteristics of legal appearance (What), the legal counsel should think about what they want to offer in court as well as whether the data are significant and acceptable. They should also inform the researchers if any extra proof is required. In litigation processes, organisations (Who) will have to be defined. The testimony listing order and the interim injunction question list must be defined by the legal prosecuting attorney for illegal charges. In terms of a schedule of the complete event for presentation (When), legal investigators should also create a whole storyboard for the court, dependent on the proof supplied, and evaluate if any pieces of timing information are lacking.

a. Ethical Principle Implementation of the ETHICore

The focus groups identified, throughout the interview, 13 ethical principles, as shown in Table 3. The interviews revealed important ethical considerations to be included in order to ensure that the digital forensic investigation is being conducted lawfully and ethically. The ethical principles identified have paved the way for the technical steps to be followed ethically and according to the international standards without compromising the quality or accuracy of the investigation. The stages are referred to as “S1, S2” and the ethical principles are referred to as “E1, E2”.

Table 3. Ethical principles in digital forensic investigations.

Ethical Principle	Ethical Principle	Description
E1	Define concern	Begin with meticulously outlining the concern of the case investigation.
E2	Confidentiality preservation	The confidentiality of information must be ensured only by investigation parties classified as being of interest to the case.
E3	Investigation scope	If it is proven that other parties have been involved, the investigation will be extended to include them. Investigation procedures of third parties must be conducted only by investigative units classified as being of interest to the case.
E4	Data relevancy	Any private information obtained through the investigation that is considered irrelevant to the investigation must be excluded in reports.
E5	Data storage	A reliable and secured data storage platform must be established to preserve the obtained data for the examination process.
E6	Examination process	Qualified people with proven experiences must lead the investigation and oversee the entire process.
E7	Documentation of investigation's procedures	All actions must be recorded and the analysed and judged confidential and relevant information to the investigation must be documented in detail.
E8	Auditing process	Outline the auditing strategy and plans to inspect, observe, and confirm the correctness of the findings of all forensic teams.
E9	Report writing	After concluding the report and identifying all the findings, the report must be structured to include all details of the investigation including what evidence was examined, how data were classified, and who was involved in the investigation.
E10	Transparency of the investigation	In case the investigation has been extended to a further range, the reason and clarifications must be submitted to justify why the investigation was extended.
E11	Professional training	Regular training must be provided to the forensic investigators to ensure the accuracy and quality of work presented.
E12	Confidentiality, integrity, and availability of the investigation	The work must be performed lawfully with a high level of confidentiality and integrity to make sure the evidence is valid and available upon request.
E13	Investigators' well-being	The well-being of the investigators must be taken as a highest priority so they can continue the work professionally with accurate results.

Thirteen ethical principles have been extracted from the interviews to help in shaping the Feasible Forensic Framework from an ethical perspective and ensure that it matches the technical roadmap to follow lawful and ethical procedures. Figure 4 explains how the ethical principles can be applied to the Feasible Forensic Framework with a reference to each layer of each stage.

b. A Thematic Roadmap of the Feasible Forensic Framework

The focus group interviews and discussions with experts revealed seven layers that play a key role in digital forensic investigations. According to the experts, including these themes and layers in the framework will empower the capability of forensic investigators to conduct effective investigations and obtain credible evidence. These themes were identification, motivation, legal advice, security, forensic preparation, data acquisition, and data examination. These are the priority areas for identifying the nature of the event, setting an investigation plan, and designing and creating a suitable procedure for acquiring evidence,

establishing a map, and identifying the tools and techniques required for analysing the evidence. Each one of these themes represents a distinctive dimension, which has been listed under each layer in Figure 5. The figure presents a roadmap of the Feasible Forensic Investigation in detail, explaining the different route of each layer and sublayers from a technical perspective. The next section identifies clearly the ethical guidelines and considerations to build the Feasible Forensic Framework to resolve ethical issues of digital forensic investigations.

