JURNAL RISET DAN APLIKASI: AKUNTANSI DAN MANAJEMEN

Reconstructing Audit Evidence Integrity through Digital Forensics

Naela Zaqiyatul Misqiyah[1*], Sopian[2].

Politeknik Keuangan Negara STAN, Jl Bintaro Utama Sektor V, Bintaro Jaya, Tangerang Selatan, 15222

***naela_4132230038@pknstan.ac.id**

doi.org/10.33795/jraam.v8i2.001

Article Information

Submission date	29-05-2025
Revised date	15-01-2026
Accepted date	26-01-2026

Keywords:

Certification;
Digital Evidence;
Digital Forensic;
Digital Forensic Laboratory (DFL);
Licensing;
Training.

Abstract: Reconstructing Audit Evidence Integrity through Digital Forensics

Purpose: *this study determines how the digital forensics laboratory (DFL) is used to assist investigative audit.*

Method: *this study adopts a descriptive qualitative research design.*

Results: *the use of BPKP's Digital Forensics Laboratory (DFL) complies with international standards, which have been codified in BPKP rules and SOPs.*

Novelty: *the author examines the use of the DFL, both the concept and the actual practices.*

Contribution: *this study enriches the literature on digital forensics and serve as a reference for BPKP's Deputy for Investigation in enhancing the effectiveness of digital forensics laboratory utilization.*

Kata kunci:

Sertifikasi;
Bukti Digital;
Forensik Digital;
Laboratorium Forensik Digital (DFL);
Lisensi;
Pelatihan.

Abstrak: Merekonstruksi Integritas Bukti Audit melalui Forensik Digital

Tujuan: untuk mengetahui bagaimana laboratorium forensik digital (DFL) digunakan dalam membantu audit investigatif.

Metode: penelitian ini menggunakan desain penelitian deskriptif kualitatif.

Hasil: penggunaan laboratorium forensik digital BPKP telah mematuhi standar internasional yang telah dikodifikasi ke dalam peraturan dan SOP BPKP.

Kebaruan: penulis menguji penggunaan DFL, baik dari sisi konsep maupun praktik aktual di lapangan.

Kontribusi: penelitian ini memperkaya literatur mengenai forensik digital dan menjadi referensi bagi Deputi Bidang Investigasi BPKP dalam meningkatkan efektivitas pemanfaatan laboratorium forensik digital.

1. Introduction

Corruption has long been a deeply rooted problem in Indonesia and remains one of the main challenges in the nation's development process (see Figure 1). BPKP actively contributes to anti-corruption efforts in Indonesia through one of its echelon I units, the Deputy for Investigation. Previous research has shown that irregularities identified in fraud audits conducted by BPKP

have an influence on the level of corruption at the provincial level in Indonesia [1]. Investigative audits continue to emphasize the systematic process of identifying, collecting, analyzing, and evaluating evidence, even under technological exposure [2]. In the process of collecting evidence to substantiate indications of irregularities in an audit case, auditors apply the concept of fraud axioms: (a) fraud is inherently concealed, (b) the burden of proof is reversed, and (c) the occurrence of fraud is determined solely by the court [1]. According to the first fraud axiom, perpetrators often commit fraudulent acts in a concealed manner. Consequently, digital forensic teams need specialized tools to obtain digital evidence that can substantiate audit hypotheses. In response to this need, the Deputy for Investigation initiated the establishment of the BPKP Digital Forensic Laboratory (DFL) in 2012. The laboratory functions as a forensic facility aimed at detecting irregularities committed by specific individuals [3].

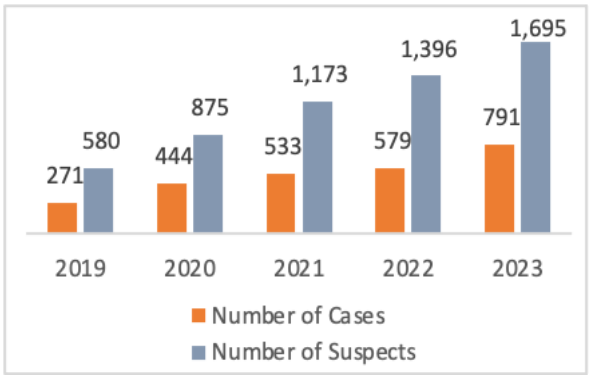

Figure 1. Corruption Trend in Indonesia

A significant portion of the evidence collected by audit teams now exists in digital form. This concern arises because, in judicial proceedings, the admissibility and authenticity of audit evidence are frequently challenged [4]. The legal foundation for the admissibility of digital evidence is stipulated in Law No. 1 of 2024 concerning Electronic Information and Transactions (UU ITE), which declares that electronic information and/or electronic documents and/or their printed results shall constitute valid evidence. However, while the law extends the definition of admissible evidence to include electronic forms, it does not provide explicit guidelines for verifying the authenticity of such digital evidence [5].