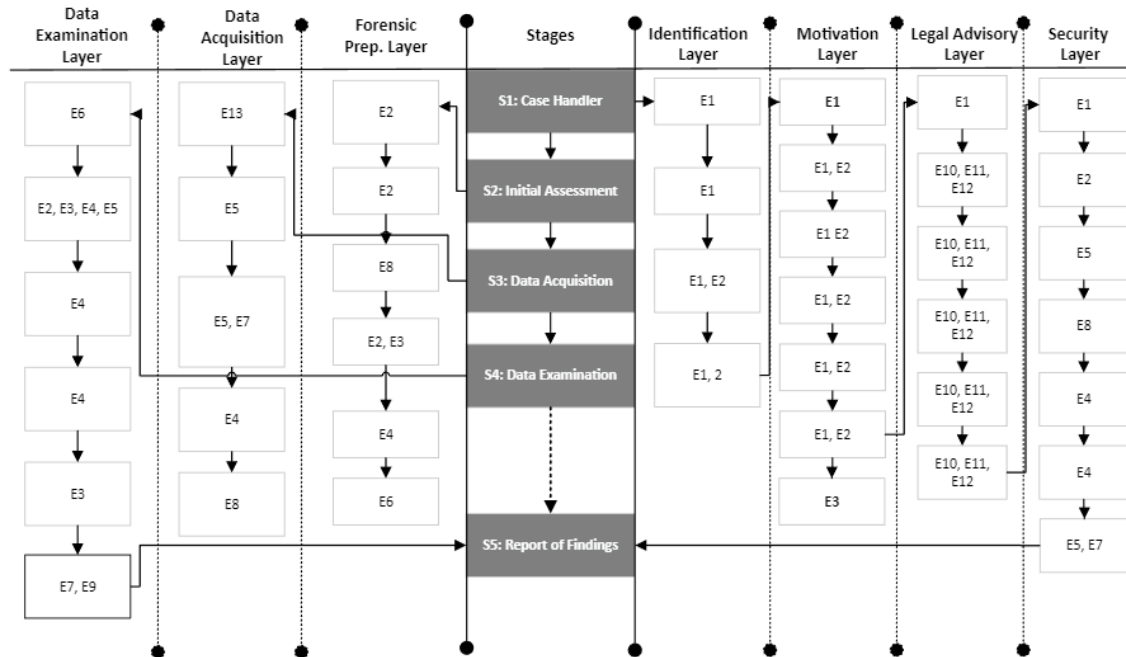


Figure 4. ETHICore: Ethical Compliance and Oversight Framework.

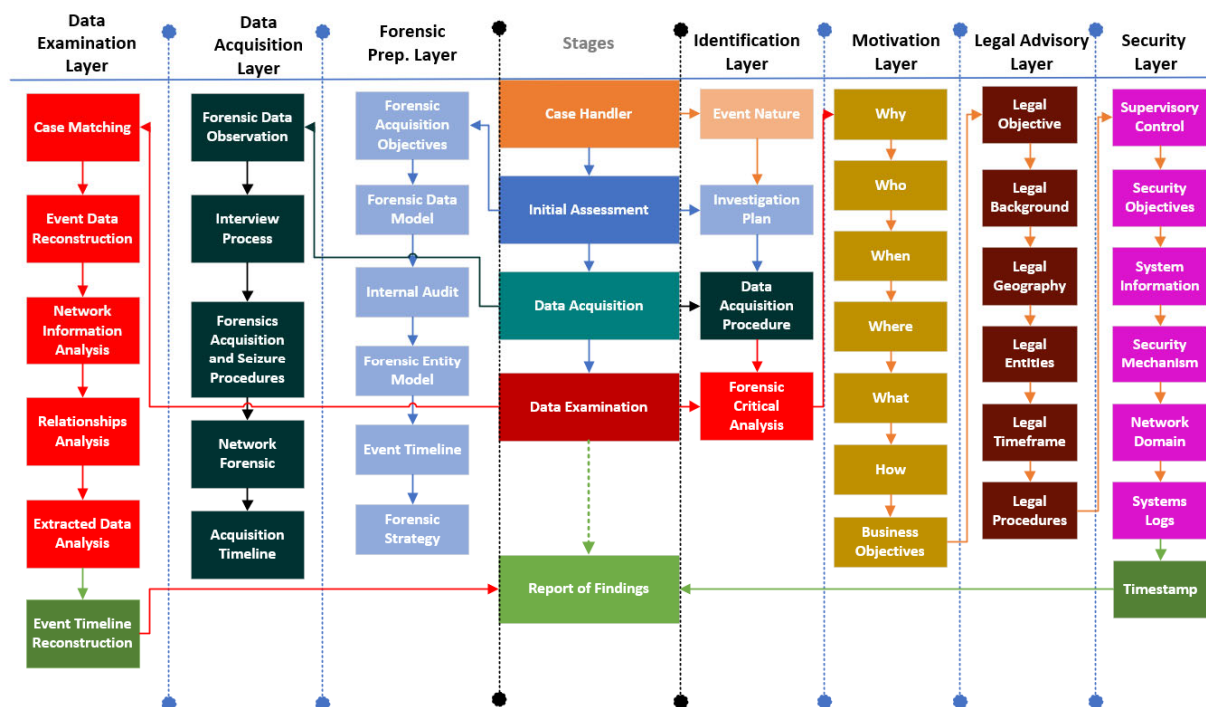


Figure 5. ETHICore: Ethical Compliance and Oversight Framework (thematic roadmap).