Existing literature on digital forensics in Indonesia remains limited, particularly regarding its institutional application within public sector auditing. Conversely, several other countries have demonstrated a stronger awareness of the significance of digital forensics. For instance, a study conducted in Iraq elaborated on the digital forensic process and the tools that can be applied in practice [6]. Research conducted in India outlined the stages of forensic analysis on storage media, the examination of concealed data, network forensics methodologies, and the various forms of digital crimes that may occur [7]. This paper introduces a novel tool that integrates digital forensic investigation with crime data mining techniques. A study published in IEEE Access, involving researchers from multiple countries, highlighted several challenges encountered in digital forensics. Among these, the most critical were identified at the evidence acquisition and pre-processing stages [8]. Those studies indicates that while the technical foundations of digital forensics are well established internationally, there remains a conceptual and institutional gap in how digital forensics is integrated into public accountability mechanisms.

This study aims to explore the utilization of BPKP's Digital Forensic Laboratory as a mechanism to effectively manage and safeguard audit evidence. This is expected to strengthen the evidentiary process in litigation, considering that the integrity of digital evidence is frequently questioned, particularly regarding whether the evidence has remained unaltered from its initial collection to its presentation in court [9]. Furthermore, the author seeks to assess the extent to which BPKP's Digital Forensic

Laboratory complies with established standards, as well as to explore the benefits and challenges arising from its utilization in supporting investigative audit activities performed by BPKP auditors.

2. Method

This study adopts a descriptive qualitative research design. As stated by Creswell, qualitative research involves an exploratory approach aimed at understanding the meaning of a phenomenon as experienced by individuals or groups [10]. This descriptive qualitative study utilizes an inductive approach, which begins with the collection of data followed by the exploration of emerging themes or issues to be examined in greater depth [11]. Based on the data collected, the author carried out data analysis and derived conclusions from the processed results.

The main source of data in this study was obtained through interviews with eleven participants, comprising three members of BPKP's Digital Forensic Laboratory (DFL), six auditors from BPKP, one representative from a ministry or government agency (K/L), and one representative from a state-owned enterprise (BUMN). A detailed summary of the interviews is provided in Table 1. The author decided to interview those informants to ensure trustworthiness of the data. The credibility of the data established through triangulation of information from different sources/roles (LFD personnel, auditor, and institutional user) [12].

Table 1. The details of The Interviews

Jabatan Narasumber	Tanggal Wawancara	Lokasi	Kode
DFL Coordinator	December 18th, 2024	*Zoom meeting*	DFL.01
DFL team	December 16th, 2024	BPKP	DFL.02
DFL team	January 7th, 2025	BPKP	DFL.03
Senior Auditor	January 7th, 2025	BPKP	TA.01
Junior Auditor	January 11th, 2025	*Zoom meeting*	TA.04
Senior Auditor	December 24th, 2024	BPKP	TA.05
Senior Auditor	December 23rd, 2024	BPKP	TA.06
Senior Auditor	January 3rd, 2025	BPKP	TA.02
Senior Auditor	December 16th, 2024	Written (Document-Based)	TA.03
Lead Auditor of K/L	January 15th, 2025	*Zoom meeting*	K/L
Senior Officer Audit BUMN	January 24th, 2025	Written (Document-Based)	BUMN

Following the completion of the interviews, the author conducted data classification through domain and taxonomic analysis. The interview transcripts were carefully reviewed, with segments labeled as domain for data relevant to the research focus and non-domain for data deemed unrelated. Subsequently, the predefined domains were developed into more specific subcategories, a process known as taxonomic analysis. This approach was selected to enable a structured exploration of themes emerging from the interviews, beginning from broad categories (domain) to more detailed subcategories (taxonomies). The author used 3 domains, namely usage, benefit, and challenges. The DFL usages is described by the taxonomy of man, material, machine, money, method. The DFL benefits is described by the taxonomy of producing evidence that cannot be found with conventional audit methods, identifying and tracking evidence of fraud, ensuring the integrity of digital evidence, supporting the litigation process, and indicating special relationships. The DFL challenges is described by the taxonomy of human resource workload, understanding of the business processes of the object of inspection, support from middle management, awareness of DFL procedures, and attitude from targeted electronic media owners. Each taxonomy described by the sub taxonomy.

3. Results and Discussion

Compliance of BPKP's Digital Forensic Laboratory with International Standards . The integrity of evidence in Indonesian judicial proceedings is frequently compromised by systemic challenges related to technological advancements, procedural inconsistencies, and verification difficulties. The key problem is lack of clear digital forensics standards which cause inconsistent evidence assessment in courts [13]. One of the key references guiding digital forensic procedures is the standard developed by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). ISO/IEC 27037:2012 focuses on the processes of identifying, collecting, acquiring, and preserving digital evidence [14], whereas ISO/IEC 27042:2015 emphasizes the analysis and interpretation phases, which culminate in the production of a digital forensic report [15].

In the implementation of ISO/IEC 27037:2012, the BPKP Digital Forensic Laboratory (DFL) must fulfill nine key components outlined within the standard.

First, Chain of custody (CoC). The Digital Forensic Laboratory (DFL) team rigorously upholds the Chain of Custody (CoC) for all data and devices under its possession, from initial collection at the scene, through seizure or borrowing procedures, transportation to the forensic laboratory, and ultimately to their return or presentation in court. This process ensures the integrity of the evidence used in court. The CoC process has been formalized within BPKP's internal DFL Standard Operating Procedures (SOP). This was corroborated by Informant DFL.01 during the interview.

> *"The chain of custody has to record everything, who took it, when, where, and what the condition was. It also has to be photographed all the way until it arrives at the lab. All that documentation has to be there, because to make it valid as audit evidence or even as court evidence, those requirements must be met. That's part of the SOP and also required by the ISO certification."*

Informant DFL.02 also stated, *"The chain of custody starts from the moment we collect the evidence until it is returned. The chain of custody simply records the movement of the item, where it has been and who has had control over it*."

CoC requires comprehensive documentation tracking every detail of evidence handling, including who, when,

where, and the condition of the evidence, with photograph documentation through the process. Resources confirm these requirements notes that chain of custody documentation determines evidence admissibility, with documentation potentially done through written forms, oral testimony, or combination [16]. Other research emphasizes that establishing CoC provides a *"traceable record that guarantees unbroken control over a document, raw data, or a sample"* and recommends outlining guidelines in SOPs [17].

Second, Preventive Measures at the Location. Based on the author's observations, BPKP's Digital Forensic Laboratory (DFL) is equipped with multiple layers of secured doors. The first layer provides access to the reception room, approximately 3 by 2.5 meters in size, furnished with a desk, chairs, and a monitor screen.

The subsequent door is secured with both fingerprint and facial recognition systems, accessible only to authorized members of the DFL team. Regarding the management of digital evidence, BPKP has equipped the DFL with facilities to handle the entire process, from receipt and disassembly to data acquisition and analysis. As stated by Informant DFL.03, the DFL provides designated spaces for each stage, including reception, disassembly, data retrieval, and analytical processing of the evidence. The statement from Informant DFL.03 is presented below.

> *"Here, we have procedures outlining what must be done when we receive electronic devices. The procedures specify which rooms the items should pass through, from the first room to the next, step by step. For example, the disassembly process takes place in this area, while both disassembly and acquisition are handled here. The analysis is conducted on these computers, and the storage is done in this section. Each step must be clearly defined and followed in sequence."*

Forensic equipment requires careful handling, and the confidential data stored within must be adequately secured. Consequently, the DFL has established a series of safety and security systems designed to protect both forensic instruments and digital data. The laboratory features an emergency exit, specialized fire extinguishers, water sprinklers, and smoke detectors. As explained by Informant DFL.01.

> *"In terms of safety, the laboratory is equipped with an emergency exit, fire extinguishers, water sprinklers, and smoke detectors. The fire extinguishers, however, must not contain liquid; they use a bubble-based type to prevent potential damage to data."*

Informant DFL.03 further explained that the security system within the DFL is governed by established Standard Operating Procedures (SOPs). DFL require comprehensive safety measures to protect personnel, equipment, and sensitive data. Research by Al-Khafaji emphasize that scientific laboratories need stringent safety protocols to protect personnel and equipment [18]. The laboratory is equipped with essential safety features including emergency exit, water sprinkles, and smoke detectors.

Third, Roles and Responsibilities. The Digital Forensic Laboratory (DFL) comprises 13 personnel, twelve of whom are certified auditors, and one is a functional computer specialist. To formally define their roles and responsibilities, the DFL team operates under an official decree issued by the Deputy for Investigation of BPKP No. HK.01.01/KEP-124/D5/04/2023 about Establishment of BPKP's Digital Forensic Laboratory. The organizational composition of the DFL, as stipulated in the official Decree, includes several key positions: the Head of the DFL, Quality Manager, Technical Manager, Administrative Manager, Supervisor, Laboratory Officer, and Analysts. The DFL's organizational structure includes key position such as above. This structure approach aligns

Table 2. Certification of DFL team

Certification	Numbers of Personnel
Cellebrite Certified Operator	3
Cellebrite Certified Physical Analyst	3
Computer Hacking Forensic Investigator	12
Encase Certified Examiner	5
Magnet Certified Cloud Examiner	9
Magnet Certified Forensics Examiner	11
Magnet Certified macOS Examiner	4
Wiley Certified Data Scientist	2

Table 3. Training Program of DFL Team

Training Program	Numbers of Personnel
ACL Galvanize Data Analytics	5
Advanced Analysis of Windows Artifacts with EnCase Forensic (Encase Advance)	2
AX200 Magnet AXIOM Examination	2
BS050 Customized Digital Forensics for Implementation	10
Building an Investigation with EnCase Forensic Training (CF2)	5
Cellebrite Certified Operator (CCO)	4
Cellebrite Certified Physical Analyst (CCPA)	3
Computer Hacking Forensic Investigator (CHFI)	12
Foundations in Digital Forensics with Encase Forensic (CF1)	6
Magnet Certified Cloud Examiner	9
Magnet Certified Forensics Examiner	11
Magnet Certified macOS Examiner	4
Magnet Macintosh OS Examination	3
Mobile Phone Analysis with Oxygen Forensic	1
Internal Audit Training based on ISO 9001	12

with ISO/IEC 17025:2017 which emphasize clear personnel and responsibilities [19].

Fourth, Competence. To date, there has been no standardized benchmark for evaluating individual competency levels. One practical approach to assessing the expertise of digital forensic professionals is by reviewing their professional certifications and training histories. The table below summarizes the certifications held by the DFL personnel.

Aside from professional certifications, DFL personnel have attended several training programs, which are outlined as follows Table 3.