7. Discussion

There are many ethical challenges in and technical components of IT protection, including access control, biometrics, encryption, network security, and security algorithms. They each have their own approach and line of thinking, yet they all adhere to the same set of basic ideas. These are the basics of IT security—confidentiality, integrity, and availability. Various facets of IT protection are tied jointly by this key notion. The fundamental IT security concept is used in the design, evaluation, and auditing of IT protection throughout various enterprises.

In the same manner, digital forensics research must have a basic value that allows professionals to see the fundamental notion throughout various digital forensics research processes. The act of determining and relating retrieved data and digitised proof to create facts for legal challenges is known as a digital forensic investigation. The key principles of reconnaissance, reliability, and relevance are employed to meet this need, which are defined as follows:

1. **Reconnaissance**—A digital forensics researcher must, comparable to what must be completed before ethical hacking, deplete all methodologies, practices, and tools established for a specific operating condition to obtain, recoup, decipher, explore, retrieve, analyse, and transform data stored on various storage devices into legible proof. Digital forensics researchers ought to uncover and be focused on retrieving the reality underlying the data regardless of how and where they are kept.
2. **Reliability**—Data extraction is not the same as replicating data with Windows Explorer or storing information on a disc. During the extraction, analysis, storage, and transportation of data, the line of proof must be maintained. In summary, the non-repudiation element of digital forensics can be defined as the collection of evidence, chronology, and information quality, as well as the user's connection with the proof. The digital evidence should be credible and acceptable for court scrutiny if it cannot be disputed or refuted.
3. **Relevance**—Even if the evidence is admissible, relevant paradigms of the information must be connected with the case to enhance its usefulness and weight. Both the aspects of time and expenditures can be managed more effectively if the legal professional suggests which data must be gathered and which would be most effective.

a. The Bond That Binds Them All Together

To return to the general rule, a structure is dependent on the firm's participation. For example, there are directors, owners, architects, builders, and contractors in the Zachman framework (Zachman) for enterprise-wide frameworks.

System proprietors, digital forensics researchers, and legal professionals are all anticipated to be engaged in a normal digital forensics inquiry. Nevertheless, if the duties and obligations of these people are split deeper, one can classify them into eight different types of individual investigators. The following jobs are unique for every individual, yet they could be performed by the same individual if necessary:

- Case handler.
- Owner of the system.
- Legal advisors.
- Auditors, architects, and security professionals of the system.
- Digital forensics specialists.
- Investigator and system administrator.
- Analyst.
- Legal prosecutor.

The case handler is the orchestrator and organiser of the whole digital inquiry. They would be in charge of the issue and therefore decide whether the inquiry should proceed. The proprietor of the system being examined is the system/business operator. They are typically the case's complainant and supporter. If the situation involves web hackers, for example, their computer might be harmed, but they would have to approach the authorities

for an inquiry. In certain cases, the proprietor may be a possible suspect. For instance, if the case involves the illicit downloading of music tracks, the proprietor would be the main suspect.

The very first legal professional whom the case manager should consult for legal counsel is a legal advisor. He or she may counsel the case manager on whether it is appropriate to move ahead with court battles. Because a digital forensics inquiry is a procedure for obtaining relevant information for a legal matter, resources and time may be saved if the case manager can obtain legal guidance and evaluate whether it is possible to present the case in court at an intermediate phase of the research. Furthermore, the researcher might focus more on obtaining electronic information pertinent to the issue.

Even if legal counsel is provided, the case manager must investigate and obtain a better understanding of the systems undergoing inspection and their safety architecture. The system/solution architect, security consultant, and internal auditor should all be questioned in a large organisation. The case manager will be ready to evaluate the extent of the issue and identify the security management architecture that has been installed on the platforms based on these conversations.

The case manager may then appoint or engage appropriate digital forensics specialists to oversee the overall process. The investigation of digital forensics is not a one-time event. Various research techniques may be developed based on the nature of the industry, systems engineering, and legal counsel. As a result, when planning the complete investigation approach, digital forensics experts should review all of the contributions and demands from the professional counsel. They must also consider whether it is essential to enlist the help of third-party suppliers or an outside expert to complete certain aspects of the inquiry. Subsequently, digital forensics experts will present the digital forensics investigator with the established plan. The inspector's primary duties include gathering, extracting, preserving, and storing digital information from networks. Based on the system manager's agreement, a digital forensics researcher might or might not be allowed to control the system specifically. The firm's system administrator or operatives may well be asked to execute the defined plan and function as the inspector's proxy in the data gathering process.

The digital forensics analyst will need to select the valuable data from the gathered data and compare them with the theoretical model presented for inquiry. Researchers might be required to conduct a variety of tests to confirm or refute the hypothesised model used to simulate the scenario. They must also rebuild the defence's chronology using the retrieved data.