All certifications and training activities were conducted by BPKP. This was confirmed by Informant DFL.01, who remarked, *"All of them are provided by the office; personal ones are too expensive."* and by Informant DFL.02, who stated, *"From the office."* These statements indicate that BPKP's top management has shown strong commitment and support in facilitating and enhancing the capacity of the DFL.

Professional certification and training are indeed a robust approach to assessing digital forensics expertise, with multiple studies confirming the importance of comprehensive skill development. Craiger et al. demonstrate that digital forensics competence requires a multifaceted skill set encompassing technical knowledge, legal understanding, and communication abilities [20].

Fifth, Reasonable Care. In accordance with ISO/IEC 27037:2012, digital data must be stored in a secure and controlled environment. Laboratories responsible for storing digital evidence should not be exposed to magnetic fields, dust, vibration, humidity, or other environmental factors that could compromise data integrity. The environmental management of the DFL laboratory considers aspects such as layout, cleanliness, temperature, and magnetic exposure. As explained by Informant DFL.03.

> *"Environmental management in the laboratory follows specific procedures that clearly outline each step once we receive electronic devices. Cleanliness and temperature are critical, as excessive heat can be harmful when processing large volumes of data. We also monitor any magnetic fields in the surrounding area, as these can affect electronic storage systems."*

Digital forensic laboratories must implement rigorous environmental management procedures to preserve the integrity of electronic evidence, with careful attention to temperature, cleanliness, and magnetic field exposure. One of the studies state the importance of systematic procedures in digital forensic analysis [21].

Sixth, Documentation. DFL personnel, together with their clients, carry out documentation at every stage of the process, from pre-planning, planning, execution, and reporting. A key aspect of this documentation is maintaining a comprehensive Chain of Custody (CoC). As explained by Informant DFL.03,

> *"The chain of custody must record everything, who collected the evidence, the date, the time, the location, and the condition of the item. Photographic documentation is also required until the evidence arrives at the laboratory." Informant DFL.02 further elaborated, "The chain of custody serves as an audit trail. It does not necessarily ensure that the data remains undamaged, but rather helps determine who is accountable if any damage occurs."*

Proper documentation is crucial during the handover of electronic media for data acquisition. When the DFL team collaborates with investigative authorities, the investigators possess legal authority to seize evidence, which allows the process to proceed with only a handover report from the investigator to the DFL team. Conversely, when collaborating with non-investigative institutions, the DFL team lacks the authority to confiscate evidence. In such cases, formal authorization in the power of attorney form, signed by both the head of the respective institution and the Deputy for Investigation of BPKP, is required.

Proper documentation is crucial in digital forensics, with distinct protocols for evidence handover depending on the investigating authority's legal status. Documentation by DFL team ensures the integrity of digital evidence collection, addressing the critical need for legal compliance and chain of custody [22].

Seventh, Guidance. The highest level of oversight within BPKP's Digital Forensic Laboratory (DFL) is exercised by the Deputy for Investigation, who has actively encouraged the DFL team to support investigative audit engagements. As stated by Informant DFL.01.

> *"Almost all, in fact, under the Deputy's recent directive, all ATT, AI, and PKKN assignments are now required*

to include a forensic coordinator in the assignment letter."

The Digital Forensic Coordinator issues operational guidance upon receiving a disposition letter requesting forensic assistance. Such guidance includes determining team composition according to individual expertise, defining objectives and scope, and providing supervision throughout implementation, especially when difficulties occur. A study reinforces the importance of standard operating procedures, noting that each digital forensics investigation is unique and requires special examination, making the coordinator's guidance crucial for through and secure implementation [23].

Eighth, Prioritization of Data Collection and Acquisition. The DFL team is required to maximize the volume and relevance of data collected and acquired. In the forensic process, the materials analyzed typically consist of electronic devices and the raw data extracted from them. As stated by Informant DFL.02,

"It depends on the type and form of the electronic media from which we need to retrieve data. For instance, as shown in my slides, the items include mobile phones, laptops, CCTV systems, and voice recorders."

Representatives from both state-owned enterprises and ministries, whose data were previously processed by the DFL team, confirmed that several electronic media had been borrowed for forensic analysis. The state-owned enterprises and ministries, whose data were previously representative stated, *"Computers and emails."* The ministry representative added,

"Mr. A (forensic personnel) instructed us to formally submit a letter requesting assistance. We provided a mobile phone and an external hard disk. The internal hard disk and the phone belonged to Mr. B (K/L personnel), who handed them over directly."

The data acquisition process employs devices such as write blockers or duplicators. The DFL utilizes the Tableau Comprehensive Write Block Kit, a globally recognized and widely used tool among digital forensic practitioners [24]. This device facilitates the imaging process, which involves duplicating the entire contents of a storage medium from the targeted electronic device.

By using a write blocker, the data can be safely copied without alteration, while maintaining the integrity and traceability of the source data. The imaging procedure follows a sector-by-sector approach to ensure that the duplicate is an exact and unmodified replica of the original [24]. This equipment is used for acquiring data from laptops, desktop computers, mobile phones, and external hard drives.

Digital forensic data collection prioritization requires a systematic approach that maximizes data volume and relevance while maintaining strict integrity protocol. Several studies state key prioritization strategies in digital forensic include using write blockers to prevent data alternation [25], employing sector by sector imaging to create exact replicas of original data, and selecting appropriate acquisition methods based on media type [26].