The case manager will evaluate the gathered insights, chronology, and pertinent data with the legal representative to decide if the adversarial system can proceed. The legal attorney or counsellor is usually this type of professional. They may counsel the case manager on whether the evidence obtained is sufficient, pertinent, acceptable, and favourable to a party. They must, likewise, recommend the most practical judicial process to the issue manager. A case may be represented as civil litigation, penal litigation, or perhaps even arbitration. The legal counsel should determine the most suitable venue and manage the case throughout the litigation procedure. Figure 3 depicts the whole process flow. An innovation-based digital forensics investigative structure would indeed be necessary to tie positions, duties, and processes altogether. These jobs and their tasks are connected using the Feasible Forensic Framework.

b. Legal-Side Focus

One of this new framework's advantages is its scope. Various guidelines and requirements could be connected collectively in a more comprehensive way using this structure. The study of digital forensics is no longer viewed solely from a technical perspective. Elements of industry, society, and law are all considered. Furthermore, legal representatives and prosecutors can work far more proactively and methodically in modern forensics inquiries overall. A legal professional may serve as a legal advisor and/or legal prosecutor as per the structure.

As a legal advisor, this person can concentrate on the following questions:

- i. **Legal goals (Why)**
 - (a) What is the ultimate resolution of this issue?
 - (b) What is the law regarding this issue?
 - (c) Does the case fall under the category of criminal or civil?
 - ii. **Legal backgrounds and primary disputes (What)**
 - What is/are the applicable law(s) or ordinance(s)?
 - To which parts of the ordinance should one refer?
 - What were the ordinance's main points?
 - What documentation is required and related?
 - What information should be gathered?
 - What is the difference between legal and factual issues?
 - iii. **Legal processes for subsequent inquiries (How)**
 - Is an order (such as the Anton Piller Injunction) necessary?
 - Is a background check or any kind of warrant required?
 - Is there anything that needs to be done to preserve the proof?
 - iv. **Legal location (Where)**
 - Is it under the legislative authorities of the country?
 - v. **Legal individuals and members (Who)**
 - Who is the claimant or the participants?
 - Who holds the responsibility of being the legal councillor, prosecutor, legal staff, or other relevant legal staff?
 - vi. **Legal timeline (When)**
 - What exactly is the deadline for the case?
 - Is it under the ultimate timeframe limit?
 - How much time is it expected to take?
 - What are the durations of similar cases and expenses?
- Case handlers focus on the problems of the dispute and dredge up pertinent information regarding legal counsel. The case manager will have a much better overview of the issue after the forensic analysis techniques are performed and be ready to decide and conduct a discussion with the legal counsel. Typically, the legal prosecutor will use information from the investigation leader and forensic experts, rebuild the evidence, and explain it from a legal standpoint. As a result, the legal prosecutor would concentrate on the following issues and questions:
- vii. **Goals of legal presentation (Why)**
 - Should the case be continued or dismissed?
 - Has enough evidence been gathered?
 - What type of legal action should be pursued?
 - viii. **Characteristics of legal representation (What)**
 - Should a penalty be approved?
 - What data should have been included and what should be left out?
 - How should the information be proffered?
 - What evidence is important and acceptable in this case?
 - ix. **Methods for presenting legal arguments (How)**
 - What kind of legal strategy should be used? (Is it better to use international arbitration or local civil lawsuits?)
 - What strategy should be used during the legal process?
 - Where should the lawsuit take place in terms of legal authority?
 - Where should the regulation take place?
 - Where does the hearing take place?
 - x. **Entities involved in legal proceedings (Who)**

- Who should be called as a witness?
 - Is it necessary to summon any expert testimony?
 - Who are the judges, cabinets, and arbitrators?
- xi. **For the presentation, a timeline of the full event is provided (When)**
- Is the complete storyboard being rebuilt?
 - Is there a timeframe lacking from the evidence?
 - When do you think the case must be introduced?

8. Conclusions

This study concluded that most organisations are not aware of the need to design IT support to support legal actions and meet the ethics and business's regulatory requirements. The Feasible Forensic Framework introduces two key properties. The initial property is that the framework proposes digital artefacts and mapping to generalise the steps of the attacks. The second property is that it provides detailed steps for ethically examining and analysing the digital evidence required for an investigation. Security audit and activity logging are required to properly manage records in a digital forensic investigation. The framework highlights the benefits of making an organisation forensically ready and resolving ethical issues relevant digital forensic investigations.

The discussion suggested that forensic readiness benefits the structure of IT security. Organisations can use this particular framework to improve their strategies related to IT security. Identifying security vulnerabilities will enable the business to strengthen its defences. With security in mind, a proper investigation of forensic readiness can be conducted.