Ninth, Preservation. Digital evidence must be properly safeguarded to eliminate the risk of damage or alteration. To ensure this, the DFL team manages its laboratory environment with attention to layout, cleanliness, temperature, and magnetic exposure. The DFL also operates a centralized main server that stores all acquisition results previously conducted, thereby maintaining the preservation and integrity of digital data.

All software utilized by the DFL team is fully licensed rather than open source. This measure strengthens preservation by ensuring both the security and reliability of forensic processes, preventing any modification or corruption of data during analysis. Moreover, the use of licensed software allows the DFL

team to seek technical assistance and consultation directly from developers when issues arise.

Digital evidence preservation requires a multifaceted approach that carefully manages laboratory conditions, storage infrastructure, and forensic software to maintain evidence integrity. A study confirms that strict preservation protocols are crucial for ensuring digital evidence's legal admissibility [27].

Overall, these practices demonstrate that the DFL has complied with the components required under ISO/IEC 27037:2012. In addition to its technical components, the standard also outlines the key stages of digital evidence handling, such as identification, collection, acquisition, and preservation. Furthermore, ISO/IEC 27042:2015 extends these principles by regulating the analysis, interpretation, and reporting of digital forensic results.

Based on previous two standards, the digital forensic process implemented by BPKP is adapted to align with BPKP's internal business processes. The forensic procedure follows four stages: pre-planning, planning, execution, and reporting, in accordance with BPKP Regulation No. 17 of 2017. The overall digital forensic process carried out within BPKP is illustrated in the Figure 2.

In addition to adopting the two standards, the DFL also implements ISO/IEC 27043:2015, which pertains to information technology - security techniques - and the principles and processes for incident investigation. This standard governs the response to incidents involving digital media and is commonly applied in cases that involve investigators, as such situations often require rapid response [28].

A critical aspect of the forensic process is to secure as much relevant digital media as possible related to the ongoing investigation. The digital forensic procedures carried out are largely consistent with those outlined in the previously discussed standards. However, the pre-planning and planning stages cannot be executed thoroughly due to the need for immediate response. The DFL team typically proceeds directly to the incident site to conduct the identification and collection of acquirable electronic media.

The DFL has been officially accredited by the National Accreditation Committee (Komite Akreditasi Nasional/KAN). On October 18th, 2023, KAN granted accreditation under SNI ISO/IEC 17025:2017, ensuring that the laboratory operates under recognized international standards.

Benefits in Utilizing Digital Forensic Laboratory. First, Producing unattainable evidence through conventional audit methods. When personnel from the audited institution are involved in irregular or fraudulent activities, they do not necessarily provide documents that may indicate such misconduct. One method considered particularly effective in uncovering hidden facts, which cannot be obtained directly from the institution, is the use of digital forensic processes. Consequently, a digital forensic laboratory has been developed to support investigative audits. This laboratory assists in complementing evidence that the audit team may not be able to uncover through conventional methods, as noted by Informant TA.04.

> *"During the audit process, we frequently visited the forensic laboratory to review the data that had been collected. This allowed us to uncover narratives and pieces of the puzzle that were not apparent during the PKKN audit, with such missing elements being revealed through the forensic analysis."*

The process of obtaining such information begins with data acquisition using a write blocker device. This enables exact copying of data from the targeted electronic media to storage prepared by the DFL team, including files that have been deleted by the media owner.