Author Contributions: Conceptualization, A.A. (Amr Adel); Validation, A.A. (Amr Adel); Formal analysis, A.A. (Amr Adel); Investigation, A.A. (Amr Adel); Resources, A.A. (Amr Adel); Writing—original draft, A.A. (Amr Adel); Writing—review & editing, A.A. (Ali Ahsan); Supervision, A.A. (Ali Ahsan) and C.D.; Project administration, C.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research has not received a grant.

Institutional Review Board Statement: The ethical aspects of this research project have been approved by the Human Research Ethics Committee (HREC) of Torrens University Australia, reference number 0303.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author, upon reasonable request.

Conflicts of Interest: The authors declare no competing interests.

References

- Pollitt, M. Six Blind Men from Indostan. In *Digital Forensics Research Workshop (DFRWS)*. 2004. Available online: https://dfrws.org/wp-content/uploads/2019/06/2004_USA_pres-a_framework_for_digital_forensic_science.pdf (accessed on 27 November 2023).
- Brill, A.E.; Pollitt, M.; Morgan Whitcomb, C. The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications. *J. Digit. Forensic Pract.* **2006**, *1*, 3–11. [CrossRef]
- Prasanthi, B.V. Cyber Forensic Science to Diagnose Digital Crimes—A study. *Int. J. Comput. Trends Technol. (IJCTT)* **2017**, *50*, 107–113. [CrossRef]
- Digital Forensics: An Integrated Approach for the Investigation of Cyber/Computer Related Crimes. Available online: <https://uobrep.openrepository.com/handle/10547/326231> (accessed on 9 June 2024).
- Karie, N.M.; Venter, H.S. Taxonomy of Challenges for Digital Forensics. *J. Forensic Sci.* **2015**, *60*, 885–893. [CrossRef] [PubMed]
- Luciano, L.; Baggili, I.; Topor, M.; Casey, P.; Breitingner, F. Digital Forensics in the Next Five Years. In *Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–14.
- Simon, M.; Choo, K.-K.R. Digital Forensics: Challenges and Future Research Directions'. Rochester, NY, USA, 7 April 2014. Available online: <https://papers.ssrn.com/abstract=2421339> (accessed on 9 June 2024).