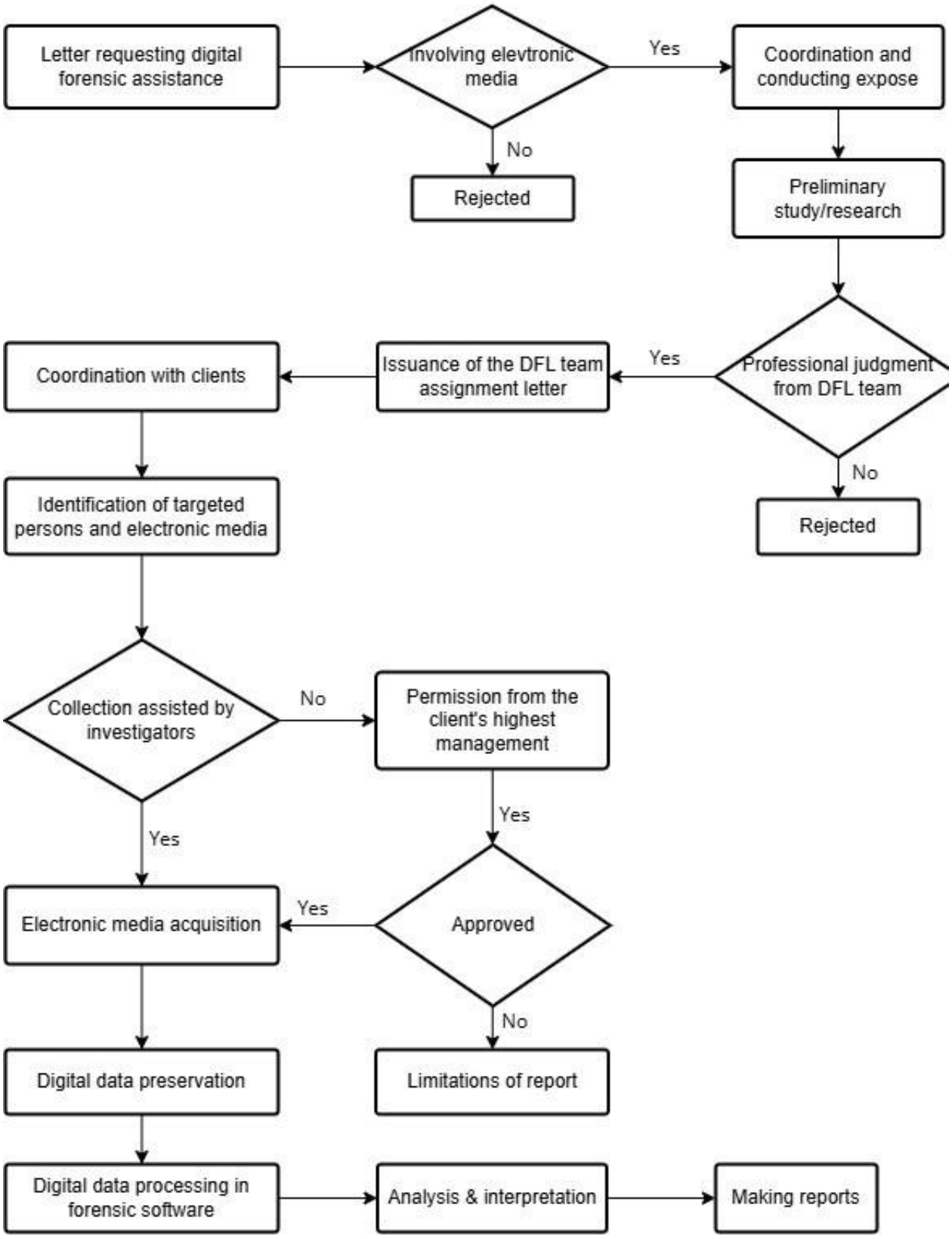

Figure 2. Digital Forensic Process in BPKP

By utilizing pre-defined and continuously developed keywords, the DFL team can be guided toward information or documents indicating potential fraud. Common evidence collected by the DFL team includes official documents, financial records, proof of fund transfers, back-dated documents, and email or WhatsApp communications (including attached files) related to specific agreements or collusions. This also involves tracing the lifecycle of documents, from draft to formal approval, which can be reconstructed through digital forensic processes.

Second, Identifying and tracing evidence of fraud. Most members of the DFL team are auditors with prior experience in investigative audits, ranging from investigative audits and audits of state financial losses to audits conducted for specific purposes. This expertise represents a significant added value for the DFL. The team not only performs data acquisition but also participates in analyzing potential corruption or fraudulent activities.

Their familiarity with common fraud schemes allows the DFL team to identify anomalies in financial transactions, such as duplicate entries, fictitious transaction evidence, price markups, or concealment schemes that might go undetected in conventional audits. Other common tactics employed by fraudsters include changing file types or securing files with passwords.

During the analysis process, the DFL team actively communicates with relevant partners regarding the information or documents discovered, assessing whether such evidence is relevant and capable of supporting the hypotheses that have been formulated.

Third, Ensuring the integrity of digital evidence. The DFL team employs write blocker hardware to clone the complete data from targeted electronic media. The use of such devices ensures that the displayed data precisely reflects the original and prevents any modification during acquisition [24]. The acquired data is rendered read-only, preventing alteration throughout the preservation and analysis processes. Forensic analysis is conducted using specialized software that further safeguards the integrity of the acquired files.

The integrity of forensic digital evidence is also maintained using licensed or commercial software. Acquiring such software involves strict procedures and may include specific inquiries from the provider. One of the tools utilized by the DFL team is Oxygen, which assesses prospective users before granting access.

Another advantage of digital forensic processes is the minimization of data leakage risk. This is achieved through offline forensic operations conducted in a secure, closed environment disconnected from the internet, substantially reducing the potential for unauthorized access and ensuring the protection of sensitive data.

Fourth, Indicating special relationships. Another benefit of the DFL's processes is the identification of potential special relationships that may be relevant to corruption cases. The DFL team identifies companies and key individuals within those companies, such as commissioners, directors, and shareholders, using data from the Directorate General of General Legal Administration (Administrasi Hukum Umum - AHU), Ministry of Law and Human Rights. The DFL can access this data through a Memorandum of Understanding (MOU) established between the Deputy of Investigation and the AHU Directorate.

Starting with companies identified by the audit team, the DFL maps affiliated companies and related parties using AHU data. To facilitate the audit team's understanding of the analysis, the DFL visualizes these relationships using Maltego. Previous research indicates that Maltego can effectively trace the flow of funds in fraud cases and reveal interconnections among individuals and entities [29].

Challenges in Utilizing the Digital Forensic Laboratory. First, Excessive workload of the DFL team. The DFL team faces a significant workload due to its limited staff of only 13 members, while assignments originate from audit teams, investigators, ministries/agencies, and state-owned enterprises. The high demand for digital forensic assistance, coupled with the inherently time-consuming nature of forensic procedures, poses a challenge for the DFL team in effectively allocating their working hours.