8. Watson, S.; Dehghantanha, A. Digital forensics: The missing piece of the Internet of Things promise. *Comput. Fraud Secur.* **2016**, *2016*, 5–8. [CrossRef]
9. Ferguson, R.I.; Renaud, K.; Wilford, S.; Irons, A. PRECEPT: A framework for ethical digital forensics investigations. *J. Intellect. Cap.* **2020**, *21*, 257–290. [CrossRef]
10. Gruber, J.; Voigt, L.L.; Benenson, Z.; Freiling, F.C. Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations. *Forensic Sci. Int. Digit. Investig.* **2022**, *43*, 301438. [CrossRef]
11. Losavio, M.; Adams, J.; Rogers, M. Gap Analysis: Judicial Experience and Perception of Electronic Evidence. *J. Digit. Forensic Pract.* **2006**, *1*, 13–17. [CrossRef]
12. Kebande, V.R.; Venter, H.S. A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. *WIREs Forensic Sci.* **2019**, *1*, e1350. [CrossRef]
13. Adel, A. A Conceptual Framework to Improve Cyber Forensic Administration in Industry 5.0: Qualitative Study Approach. *Forensic Sci.* **2022**, *2*, 111–129. [CrossRef]
14. Ab Rahman, N.H.; Cahyani, N.D.W.; Choo, K.-K.R. Cloud incident handling and forensic-by-design: Cloud storage as a case study. *Concurr. Comput. Pract. Exp.* **2017**, *29*, e3868. [CrossRef]
15. Ab Rahman, N.H.; Glisson, W.B.; Yang, Y.; Choo, K.-K.R. Forensic-by-Design Framework for Cyber-Physical Cloud Systems. *IEEE Cloud Comput.* **2016**, *3*, 50–59. [CrossRef]
16. Cusack, B.; Maeakafa, G. Establishing effective and economical traffic surveillance in Tonga. In Proceedings of the 14th Australian Digital Forensics Conference, Perth, Australia, 5–6 December 2016; pp. 50–56. [CrossRef]
17. Adel, A. Developing a Digital Forensic Capability for Critical Infrastructures: An Investigation Framework, Auckland University of Technology. 2020. Available online: <https://hdl.handle.net/10292/13317> (accessed on 9 June 2024).
18. Bankole, F.; Taiwo, A.; Claims, I. An extended digital forensic readiness and maturity model. *Forensic Sci. Int. Digit. Investig.* **2022**, *40*, 301348. [CrossRef]
19. Li, M.; Lal, C.; Conti, M.; Hu, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Gener. Comput. Syst.* **2021**, *115*, 406–420. [CrossRef]
20. Singh, K.S.; Irfan, A.; Dayal, N. Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks. In Proceedings of the 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019; pp. 584–590.
21. Singh, A.; Ikuesan, A.R.; Venter, H.S. Digital Forensic Readiness Framework for Ransomware Investigation. In Proceedings of the Digital Forensics and Cyber Crime; Breiting, F., Baggili, I., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 91–105.
22. Kumar, G.; Saha, R.; Lal, C.; Conti, M. Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Gener. Comput. Syst.* **2021**, *120*, 13–25. [CrossRef]
23. Dimitriadis, A.; Ivezic, N.; Kulvatunyou, B.; Mavridis, I. D4I-Digital forensics framework for reviewing and investigating cyber attacks. *Array* **2020**, *5*, 100015. [CrossRef]
24. Al-Masri, E.; Bai, Y.; Li, J. A Fog-Based Digital Forensics Investigation Framework for IoT Systems. In Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 21–23 September 2018; pp. 196–201.
25. 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**, *73*, 294–306. [CrossRef]
26. Sathwara, S.; Dutta, N.; Pricop, E. IoT Forensic A digital investigation framework for IoT systems. In Proceedings of the 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018; pp. 1–4.
27. Horsman, G. Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. *Digit. Investig.* **2019**, *28*, 146–151. [CrossRef]
28. Kebande, V.R.; Ray, I. A Generic Digital Forensic Investigation Framework for Internet of Things (IoT). In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 356–362.
29. Lutta, P.; Sedky, M.; Hassan, M.; Jayawickrama, U.; Bakhtiari Bastaki, B. The complexity of internet of things forensics: A state-of-the-art review. *Forensic Sci. Int. Digit. Investig.* **2021**, *38*, 301210. [CrossRef]
30. Bakhshi, T. Forensic of Things: Revisiting Digital Forensic Investigations in Internet of Things. In Proceedings of the 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), Karachi, Pakistan, 10–11 December 2019; pp. 1–8.
31. Lillis, D.; Becker, B.; O'Sullivan, T.; Scanlon, M. Current Challenges and Future Research Areas for Digital Forensic Investigation. *arXiv* **2016**, arXiv:1604.03850. [CrossRef]
32. Vincze, E.A. Challenges in digital forensics. *Police Pract. Res.* **2016**, *17*, 183–194. [CrossRef]
33. Montasari, R.; Hill, R. Next-Generation Digital Forensics: Challenges and Future Paradigms. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019; pp. 205–212.
34. Quick, D.; Choo, K.-K.R. Big forensic data reduction: Digital forensic images and electronic evidence. *Clust. Comput* **2016**, *19*, 723–740. [CrossRef]
35. Scanlon, M. Battling the digital forensic backlog through data deduplication. In Proceedings of the 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland, 24–26 August 2016; pp. 10–14.

36. Quick, D.; Choo, K.-K.R. Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. *Future Gener. Comput. Syst.* **2018**, *78*, 558–567. [\[CrossRef\]](#)
37. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *78*, 544–546. [\[CrossRef\]](#)
38. Haefner, N.; Wincent, J.; Parida, V.; Gassmann, O. Artificial intelligence and innovation management: A review, framework, and research agenda. *Technol. Forecast. Soc. Change* **2021**, *162*, 120392. [\[CrossRef\]](#)
39. Torous, J.; Bucci, S.; Bell, I.H.; Kessing, L.V.; Faurholt-Jepsen, M.; Whelan, P.; Carvalho, A.F.; Keshavan, M.; Linardon, J.; Firth, J. The growing field of digital psychiatry: Current evidence and the future of apps, social media, chatbots, and virtual reality. *World Psychiatry* **2021**, *20*, 318–335. [\[CrossRef\]](#) [\[PubMed\]](#)
40. Al-Khateeb, H.; Epiphaniou, G.; Daly, H. Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger. In *Blockchain and Clinical Trial: Securing Patient Data*; Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G., Al-Khateeb, H., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 149–168, ISBN 978-3-030-11289-9.
41. D’Anna, T.; Puntarello, M.; Cannella, G.; Scalzo, G.; Buscemi, R.; Zerbo, S.; Argo, A. The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data. *Healthcare* **2023**, *11*, 634. [\[CrossRef\]](#) [\[PubMed\]](#)
42. Lone, A.H.; Mir, R.N. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digit. Investig.* **2019**, *28*, 44–55. [\[CrossRef\]](#)
43. Ali, M.; Ismail, A.; Elgohary, H.; Darwish, S.; Mesbah, S. A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain. *Symmetry* **2022**, *14*, 334. [\[CrossRef\]](#)
44. Elgohary, H.M.; Darwish, S.M.; Elkaffas, S.M. Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications. *IEEE Access* **2022**, *10*, 14669–14679. [\[CrossRef\]](#)
45. Sarishma; Gupta, A.; Mishra, P. Blockchain Based Framework to Maintain Chain of Custody (CoC) in a Forensic Investigation. In *Proceedings of the Advances in Computing and Data Sciences*; Singh, M., Tyagi, V., Gupta, P.K., Flusser, J., Ören, T., Sonawane, V.R., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 37–46.
46. Khan, A.A.; Shaikh, A.A.; Laghari, A.A.; Dootio, M.A.; Rind, M.M.; Awan, S.A. Digital forensics and cyber forensics investigation: Security challenges, limitations, open issues, and future direction. *Int. J. Electron. Secur. Digit. Forensics* **2022**, *14*, 124–150. [\[CrossRef\]](#)
47. Khan, A.A.; Shaikh, A.A.; Laghari, A.A. IoT with Multimedia Investigation: A Secure Process of Digital Forensics Chain-of-Custody using Blockchain Hyperledger Sawtooth. *Arab. J. Sci. Eng.* **2023**, *48*, 10173–10188. [\[CrossRef\]](#)
48. Isaac Abiodun, O.; Alawida, M.; Esther Omolara, A.; Alabdulatif, A. Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 10217–10245. [\[CrossRef\]](#)
49. Conlan, K.; Baggili, I.; Breiting, F. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digit. Investig.* **2016**, *18*, S66–S75. [\[CrossRef\]](#)
50. Choi, D.-H. Digital Forensic: Challenges and Solution in the Protection of Corporate Crime. *J. Ind. Distrib. Bus.* **2021**, *12*, 47–55. [\[CrossRef\]](#)
51. Kumar, A.; Chauhan, M.; Jain, A.K.; Johri, P. Analysis on Digital Forensics Challenges and Anti-forensics Techniques in Cloud Computing. In *Proceedings of the 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, Moradabad, India, 16–17 December 2022; pp. 699–702.
52. Gashi, H.; Zargari, S.; Jalali Ghazaani, S. Data Hiding in Anti-forensics—Exploit Delivery Through Digital Steganography. In *Proceedings of the Cybersecurity Challenges in the Age of AI, Space Communications and Cyborgs*; Jahankhani, H., Ed.; Springer Nature Switzerland: Cham, Switzerland, 2024; pp. 65–76.
53. Javed, A.R.; Ahmed, W.; Alazab, M.; Jalil, Z.; Kifayat, K.; Gadekallu, T.R. A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access* **2022**, *10*, 11065–11089. [\[CrossRef\]](#)
54. Singh, A.; Ikuesan, R.A.; Venter, H. Secure Storage Model for Digital Forensic Readiness. *IEEE Access* **2022**, *10*, 19469–19480. [\[CrossRef\]](#)
55. Horsman, G.; Sunde, N. Unboxing the digital forensic investigation process. *Sci. Justice* **2022**, *62*, 171–180. [\[CrossRef\]](#) [\[PubMed\]](#)
56. Prakash, V.; Williams, A.; Garg, L.; Barik, P.; Dhanaraj, R.K. Cloud-Based Framework for Performing Digital Forensic Investigations. *Int. J. Wirel. Inf. Netw.* **2022**, *29*, 419–441. [\[CrossRef\]](#)
57. Yaacoub, J.-P.A.; Noura, H.N.; Salman, O.; Chehab, A. Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet Things* **2022**, *19*, 100544. [\[CrossRef\]](#)
58. 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. [\[CrossRef\]](#)
59. Casino, F.; Dasaklis, T.K.; Spathoulas, G.P.; Anagnostopoulos, M.; Ghosal, A.; Borocz, I.; Solanas, A.; Conti, M.; Patsakis, C. Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. *IEEE Access* **2022**, *10*, 25464–25493. [\[CrossRef\]](#)
60. Horsman, G. Defining principles for preserving privacy in digital forensic examinations. *Forensic Sci. Int. Digit. Investig.* **2022**, *40*, 301350. [\[CrossRef\]](#)
61. Stoykova, R. The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Comput. Law Secur. Rev.* **2023**, *49*, 105801. [\[CrossRef\]](#)