Second, Limited understanding of the business processes of audited entities. Although the DFL team consists of certified auditors familiar with audit procedures, they are not always closely involved in the ongoing developments of cases, unlike audit teams that continuously receive up-to-date information. One contributing factor is the high workload, which requires each DFL member to handle multiple assignments simultaneously. Understanding the business processes of the audited entities is critical in audits for identifying areas vulnerable to fraud.

While the DFL team can develop keywords based on their audit knowledge, there is a risk that the findings may not be relevant to the hypotheses constructed by the audit team. Furthermore, a high workload can reduce communication with the audit team, diminishing the effectiveness of the DFL in producing digital evidence that is relevant and supportive of the audit hypotheses.

Third, Uneven awareness of DFL procedures. Auditors generally have limited understanding of the procedures for accessing DFL services. Several informants reported lacking clear information regarding the complete process for utilizing DFL facilities and often needing to coordinate informally to access these services.

Audit teams sometimes raise questions about the boundaries of authority between the audit team and the DFL. For instance, when audit team members participate in searching for digital evidence within forensic software, they question the limits of their responsibilities. Informant TA.04 highlighted that there is no clear mapping of DFL tasks or defined boundaries of responsibility in supporting investigative audits.

This lack of clarity can lead to inefficiencies in audits involving digital forensic support, as audit teams must allocate additional time to locate and verify documents acquired through forensic processes.

Fourth, Resistance from targeted electronic media owners. As auditors, BPKP personnel do not possess the authority to seize electronic media in the same manner as investigators. Targeted electronic media are acquired through a borrowing process, which requires approval from the highest authority of the institution if the media belongs to the organization, or personal consent if the device is privately owned. This process is voluntary and non-coercive, which often results in resistance to surrendering electronic media for forensic examination.

Resistance is particularly prevalent among legally aware individuals who understand that BPKP lacks the authority to forcibly retain electronic devices for acquisition. This situation is commonly observed among employees of state-owned enterprises who are knowledgeable about their rights and may choose to refuse access. Informant TA.01 highlighted that, due to the lack of enforcement authority, any resistance encountered must be reported to immediate supervisors and documented in the audit report.

4. Conclusion

The use of the Digital Forensic Laboratory (DFL) demonstrates how technology innovation in auditing is used by a government institution aligns with international ISO/IEC standards. This alignment reflects not only technical compliance, but also a pursuit of legitimacy

and credibility of public accountability. The DFL provides several benefits in supporting investigative audits, including producing unattainable evidence through conventional audit methods, identifying and tracing evidence of fraud, ensuring the integrity of digital evidence, supporting the litigation processes and indicating special relationships. However, several challenges remain in optimizing the use of the digital forensic laboratory, such as the excessive workload of the DFL team, limited understanding of business processes of audited entities, limited support from middle management within audit teams, uneven awareness of DFL procedures, and resistance from targeted electronic media owners.

The novelty of this study lies in its comprehensive examination of the Digital Forensic Laboratory (DFL), bridging the gap between theoretical frameworks and actual operational practices within a government oversight institution. While existing literature often focuses on the technical dimensions of forensic tools, this research provides a new perspective by analyzing how international ISO/IEC standards are operationalized amidst real-world institutional challenges.

This study is primarily based on interviews and practical experience from audit and DFL teams, which may render the findings context-specific and not fully representative of digital forensic practices in other institutions or jurisdictions. Furthermore, the paper emphasizes a qualitative description of the DFL's benefits and challenges, without providing a quantitative assessment of operational effectiveness, time efficiency, fraud detection success rates, or added value to audits. Future studies could involve a comparative approach by examining digital forensic practices not only within BPKP but also in other government agencies, law enforcement institutions, or private organizations. The limitation regarding the absence of quantitative evaluation may employ quantitative methods to assess the efficiency and effectiveness of DFL operations. It is hoped that this study will enhance academic knowledge and contribute to the literature on digital forensics, which remains limited. Additionally, the authors anticipate that the findings may serve as a reference for the Deputy of Investigation at BPKP in promoting the effective utilization of the digital forensic laboratory.

References

[1] Rosyadi CF, Budding T. The Effectiveness of BPKP Fraud Audit Finding on Determining the Level of Corruption in Indonesian Provinces. Journal of Society and Governance 2017;1:88–109.

[2] BPKP. Peraturan Badan Pengawasan Keuangan dan Pembangunan Republik Indonesia Nomor 17 Tahun 2017 tentang Pedoman Pengelolaan Kegiatan Bidang Investigasi. BPKP 2017.

[3] Sinosi SM, Moerdianto R, Pontoh GT, Mediaty. Implementasi Big Data Analytics dalam Praktik Audit pada Perusahaan: Literature Review. Jurnal Ekonomi Dan Bisnis 2022;11:195–203.

[4] Machrusy MM Al, Dewi MA. Terungkapnya Kasus Korupsi melalui Bukti Audit. Kultura: Jurnal Ilmu Hukum, Sosial Dan Humaniora 2023;1:100–7.

[5] Fadhli MS. Kedudukan UU ITE dalam Ketentuan Alat Bukti Elektronik sebagai Alat Bukti Tambahan Kejahatan Siber. Jurnal Hukum Dan Kewarganegaraan 2024;5.

[6] Salih K, Dabagh N. Digital Forensic Tools: A Literature Review. Journal of Education and Science 2023;32:109–24. https://doi.org/10.33899/edusj.2023.137420.1304.

[7] K. Sindhu K, B. Meshram B. Digital Forensics and Cyber Crime

Datamining. Journal of Information Security 2012;03:196–201. https://doi.org/10.4236/jis.2012.33024.

[8] Casino F, Dasaklis TK, Spathoulas GP, Anagnostopoulos M, Ghosal A, Borocz I, et al. Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. IEEE Access 2022;10:25464–93. https://doi.org/10.1109/ACCESS.2022.3154059.

[9] Anggraini Y. Kekuatan Hukum Alat Bukti Elektronik dan Kredibilitasnya dalam Pembuktian Hukum Pidana. Jurnal Hukum Dan Kewarganegaraan 2024;6.

[10] Creswell JW, Creswell JD. Research Design Qualitative, Quantitative, and Mixed Methods Approachs. 5th ed. California: Sage Publications, Inc.; 2018.

[11] Saunders M, Lewis P, Thornhill A. Research Methods for Business Students: Fifth Edition. 5th ed. Harlow: Pearson Education; 2009.

[12] Carter N, Bryant-Lukosius D, DiCenso A, Blythe J, Neville AJ. The Use of Triangulation in Qualitative Research. Oncol Nurs Forum 2014;41:545–7. https://doi.org/10.1188/14.ONF.545-547.

[13] Fernando D, Heniarti DD, Firman Zakaria CA. Transformasi Alat Bukti Elektronik Menggunakan Digital Forensik dalam Pembaharuan Hukum Acara Pidana . Journal Justiciabelen (JJ) 2025;5:60. https://doi.org/10.35194/jj.v5i01.5506.

[14] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27037:2012 Information Technology - Security Techniques - Guidelines for Identification, Collection, Acquisition. and Preservation of Digital Evidence 2012:1–48.

[15] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27042:2015 Information Technology - Security Techniques - Guidelines for The Analysis and Interpretation of Digital Evidence 2015:1–11.

[16] Chamberlain RT. Chain of Custody: Its Importance and Requirements for Clinical Laboratory Specimens. Lab Med 1989;20:477–80. https://doi.org/10.1093/labmed/20.7.477.

[17] Benner J. Establish a Transparent Chain-of-Custody to Mitigate Risk and Ensure Quality of Specialized Samples. Biopreserv Biobank 2009;7:151–3. https://doi.org/10.1089/bio.2010.0002.

[18] Al-Khafaji NYH, Noori MI, Abbas ZM, Sharif SJ. Review safety and security of scientific in laboratories (S3IL). American Journal of Applied Science and Technology 2025;05:5–8. https://doi.org/10.37547/ajast/Volume05Issue01-02.

[19] Chesnokova E V. On the Development of Working with Personnel in Forensic Organizations under the Requirements of the International Standard ISO/IEC 17025:2017. Theory and Practice of Forensic Science 2020;15:75–83. https://doi.org/10.30764/1819-2785-2020-1-75-83.

[20] Craiger P. Training and Education in Digital Evidence. Handbook of Digital and Multimedia Forensic Evidence, Totowa, NJ: Humana Press; n.d., p. 11–22. https://doi.org/10.1007/978-1-59745-577-0_2.

[21] Villar-Vega HF, Perez-Lopez LF, Moreno-Sanchez J. Computer forensic analysis protocols review focused on digital evidence recovery in hard disks devices. J Phys Conf Ser 2019;1418:012008.

https://doi.org/10.1088/1742-6596/1418/1/012008.

[22] Hershensohn J. I.T. Forensics: The Collection and Presentation of Digital Evidence. US Department of Justice FBI 2005:1–14.

[23] Bulbul HI, Yavuzcan HG, Ozel M. Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). Forensic Sci Int 2013;233:244–56. https://doi.org/10.1016/j.forsciint.2013.09.007.

[24] Yudha F. Perancangan Nenggala Disk Duplicator (NDD) untuk Mendukung Proses Investigasi Forensik Digital. Teknoin 2018;24:29–40. https://doi.org/10.20885/teknoin.vol24.iss1.art4.

[25] Akbal E, Dogan S. Forensics Image Acquisition Process of Digital Evidence. International Journal of Computer Network and Information Security 2018;10:1–8. https://doi.org/10.5815/ijcnis.2018.05.01.

[26] Horsman G. An "order of data acquisition" for digital forensic investigations. J Forensic Sci 2022;67:1215–20. https://doi.org/10.1111/1556-4029.14979.

[27] a Abdul–Samad A, Md Siraj M, Hajar Othman S, Hafiz Rahman M, Zaharudin Ahmad Darus M. Comprehensive Review on Data Preservation Models and Standards in Digital Forensic. 2024 International Conference on Data Science and Its Applications (ICoDSA), IEEE; 2024, p. 277–82. https://doi.org/10.1109/ICoDSA62899.2024.10651616.

[28] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes 2015:1–42.

[29] Botha JG, Leenen L. Cryptocurrency-crime Investigation: Fraudulent use of Bitcoin in a Divorce Case. International Conference on Cyber Warfare and Security 2024;19:34–42. https://doi.org/10.34190/iccws.19.1.2050.

This page left intentionally blank.