62. Maratsi, M.I.; Popov, O.; Alexopoulos, C.; Charalabidis, Y. Ethical and Legal Aspects of Digital Forensics Algorithms: The Case of Digital Evidence Acquisition. In *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*; Association for Computing Machinery: New York, NY, USA, 2022; pp. 32–40.
63. Samdani, S.; Kumar, D.D. A Holistic Examination Of Investigative And Prosecutorial Practices In Addressing Cyber And Physical Offenses Within India. *Educ. Adm. Theory Pract.* **2023**, *29*, 525–532. [CrossRef]
64. Ogunseyi, T.B.; Adedayo, O.M. Cryptographic Techniques for Data Privacy in Digital Forensics. *IEEE Access* **2023**, *11*, 142392–142410. [CrossRef]
65. Firdonsyah, A.; Purwanto, P.; Riadi, I. Framework for Digital Forensic Ethical Violations: A Systematic Literature Review. *E3S Web Conf.* **2023**, *448*, 01003. [CrossRef]
66. Di Nuzzo, V. Search and Seizure of Digital Evidence: Human Rights Concerns and New Safeguards. In *Investigating and Preventing Crime in the Digital Era: New Safeguards, New Rights*; Bachmaier Winter, L., Ruggeri, S., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 119–149, ISBN 978-3-031-13952-9.
67. Renaud, K.; Bongiovanni, I.; Wilford, S.; Irons, A. PRECEPT-4-Justice: A bias-neutralising framework for digital forensics investigations. *Sci. Justice* **2021**, *61*, 477–492. [CrossRef] [PubMed]
68. Horsman, G.; Sunde, N. Part 1: The need for peer review in digital forensics. *Forensic Sci. Int. Digit. Investig.* **2020**, *35*, 301062. [CrossRef]
69. Solanke, A.A. Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. *Forensic Sci. Int. Digit. Investig.* **2022**, *42*, 301403. [CrossRef]
70. Karagiannis, C.; Vergidis, K. Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information* **2021**, *12*, 181. [CrossRef]
71. Wilson-Kovacs, D. Digital media investigators: Challenges and opportunities in the use of digital forensics in police investigations in England and Wales. *Polic. Int. J.* **2021**, *44*, 669–682. [CrossRef]
72. Tully, G.; Cohen, N.; Compton, D.; Davies, G.; Isbell, R.; Watson, T. Quality standards for digital forensics: Learning from experience in England & Wales. *Forensic Sci. Int. Digit. Investig.* **2020**, *32*, 200905. [CrossRef]
73. Chen, C.; Dong, B. Digital forensics analysis based on cybercrime and the study of the rule of law in space governance. *Open Comput. Sci.* **2023**, *13*. [CrossRef]
74. Marshall, K.; Rea, A. Legal Challenges in Cloud Forensics'. In AMCIS. 2021. Available online: https://web.archive.org/web/20220803140614id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1341&context=amcis2021 (accessed on 18 February 2024).
75. Sarfraz, M. *Cybersecurity Threats with New Perspectives*; BoD—Books on Demand: London, UK, 2021; ISBN 978-1-83968-852-2.
76. Sharma, B.K.; Hachem, M.; Mishra, V.P.; Kaur, M.J. Internet of Things in Forensics Investigation in Comparison to Digital Forensics. In *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*; Singh, P.K., Bhargava, B.K., Paprzycki, M., Kaushal, N.C., Hong, W.-C., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 672–684, ISBN 978-3-030-40305-8.
77. Gogolin, G. (Ed.) *Digital Forensics Explained*, 2nd ed.; CRC Press: Boca Raton, FL, USA, 2021; ISBN 978-1-00-304935-7.
78. Mohammed, S.; Sridevi, R. A Survey on Digital Forensics Phases, Tools and Challenges. In *Proceedings of the Third International Conference on Computational Intelligence and Informatics*; Raju, K.S., Govardhan, A., Rani, B.P., Sridevi, R., Murty, M.R., Eds.; Springer: Singapore, 2020; pp. 237–248.
79. Yeboah-Ofori, A.; Brown, A.D. Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *J. Forensic Leg. Investig. Sci.* **2020**, *6*, 1–8. [CrossRef] [PubMed]
80. Stigall, M.; Choo, K.-K.R. Digital Forensics Education: Challenges and Future Opportunities. In *Proceedings of the National Cyber Summit (NCS) Research Track 2021*; Choo, K.-K.R., Morris, T., Peterson, G., Imsand, E., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 28–46.
81. Muthye, S.S. Challenges in Digital Forensics and Future Aspects. In *Unleashing the Art of Digital Forensics*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2022; ISBN 978-1-00-320486-2.
82. Bas Seyyar, M.; Geradts, Z.J.M.H. Privacy impact assessment in large-scale digital forensic investigations. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 200906. [CrossRef]
83. Casey, E.; Souvignat, T.R. Digital transformation risk management in forensic science laboratories. *Forensic Sci. Int.* **2020**, *316*, 110486. [CrossRef]
84. Stoykova, R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Comput. Law Secur. Rev.* **2021**, *42*, 105575. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.